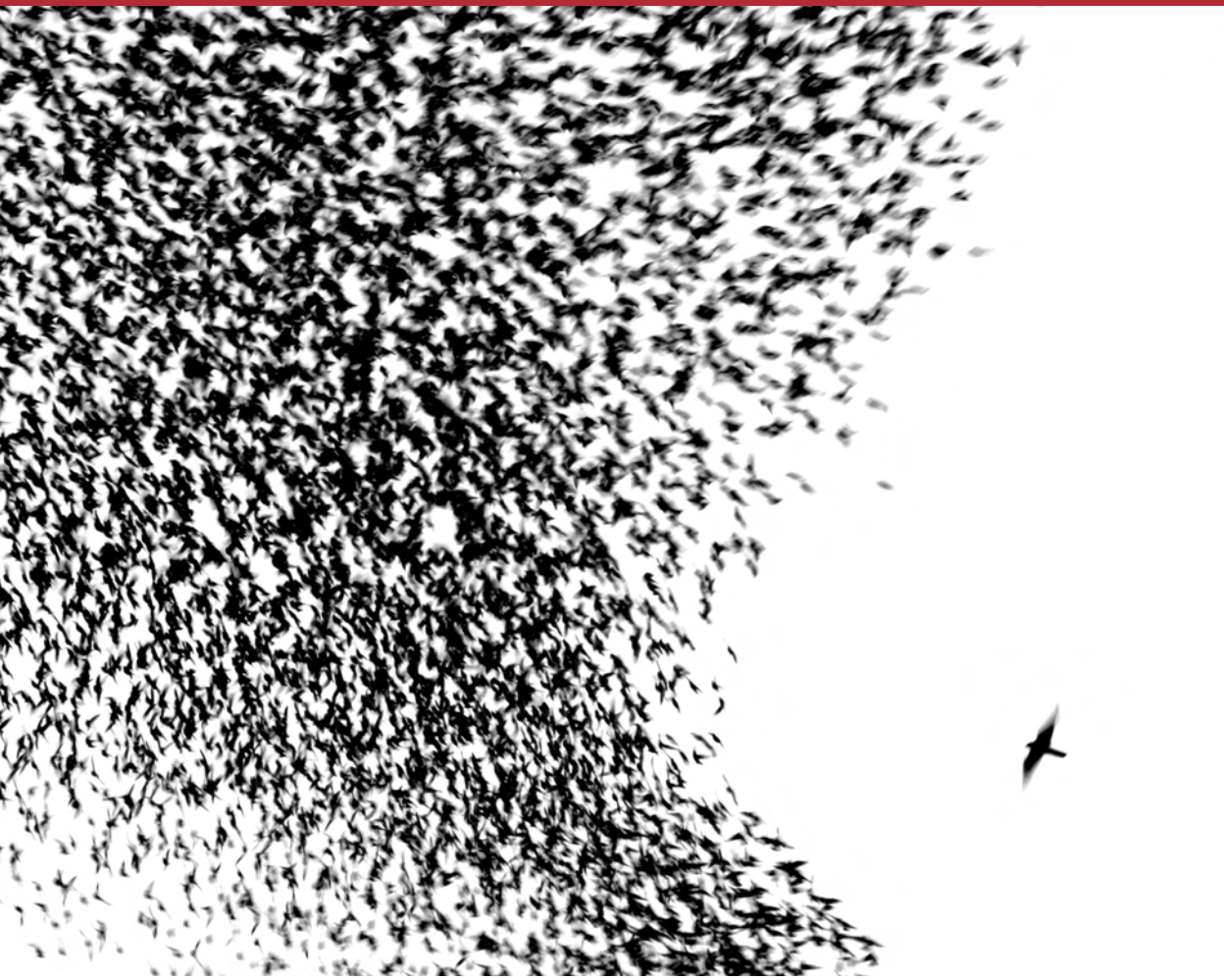
Published by White Page Ltd in association with the Serious Fraud Office

SFO serious fraud office

Serious Economic Crime

A boardroom guide to prevention and compliance



With contributions from leading advisers and featuring introductions from:

OLAF · Transparency International UK · City of London Police · Society of Corporate Compliance and Ethics · OECD · The World Bank

SFO | CONFIDENTIAL

Do you have inside information on serious fraud or corruption?

WE'RE LISTENING

Call us in confidence on 020 7239 7388

email: confidential@sfo.gsi.gov.uk

Serious Economic Crime

A boardroom guide to prevention and compliance

Published in association with the Serious Fraud Office

Consulting Editor: Harry Travers, BCL Burton Copeland

Published by White Page Ltd

whitepage

Serious Economic Crime

A boardroom guide to prevention and compliance

Consulting editor Harry Travers
BCL Burton Copeland

Editor Nigel Page

Chief production editor and sub-editor Matt Rowan

Publisher Tim Dempsey

Publishing director Nigel Page

Printing and binding Argent Litho Ltd

Serious Economic Crime
A boardroom guide to prevention and compliance
is published by:
White Page Ltd
17 Bolton Street
London W1J 8BH
United Kingdom
Phone: +44 20 7408 0268
Fax: +44 20 7408 0168
Email: mail@whitepage.co.uk
Web: www.whitepage.co.uk

Published 2011
ISBN 978-0-9565842-2-9

DISCLAIMER

This guide is written as a general guide only. It should not be relied upon as a substitute for specific legal or other professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication.

The views expressed in the articles contained in this guide are those of the authors. They do not necessarily reflect the views of the Serious Fraud Office and should not be taken as endorsed by the Serious Fraud Office. The publishers and authors bear no responsibility for any errors or omissions contained herein.

www.whitepage.co.uk

Serious Economic Crime: a boardroom guide to prevention and compliance

Foreword

Richard Alderman, Director Serious Fraud Office

We are delighted to be publishing this first edition of *Serious Economic Crime* in association with White Page. Its launch coincides with a significant period in the evolution of the Serious Fraud Office and, more broadly, with the introduction of major legislation – the UK Bribery Act – that will play a key role in the fight against corporate corruption from now on.

Having emerged from a period of uncertainty, the SFO is now securely positioned for the future. With this in mind, we are driving through a number of initiatives to further strengthen our resources, build closer links with the City, and reinforce our commitment to our international network of partners.

These are essential priorities. Economic crime today is increasingly complex in nature and international in scope. To combat this threat effectively and bring justice to the victims of fraud and corruption, we need to work in partnership with our counterparts on the world stage, as well as co-ordinating our activities with agencies closer to home.

The appointment in mid-2011 of Simon Duckworth as a non-executive director of the SFO highlights our commitment to forging closer links with the City of London. As chairman of the City of London Police Authority, Simon has brought to the SFO his wealth of experience, not just of the City and the business world, but also of high-level policing and, in particular, economic crime.

Closer links with the City of London will allow us to respond even more effectively to the challenges that complex economic crime poses for us today and tomorrow. Together we will protect the huge range of individuals and businesses affected by financial fraud and so help to underpin the City's reputation for financial probity and transparency – key assets in securing the UK's position as a pre-eminent international financial and business centre.

On the international stage, the SFO continues to shape the agenda on cross-border economic crime. And so we welcome the involvement in this publication of a wide cross-section of governmental and non-governmental organisations, from the OECD, the World Bank and Transparency International to OLAF, the European Anti-Fraud Office, alongside the

Financial Services Authority and the City of London Police.

This publication's primary purpose is to give board-level readers in the UK and international businesses informed commentary on the impact of anti-fraud and anti-corruption legislation.

As the scope of this legislation continues to expand and interact more with the legislation in other jurisdictions, so the landscape for best-practice compliance and fraud prevention has become increasingly complex. The wealth of expert insights from lawyers, accountants and specialist anti-fraud consultants in the following pages is therefore an invaluable resource.

The emphasis on compliance and prevention is significant. The SFO's remit is to identify, investigate and prosecute economic crime in the UK and beyond. But we recognise that we need to work closely with companies and financial institutions to guide and support them as they drive towards best-practice compliance. *Serious Economic Crime* is a valuable tool in supporting this important objective.

We would like to thank everyone who has contributed to this publication for their effort and commitment. We hope that the guide will be widely read by UK-based and international businesses alike. We also hope that it will increase the awareness of fraud and corruption, prevent them from happening, and help corporates to stay compliant.

Richard Alderman, September 2011

Contents

Contents

This page intentionally left blank

Serious Economic Crime: Introduction and overview

Harry Travers, Consulting Editor BCL Burton Copeland

It is significant that, for this first edition of *Serious Economic Crime*, published by White Page in association with the Serious Fraud Office, lawyers from the *private* sector – more usually known for *defending* clients against allegations of serious fraud – have been asked to contribute to, and indeed edit, the publication.

Until relatively recently, the way in which defence lawyers and the SFO were likely to interact was as part of the traditional model of the investigation and prosecution of serious fraud. This would often involve, as far as the suspect was concerned, high-profile arrests and the simultaneous execution of several search warrants early in the morning, followed perhaps by a series of interviews under caution over many months, the eventual bringing of charges, heavily fought interlocutory hearings, battles over disclosure, and ultimately the often lengthy adversarial trial process.

While it is certainly the case that all of these things still occur regularly, a large part of the discussion in this book is about a new, more consensual approach towards corporate crime on the part of the SFO, how that is operating in practice, and how it is likely to develop.

From criticism to a shift in culture

The traditional approach has occasionally led to instances where cases brought by the SFO have collapsed spectacularly, causing massive media criticism and public disquiet. In reality, such results, however dramatic, were and still are to be expected from time to time, and merely match reverses suffered by other lead UK prosecutors (such as the Crown Prosecution Service) and the Revenue and Customs Prosecutions Office (now merged into the CPS).

However, the approach in the United States has seemed more sure of producing results. Given the higher conviction rates achieved by comparable prosecution agencies in the US, it is no accident that following the reporting of the recommendations of the UK Fraud Review in 2006, a former New York Prosecutor, Jessica de Grazia, was commissioned to produce a report on the work of the SFO, "with particular reference to practice in overseas jurisdictions and any related internal organisational and structural issues".

The controversial report, published in June 2008, contained a comparison of the SFO with the US Attorney's Office for the Southern District of New York, and the Manhattan District Attorney's Office. It criticised the performance of the SFO as compared with those two agencies, and stated

that the "lack of focus" in SFO investigations was "a matter of grave concern". It criticised what it termed a "pass the buck", risk-averse and "complaint" culture in the SFO, which "discourage[d] robust decision making and innovative and effective use of powers", and also led to a "culture of delay".

A lot has changed since the publication of that report, and the 'new approach' of the SFO is well documented in the various chapters contributed to this publication by both governmental and non-governmental organisations, and private sector law firms.

An educator, not just an enforcer

Since his appointment in April 2008, the current Director of the SFO has sought to work with the City and leading law firms to try to create a culture of compliance, and a dialogue between stakeholders in the UK system for investigating and punishing the most serious economic crimes.

The temptation to 'borrow' wholesale from the US system has been resisted. It should not be forgotten that the US system of plea bargaining was famously described in *The Bonfire of the Vanities*, the movie of Tom Wolfe's novel, as the sort of system where "witnesses perjure themselves" … "prosecutors enlist the perjurers" … and "a District Attorney throws a man to the mob for political gain".

There are many in practice in the US who still hold that view, and it is important that while elements of the US plea bargaining system may be emulated in the UK, the traditional values of the UK system in terms of fairness, a level playing field, equality of arms and the need for like cases to be treated alike (for example, in deciding which should be subject to criminal investigation, and which should have the possibility of civil resolution) are upheld.

Clearly the SFO is attempting to deal with fraud firmly and to create a culture where lawfulness and the upholding of high moral standards are rewarded in business, but also where there is a credible deterrence to those tempted to eschew those standards. Part of the new collaborative process involves the SFO working with companies that are affected by fraud and by their attempts to create that culture.

The changing legal and factual landscape for corporate investigations has lent itself to these cultural changes, with issues such as self-reporting, whistleblowing and civil recovery requiring a new and constructive approach on both sides of the issue.

At the same time, the SFO clearly seems to welcome the debate as to how serious economic crime should be dealt with, so that important changes in law and prosecutorial approach are widely examined before they are introduced. Indeed, the SFO's 'new approach' is to see itself not just as a *enforcer*, but also as an *educator*.

Collaboration from all corners

In many ways this publication, with its contributions from both the public and private sector, and from a wide variety of expert sources, is emblematic of this new approach.

Part I features chapters from a number of regulators and key bodies. The Financial Services Authority (FSA) describes the role it plays in prosecuting market abuse and insider dealing, while the chapter by the City of London Police highlights what can be achieved by domestic prosecution agencies working in partnership with equivalent agencies on a global scale.

The Organisation for Economic Co-operation and Development (OECD) expands on the benefits of international co-operation, following closely the pioneering Oslo conference that brought governments, non-governmental organisations and business together in the fight against financial crime, while the World Bank outlines the historic 2010 agreement between multilateral development banks to adopt common definitions of fraud and due process and, crucially, to recognise and enforce debarment decisions of the other signatories.

The chapter by Transparency International brings global perspectives on counter-corruption measures, and in a separate chapter the World

Bank outlines its anti-corruption agenda. We hear also from the European Anti-Fraud Office (OLAF) on the European Union approach to combating money laundering, while the Society of Corporate Compliance and Ethics introduces non-regulatory compliance solutions.

The main offences

Most of the private sector law firms whose chapters feature in this publication specialise in this area, and it is a legal services market that is becoming increasingly attractive to newcomers. It is to be hoped that lawyers and corporate directors will gain insight into the current issues in this area, as well as drawing knowledge from the chapters in Part II on the 'black letter' law of serious economic crime, which address the main offences that have historically been committed by corporates and those associated with them.

In Part II, Covington & Burling outlines the provisions of the Bribery Act 2010, with the chapter by Fulbright & Jaworski examining the crucial differences between the application of the Foreign Corrupt Practices Act in the US and the new UK legislation.

The law on cartels and insider trading is examined by Linklaters and Reynolds Porter Chamberlain respectively.

The chapter by BCL Burton Copeland and barrister Nicholas Yeo at Three Raymond Buildings sets out the core, yet often overlooked, fraud and related offences prosecuted by the SFO. After all, it should not be forgotten that the majority of criminal investigations conducted by the SFO involve allegations of 'straightforward' fraud and dishonesty in a corporate context.

The main money laundering offences contained in the Proceeds of Crime Act 2002, together with the confiscation regime and law on civil recovery orders, are set out and discussed in a further chapter by Covington & Burling.

The chapter by Morrison & Foerster then goes into further detail on the principal money laundering offences, and deals also with the statutory defences. The chapter also contains a focus by PWC on the implementation of anti-money-laundering procedures in the regulated sector.

An introduction to the complex Financial Services and Markets Act 2000 by Saunders Law builds on the Financial Services Authority's introduction to the work it does in parallel with the SFO.

The scope of UN sanctions and how they apply to companies is addressed in the chapter by O'Melveny & Myers.

In addition, given the very severe economic consequences in terms of fines and reputational damage (and also prison sentences) that can result from criminal liability for fatal accidents in the workplace, it was decided that no boardroom guide on corporate crime would be complete without a chapter on the Corporate Manslaughter and Corporate Homicide Act 2007, and the main health and safety offences that companies and their directors and employees can commit. The contribution is provided by BCL Burton Copeland.

Investigations

In terms of the 'new approach' and where the investigation and prosecution of serious economic crime is going, Part III contains a wealth of material from leading private sector law firms. The key issue of how the SFO has sought to encourage corporates to self-report is dealt with by Covington & Burling, whose chapter charts the development of the initiative, which began with the publication on July 21, 2009 of the document 'Approach of the Serious Fraud Office to dealing with overseas corruption'. It then goes on to study how this has worked in practice, highlighting some of the very real pitfalls for corporates in seeking to obtain a measure of certainty as to what will happen to them if they self-report, and also the difficulties for corporates in reaching a global settlement as a result of the differences between the UK and US systems.

The idea for the chapter by Matthew Reinhard of Miller & Chevalier in Washington

DC flowed from a chat I was having with him when he commented that the way in which the SFO was talking to law firms advising corporates reminded him of the way the US Department of Justice was talking five years ago. On that basis, and in trying to predict what the SFO might be seeking to do in the UK and what issues might arise in the *next* five years, it struck me as a good idea to ask him to write a chapter on developments in the US on the investigation and prosecution of serious fraud in the *last* five years.

The chapter therefore charts the progress made in the States, particularly on the issue of how a prosecutor should form a judgement on the extent to which a corporate has shown a willingness to disclose its wrongdoing and to co-operate. This of course is highly relevant to the prosecutor's decision on whether, and how, to charge a corporate with a criminal offence. In the US, this has been beset with difficulties, with early guidance to DOJ prosecutors indicating that one factor in assessing co-operation was whether the company had agreed to waive attorney-client privilege, and another being whether a corporate "appears to be protecting its culpable employees and agents" – for example, by paying their legal fees. Both of these criteria are now apparently seen as mistakes in the US, and the relevant guidance to prosecutors has been revised.

It is to be hoped that the UK will learn from these mistakes, but it should be remembered that they were only really remedied in the US as a result of tenacious work on behalf of their clients by US lawyers. After all, the intrinsic value of a robust adversarial system is that, whatever the good intentions of the state, fairness in the criminal justice system can often only be achieved through lawyers fighting their clients' corner – if necessary, through litigation. This applies as much for corporates accused of crime in a corporate environment, as for individuals accused of general crime.

Part III also includes chapters on other issues relating to investigations conducted by prosecutors and regulators, as well as those carried out internally by companies. The chapter by Dewey & LeBoeuf focuses on 'dawn raids', particularly in the context of cartels and other anti-competitive behaviour, while the contribution by Allen & Overy deals primarily with how the damage caused to a corporate by an investigation relating to serious economic crime can be limited by a variety of practical measures, both before an investigation starts and right through to its conclusion.

A further chapter by PwC focuses on some practical issues that companies need to face when being investigated by outside enforcers such as the SFO.

The chapter from Kobre & Kim examines some key considerations in conducting effective internal investigations, with an eye to avoiding common pitfalls. It also contains an additional section from PwC containing recommendations on the practical implementation of such investigations.

A contribution by Forensic Risk Alliance makes detailed recommendations on how to run a UK or European e-discovery exercise, particularly with multi-jurisdictional investigations in mind, and given the legal and practical need to preserve electronic data where litigation is 'reasonably anticipated'.

The increasing relevance and development of the international mutual legal assistance regime, which enables prosecutors to investigate in foreign jurisdictions, is explained in the chapter from Kirkland & Ellis.

Finally in Part III, a further chapter by Forensic Risk Alliance explores the key benefits of forensic accounting in identifying, analysing, testing and presenting financial evidence.

Special focus

The final section, Part IV, is designed to give readers an insight into specialist economic crime topics – not just legal areas, but also practical advice on managing specialist risk.

While the SFO has recently been able to secure the conviction of a number of major corporate, rather than individual, defendants, it is noteworthy that none of these convictions has been secured as a result of a contested trial.

Indeed, the impression given to some observers is that the guilty pleas in the UK were entered simply because the corporate defendant had entered similar pleas in the US, and wished to seek a global settlement.

In reality, the law on achieving the conviction of a corporate defendant is anything but simple. It is based on the 'identification principle', by which a company can only be guilty if its 'directing mind' has committed the criminal act. In a speech delivered at the London School of Economics in March 2011, the current Director of the SFO explored possible changes in the law whereby the conviction of corporate defendants might be secured more easily. This is an area of particular interest to lawyers, and the chapter by Kingsley Napley examines it in detail. However, as matters stand, corporate defendants are likely to be aware of the difficulties facing the SFO as a result of the identification principle, and will continue to bear them in mind when exploring the possibility of a settlement.

In the current climate, companies, as well as being concerned about *criminal* liability for economic crime, are naturally also concerned about *civil* liability, especially as the courts will generally allow a civil claim and a criminal prosecution to proceed in parallel. Although this publication is mainly about criminal liability, it was thought appropriate to include some discussion of possible civil liability flowing from the same subject matter. This topic is so broad as to be incapable of treatment in a single chapter, but the contribution by barrister Jonathan Cohen of Littleton Chambers and BCL Burton Copeland attempts to deal with the types of civil claim that a company may face, and some of the issues that arise through the inter-relation of the civil and criminal proceedings.

One particular area that non-UK companies are concerned about is, unsurprisingly, their potential criminal liability under the Bribery Act 2010, and the chapter by Linklaters is specifically devoted to this issue.

Advice on protecting intangible assets from intellectual property theft and industrial espionage, and preventing breaches of cyber security, is given in the chapters by Stroz Friedberg.

Finally, specialist areas of corporate compliance, including implementing effective due diligence on business partners, and confidential whistleblowing regimes, are considered in the chapters contributed by Reed Smith and PwC.

A culture of co-operation

It is hoped this publication will play its part in continuing the dialogue as to how serious economic crime should be dealt with in the UK. The collaboration in producing it, between the public and private sectors and various international non-governmental organisations, reflects the new culture of co-operation that is developing in the UK as a result of the SFO's desire to engage with business and encourage a consensual approach to the treatment of serious economic crime.

Thanks are due to the publisher White Page for having the patience and tact required to regulate such an eclectic mix of contributors; to the SFO for having the courage to work with the private sector to produce it; and, of course, to the contributors, who have on occasions had to deal with what can only be described as hectoring from the consulting editor.

Harry Travers, September 2011

This page intentionally left blank

PART I

National and global perspectives

This page intentionally left blank

1

Preventing serious economic crime: the SFO's priorities and successes

Richard Alderman, Director The Serious Fraud Office

The Serious Fraud Office (SFO) was set up in 1988 to root out individuals and businesses that acquire profits fraudulently, undermining markets as a result and destroying the trust of investors and confidence in UK plc. Serious economic crime is what the SFO was set up to fight and this is the challenging work we continue to carry out today. In doing so, I believe the SFO helps instil confidence in the ethical practice of good British businesses.

Where we were

The SFO was already 20 years old when I joined it and fundamental questions were being asked about its role, its culture and how it operated. My aim was to build on the work of my predecessors yet challenge our existing approach so that I could turn it into a modern, outward-facing and collaborative organisation. Two key issues were at the top of my agenda: to put the victims of economic crime at the centre of the SFO's work and to engage with the City of London.

Against the backdrop of the global financial downturn, the past few years have been challenging for everyone at the SFO. It has been a time of transition, transformation, reduced funding and adjustment. Three years on, I am pleased to report that the SFO's performance is the best it has ever been. It is also costing the taxpayer less and less each year.

Now

The SFO's cases are extremely complicated, often requiring co-ordinated action across many jurisdictions. When money can be moved around the world in seconds and skilfully concealed by devious fraudsters, an organisation like the SFO, with its skilled investigators and prosecutors, is vital. We are the organisation best placed to protect the public as we have the powers, the technology and the expertise to track economic criminals across the world and to obtain justice for victims.

Thanks to more efficient processes and more sophisticated technology, we have slashed the time it takes our investigators to get cases to court and we are maintaining high conviction rates. But I am most proud of what we have achieved for victims. Economic criminals attack some of the most vulnerable members of British society and some of the poorest people abroad. By using legislation in innovative ways, we are recovering huge sums of money for them.

By the end of 2010-11, more than £64 million had been or was due to be returned to victims. Our action is also seeing money being taken off criminals and returned to the government: in the first few months of 2011 alone, some £10 million went to HM Treasury – a welcome sum, particularly during an economic downturn.

A change in approach

Traditionally we waited until fraud had been reported to us before we began an investigation. One of the key ways in which we have become more proactive is the sourcing of our own cases. We now respond to concerns from MPs and follow up on key issues in the media, and, through our 'open door' policy, we have also seen an increase in whistleblowers and companies coming to us to 'self-report'.

Last year, 30 per cent of the cases we took up, we had sourced ourselves; this year, we hope to increase that to 40 per cent. This is in addition to the volume of work handled by the experts in our intelligence team, who deal with around 300 queries a month – far more than a small organisation like ours can take on. While I want all cases that fit the profile of serious economic crime to land in our in-tray, I have to make some hard decisions on them as it is not always in the public interest for the SFO to take up every case.

Last year, I accepted 15 cases and I expect this figure to increase year on year. Where a case does not meet our criteria for acceptance, we refer it to one of the other law enforcement agencies that deal with economic crime.

In recent years, we have been quicker to get cases to the point of charge. This is because we have sharpened our strategy and made our investigations more focused. We now have investigators who are experienced in working with informants, instigating covert techniques and using a wide range of other approaches.

On top of all this, we have invested in new technology. The way in which economic criminals communicate has changed out of all recognition. They use social networks, emails and electronic transfer systems, all of which produce unimaginable volumes of material. Without the right technology, it would take us years of painstaking work to review all the evidence in one case alone.

Our new digital review system is one of the best on the market. While traditional computer forensics techniques dig deep into a handful of computers, our system allows us to review huge volumes of data incredibly quickly. The benefits are clear. In 2010-11 we processed the evidence contained in 70 million documents. We can now handle up to 100 gigabytes of new information a day – a 2,000 per cent increase year on year.

As a result, our case teams can respond swiftly to court requirements. For example, in response to a judge's order, one of our teams was able to identify and produce more than 47,000 emails overnight – an achievement that allowed the prosecution to progress smoothly.

Working and engaging with others

Changing the SFO's internal focus to make us more effective and efficient goes hand in hand with a more open approach to businesses and other partners. We now look beyond traditional case prosecution. From my discussions with business and professional advisers, it became clear to me that there was an appetite for a system under which companies could 'self report' cases of overseas corruption to us.

My view is that if a company is willing to come to the SFO at the outset, then we must listen. We now work with businesses that identify problems and raise them with us; we talk through potential solutions together to ensure the wrongdoing does not happen in the future.

The SFO will not and cannot help companies to sweep illegal activity under the carpet, but we do want to support good corporate behaviour and help businesses that are genuinely committed to ethical governance to recognise their mistakes and move on. This allows us to concentrate our resources on those companies we know are out there that continue to use bribery and corruption

to undercut their rivals. I am determined to bring companies like this – British or foreign – before the UK courts.

The new legal climate

The UK Bribery Act is now in force. In the two years leading up to it, I and other members of the SFO gave many talks on various aspects of the Act. We talked to industry and ethical groups and the legal advisers at high-profile corporates. We also produced readily accessible guidance to support the core guidance issued by the Ministry of Justice. Businesses therefore have little excuse for not understanding what is required of them.

My commitment is to ensure that companies can meet their requirements, move towards better corporate governance and ask us for help and guidance when appropriate. My aim is for the SFO to work with corporates as part of a solution, not for bad practices to be a continuing problem. In all cases, we want to see board-level commitment demonstrated to the highest standards of corporate governance.

Cross-border co-operation

We have memorandums of understanding with partners across the world and these help us assist overseas authorities with their investigations.

Deterring criminals abroad who target victims in the UK and use UK companies to launder money through UK financial institutions is one of the reasons why the SFO has a team of investigators who help overseas authorities. Our International assistance team has close relationships with foreign law enforcement agencies whose co-operation is often essential for our own domestic investigations and prosecutions. While the type of help we normally give is operational, we do also share information under official gateways.

Requests for assistance from overseas authorities reflect the diversity of criminal activity perpetrated all over the world. Last year the team helped over 30 jurisdictions in Europe, North and South America, the Middle East and Asia Pacific. Some of these cases involved high-profile corruption, 'Ponzi' schemes, 'boiler room' scams, corporate fraud, forgery, securities fraud, embezzlement, tax evasion and money laundering. There are often many millions of pounds at risk in these cases, which goes to show the determination of criminals to cause harm to national economies, corporates and other victims. Thanks to our help, convictions were obtained in a number of cases.

Co-operation like this reflects the increasing desire among UK law enforcement agencies to respond to overseas requests in a professional and organised manner – all of which enhances the UK's reputation on the international stage for mutual legal assistance.

Recent results

- In a Ponzi scheme, Kevin Foster was sentenced to ten years' imprisonment for running an unauthorised investment business. Over three years, through the staging of roadshows, his scheme attracted £34 million in investments from 8,500 people all over the country.
- In one of the biggest mortgage fraud cases, two men were sentenced to a combined total of 20 years' imprisonment for a £50 million fraud. Saghir Afzal was sentenced to 13 years, the second-highest sentence in an SFO case, and Ian McGarry to seven years for providing false valuations used in mortgage applications.
- In two civil recovery orders, DePuy International, the orthopaedics company, was ordered to pay almost £5 million and engineer MW Kellogg over £7 million.
- Julian Messent was sentenced to 21 months' imprisonment after pleading guilty to making or authorising corrupt payments to Costa Rican officials in the state insurance company. Mr Messent was head of the property (Americas) division at PWS International, where he was responsible for securing and maintaining contracts for reinsurance in the Central and South America regions.
- Stuart Pearson, the former chief executive of an AIM-listed investment services company, received a 12-month custodial sentence after

being found guilty of making misleading statements by falsely claiming the company was an attractive investment through official London stock market announcements and personally to investors. He was also disqualified from acting as a director of a company for five years.

- BAE Systems was fined £500,000 in December 2010 after admitting to failing to keep adequate accounting records in relation to a defence contract to supply an air traffic control system to the government of Tanzania.

The future

The SFO can do even more with greater powers – and I am pressing for them. I believe deferred prosecution would be a great tool for the SFO and it chimes well with my pledge to allow businesses, committed to acting ethically, to continue trading. I see no reason why defendants who agree to abide by preset conditions and genuinely show they are capable of setting things right should not be given the opportunity to do so.

I will push on with this debate, but in the meantime I want to achieve results that society values and I am always conscious of the need to do more for less. The UK government is committed to combating economic crime and arming agencies with the powers required to deal economic criminals the kind of body blows that white-collar criminals have previously been able to avoid. These powers are still a matter for discussion.

In the meantime, the SFO's skills and determination will continue to bring economic criminals to book, deliver justice for victims and provide value for money.

2

The FSA's role in prosecuting market abuse and insider dealing

Tracey McDermott, Acting Director of Enforcement and Financial Crime
The Financial Services Authority

The Financial Services Authority (FSA) is currently the single UK regulator of financial services. As such we have a number of responsibilities in relation to financial crime.[1]

As a gatekeeper, we seek to use our powers to prevent UK financial services from being infiltrated by those of dubious integrity.

As a supervisor, we seek to ensure that the firms we regulate have adequate systems and controls to counter the risk of financial crimes such as money laundering and bribery and corruption.

As a consumer protector, we take action to warn and educate people about the perils of dealing with unauthorised businesses and to close down and punish those operating such businesses.

This chapter focuses primarily on our role as the principal UK authority responsible for policing conduct in the UK markets.

Context

Tackling market misconduct has been, and remains, a priority for the FSA. It is directly relevant to three of the statutory objectives given to the regulator by the Financial Services and Markets Act 2000 (FSMA), namely:

- maintaining confidence in the UK financial system
- securing the appropriate degree of protection for consumers
- reducing the extent to which it is possible for a regulated business to be used for a purpose connected with financial crime.

Dealing forcefully with misconduct in the markets helps to ensure confidence in the UK financial system by providing participants in the equity markets with a level playing field. It protects consumers who invest in securities and it reinforces the importance among authorised firms of protecting highly valuable confidential information from misuse.

FSA powers

The FSA has both criminal and civil powers for tackling market abuse. In recent years there has been a focus on insider dealing, which is a relatively new concept in UK criminal law. The offence was first created in the Companies Act 1980 and evolved over the years to the offences contained in the Criminal

Justice Act 1993, which carry a maximum sentence of seven years' imprisonment.[2]

The parallel civil offence was created in the FSMA and came into force in 2001. It was updated and revised following the introduction of the Market Abuse Directive in 2005.[3] The FSMA market abuse regime is unusual among regulatory requirements in that it applies to anyone, including those overseas, whose activity relates to UK markets, rather than being limited to those authorised or approved by the FSA.

The regulator has a range of civil sanctions under the FSMA for dealing with market abusers. These include the power to impose an unlimited fine (Section 123), to issue a public statement that an individual has engaged in market abuse (Section 123), or to require the payment of compensation to victims (Section 384). The FSA can also apply to the court for a restitution order (Section 383) or for an injunction to prevent further market abuse (Section 381).

For those approved to perform regulated functions, the FSA can withdraw their approval (Section 63), and there is also a general power to prohibit any individual from performing all functions (or all specified functions) in relation to a regulated activity carried on by an authorised person, if it appears to the FSA that the individual is not a fit and proper person to perform those functions (Section 56). A finding that a person had deliberately committed market abuse or insider dealing would usually be powerful grounds, indicating a lack of fitness and propriety, for a prohibition order to be made.

There are also both criminal and civil sanctions for other forms of market misconduct, in particular market manipulation.

An abuse of trust, a threat to confidence

The insider dealing offences (both civil and criminal) are highly technical ones. The essence of the wrongdoing is, however, simple. Markets depend, for an efficient price-formation process, on participants having access at the same time to relevant information that might affect the price of a security.

In organised markets, there is a sophisticated process of formal announcements to the market underpinned by rules for listed companies governing when and how they should make such announcements.

Clearly, however, there will be times where information is known to privileged insiders – such as directors, investment bankers and lawyers – that has not yet been made public. They are given this information because they hold positions of trust and in order to advise or assist the company. They are prohibited from using that information to trade because of the unfair advantage they would have over other market users.

Insider dealing takes place when that privileged access to information is abused. As the Financial Services and Markets Tribunal said in 2006 in the case of *Parker v FSA*: "Mr Parker used information which had come to him in order to place bets to his advantage and to the detriment of IG [Index, the spread-betting company], which he knew had no access to the same information. Using ordinary language, that is cheating and it would be recognised by any reasonable person as such."

This sentiment was echoed by the Court of Appeal three years later in the case of *R v McQuoid* (2009), where Lord Judge CJ said: "The message must be clear: when it is done deliberately, insider dealing is a species of fraud; it is cheating."

But insider dealing is not serious simply because of its impact on the parties to a single deal. It also has an impact on confidence in the markets – to which, whether directly through shareholdings or indirectly through pensions or other investments, most people in the UK are exposed.

As Judge Testar said when passing sentence in *R v McQuoid*: "This is not a victimless crime – this is a crime which does undermine confidence in the integrity of the market and this is a confidence which is of great importance to the welfare of the community as a whole."

The FSA approach – credible deterrence

Up until 2007 the criminal offence of insider dealing had been prosecuted relatively

infrequently and with limited success. It was widely recognised as a difficult offence to investigate and prosecute. Indeed, unlike most criminal offences, it was often not even apparent at the start of an investigation that an offence had been committed; the trading could be timely but also entirely legitimate. This was further complicated by the requirements to prove specific mental elements and to present sometimes complex technical evidence to lay juries.

At the start of the last decade, a civil sanction for market abuse was introduced for the first time under the FSMA. Part of the aim was to achieve a quicker and more efficient way of tackling market misconduct by providing additional tools and applying the lower civil burden of proof.

As discussed above, the FSA gained a number of powers for enforcing this regime and went on to pursue some significant cases through the disciplinary and tribunal process.[4] However, it became clear in the process that tackling market abuse, even through the civil route, remained challenging, time consuming and resource intensive.

Alongside the civil regime, the regulator also used its criminal powers. Notably, in 2005, two former directors of AIT plc (Carl Rigby and Gareth Bailey) were convicted, following an FSA prosecution, of recklessly making misleading, false or deceptive statements to the market regarding profit forecasts for AIT. They were sentenced, on appeal, to 18 and nine months respectively.

In 2007, as part of the FSA's overall strategy of credible deterrence, we made the strategic decision that, together with the use of the civil market abuse regime, we would make more of our power to prosecute individuals for market misconduct and, in particular, insider dealing. We had concluded that our civil powers were not a sufficient deterrent for those who were determined to seek personal gain by abusing the markets. We decided that the risk of custodial sentences, as well as confiscation of proceeds and the stigma associated with a criminal conviction, would serve as a more effective deterrent.

Surmounting the obstacles

We were well aware at the FSA of the challenges that this would bring. We recognised at the time that because of the differences in the standard of proof and in the elements to be established under the various provisions, an approach that had criminal prosecutions at its heart would remain challenging.

Further, we were aware that insider dealing had, historically, proved a hard nut to crack. For example, the Department of Trade and Industry had formerly been the primary prosecuting authority for insider dealing. From 1995 to 2009, it brought eight prosecutions resulting in seven convictions. Some cases were undertaken by other agencies, such as the Serious Fraud Office and the Crown Prosecution Service, but insider dealing remained an offence that was rarely prosecuted.

We recognised that it was not enough to have good investigation and prosecution skills. Successful outcomes in insider dealing cases depended on the FSA also bringing to bear its significant technical and practical expertise in the operation of markets and trading and maximising its use of analysis and intelligence.

With the right tools and people in place, we secured our first criminal convictions for insider dealing in 2009. Since then, we have secured a total of ten convictions to date, all resulting in custodial sentences (some suspended). As of July 2011, 13 more individuals were awaiting trial for insider dealing and four for making false and misleading statements.

The complexity and seriousness of these cases continues to increase and we are committed to carrying this important programme of work forward into the Financial Conduct Authority (FCA).

As a prosecutor, we are required to consider confiscation in all cases; as well as imposing custodial sentences on insider dealers, the courts can deprive them of the benefit of their crimes. Our insider dealing prosecutions have so far resulted in more than £1.7 million being confiscated. We regard this as a powerful disincentive to committing a crime that is primarily driven by greed.

FSA enforcement: the process of a regulatory investigation

Appointment of investigators
We appoint investigators and, if appropriate, send a Notice of Appointment of Investigators to the firm or individual. We do this as quickly as practicable.

Scoping discussion
Our initial discussions with the firm or individual are intended to provide a clear indication of the scope of the investigation, including how the process will unfold and the individuals and documents the investigators will initially need access to.

Investigation work
The appointed investigators carry out the investigation, which may include, for example, requests for documents or information and interviews of witnesses and subjects. Following the investigation work, there is an internal legal review of the case by a lawyer who has not been part of the investigation team.

Preliminary Investigation Report (PIR)
If appropriate, we send a PIR to the firm or individual, who has 28 days to respond. They can apply for extra time to complete their response.

Submission to the FSA Regulatory Decisions Committee (RDC)
If, following their investigation, our staff believe action is justified, they submit case papers to the RDC. This includes an Investigation Report, which takes account of the firm or individual's response to the PIR. The RDC considers the submission.

Warning Notice
If the RDC decides it is appropriate, it will send out a Warning Notice informing the person concerned that the FSA intends to take further action. The firm or individual has the right to access material relied on by the RDC in taking its decision, together with secondary material which might undermine that decision. The firm or individual has 28 days to make oral or written representations to the RDC and can apply for extra time.

Oral and written representations to the RDC
After it receives the Warning Notice, the firm or individual may make written or oral representations to the RDC. The RDC will then meet again to consider the facts of the case, including the firm's or individual's written representations and any new information that may have come to light.

Decision Notice
The RDC makes its decision and, if appropriate, issues a Decision Notice. The firm or individual has 28 days to make a referral to the Upper Tribunal.

Upper Tribunal (Tax and Chancery Chamber): a fresh look
The Tribunal is entirely independent of the FSA and will consider the entire case afresh. A Tribunal hearing is normally held in public.

Private warning
We may issue a private warning at any stage in the procedure and in doing so we close the investigation.

Settlement discussions
The parties can seek to resolve the issue by having settlement discussions with us at any stage in the procedure.

Closure
If we find there is no case to answer, we close the investigation at any stage in the procedure. If the RDC finds there is no case, either before or after representations, the FSA closes the investigation. If after representations, the RDC finds there is no case, a Notice of Discontinuance may be issued.

Final Notice
If no referral is made to the Upper Tribunal following the Decision Notice, a Final Notice is issued to the firm or individual concerned.

Published information
We will publish such information about the matter to which a Decision or Final Notice relates as we consider appropriate.

Tribunal's determination
The Tribunal decides what action the FSA should take in relation to the matter referred to it (including issuing a Notice of Discontinuance if the case is not made out).

The road has not been without its obstacles. We have faced challenges around our ability to prosecute – suggestions that we had no power to prosecute money laundering offences linked to insider dealing, or to prosecute insider dealing itself without the consent of the Director of Public Prosecutions, and even suggestions that it was unfair and improper to bring prosecutions at all. However, these disputes have been determined in our favour by the Supreme Court and Court of Appeal.[5]

Facing these legal challenges and obtaining important decisions on legal points is a critical step on the path to being a credible force in this area.

Continuing the clampdown on market abuse

While we have increased the use of our criminal powers, we have also continued to utilise the civil market abuse regime. Having access to two different, but complementary, avenues for dealing with misconduct means we can be more flexible in our approach.

When making the decision about whether to prosecute criminally or use the civil regime, we carefully consider all aspects of the case and strictly follow the guidance laid down in the Code for Crown Prosecutors and the FSA Enforcement Guide (EG 12.8). This allows us to choose the right outcome depending on the specific case. A non-exhaustive list of the factors to take into account when determining whether to proceed on a regulatory or criminal basis is explicitly set out in the Enforcement Guide. Among these factors is the level of co-operation – we give credit for people and firms who effectively self-report and assist with action against others, and recognise that this may be significant in choosing between a criminal prosecution or regulatory action.

When we conclude that criminal prosecutions are not appropriate – whether for evidential or public interest reasons – we have recognised that the levels of penalty imposed must be significant enough to change behaviour.

Consequently, where we have pursued regulatory outcomes, the value and volume of fines in this area has increased. We have also prohibited a growing number of individuals from the financial services industry on the basis that their involvement in deliberate market abuse demonstrates a lack of integrity such that they are not fit and proper.

Since 2007, the total fines imposed for civil market abuse exceed £14 million and we have prohibited 12 individuals.

Financial penalties

In March 2010 we published a new policy that established a consistent and more transparent framework for the calculation of financial penalties. Under this policy, the starting point for a penalty on an individual who commits market abuse is the greater of:

- where the market abuse is related to the individual's employment, up to 40 per cent of their salary and benefits (including bonuses) from their job over the 12 months preceding the final market abuse – or, if longer, the period of the market abuse
- up to four times the financial benefit made by the individual as a direct result of the market abuse
- in serious cases of market abuse, £100,000.

The individual is also required to give up all of the financial benefit made as a direct result of the market abuse. The minimum starting point of £100,000 for serious cases reflects our intention to be bolder and more resolute in tackling market abuse.

We also recently made use of our Section 381 power under the FSMA in the market abuse cases of Samuel Kahn and Barnett Alexander. We fined Kahn over £1 million and Alexander agreed to a penalty of £700,000 together with restitution of over £600,000. In both cases we also secured injunctions from the court to prevent them from engaging in further market abuse. Alexander was also banned from working in financial services for five years.

The future

Our strategy in the area of market abuse and insider dealing is a long-term one. We knew it would take time to see the benefits of the approach we adopted in 2007, and particularly in the area of complex criminal prosecutions, we understood there are no 'quick wins'. However, we are now starting to see the results of our work, and we have a pipeline of cases that will continue to provide visible proof of our commitment.

Our aim is for people to realise that if they abuse the markets, there is a realistic prospect of being caught – and if caught, they will face the serious consequences of very significant financial penalties or imprisonment or both. Anecdotal and other indicators suggest that we are making progress towards our ultimate goal: deterring people from committing market abuse and reinforcing the consequences of failing to treat confidential information appropriately.

There have been a number of challenges in getting to this stage. As we continue to investigate increasingly complex cases, often with cross-border elements – whether in terms of money flows, location of suspects or the trading – these challenges will continue.

We are, however, confident that we are well equipped to tackle these and our focus on this will remain as we move from the FSA to the FCA. We expect to continue to tackle these cases with the same vigour and commitment to achieve our aim of clean, fair and orderly markets.

3

The City of London Police – a local force with a global remit

Adrian Leppard, Commissioner The City of London Police

The City of London Police is at the heart of the fight against fraud, with our responsibilities in combating financial crime stretching way beyond the normal confines of policing. The force continues to bring some of the UK's biggest fraudsters to justice and now, under an evolving and expanding remit, we are hosting and operating one of the most advanced police analytical systems in the world, along with a Centre of Excellence that is raising the bar in fraud investigation, detection and prevention.

Beyond the Square Mile

A quick check of the force's contact book would reveal partnerships running from the City to Westminster, from the financial industry through to the charity sector, and with law enforcement across the UK and around the world. And in a time of shrinking budgets we are paving the way for private sector investment in policing that could transform the way in which this country funds and investigates economic crime.

The Square Mile was once the only beat for the City of London Police, but these boundaries have now disappeared, leaving a bigger and bolder law enforcement operation to combat what has become a £38 billion problem for the UK.

In this brave new world, the force's Economic Crime Directorate (ECD) is taking on an increasingly diverse range of cases, from mortgage fraud to multinational money laundering, through to the advanced cyber tools being used to facilitate internet spread-betting.

In addition, globalisation has introduced new and emerging crime trends that the force can only address by working in alliance with its partner agencies, most notably the Serious Fraud Office (SFO). These relationships are the sources of the specialist knowledge and investigative capabilities needed to prevent, disrupt and detect economic crime and reduce its impact on the UK economy and its citizens. The fundamental question now for government, law enforcement and, increasingly, the private sector is what sort of economic crime capability does this country want and what can it afford?

A new agenda

Police funding will be reduced over the next four years by up to 20 per cent and there is a significant risk that the already fragmented police response to

fraud will be eroded further. The City of London Police is the national lead force for economic crime and has identified fraud as a priority area. However, the heads of economic crime in most police forces will soon have to cope with reduced resources as they seek to deal with a growing criminal threat.

To compensate for this shortfall, the City of London Police is working on plans to create a national economic crime capability, funded by police forces with, potentially, support from the private sector. Some elements are already in place, with the force working with the Home Office to agree a national reporting framework for fraud. Others aspects are still a work in progress, but the current indicators point towards a private sector more willing to offer the financial support that will guarantee a high level of policing in the field of economic crime.

The way we were and the way we are

Before looking at how the City of London Police's fraud operation has been transformed in recent years, it is first necessary to understand what has stayed the same.

Our ECD continues to operate, with five fraud squads in place to investigate 'traditional' fraud offences in areas including banking, insurance, investment, insider dealing and advance fees. The teams also work on SFO and Financial Services Authority (FSA) cases, providing advice on policing matters and, where appropriate, training on arrests, interviewing and the execution of search warrants. The ECD also contains four units focusing on specific aspects of financial crime: cheques and credit cards, money laundering, overseas anti-corruption and asset recovery.

But while this structure remains the same, the scale of the crimes it handles has grown exponentially. Together, these units are now investigating more than £5 billion worth of fraud – about £3.5 billion stolen and £1.5 billion in attempted thefts. Across 2010-11 the ECD encountered a 100 per cent increase in recorded fraud crime, and maintained a detection rate of 83 per cent. At the same time we restrained £21 million worth of assets, with £2 million handed back to victims of fraud.

This dramatic increase in workload reveals the growing threat posed by fraud but also our commitment to confronting the problem as well as the continued financial support of the City of London Corporation. It also fits into a much wider picture of intelligence gathering, training and partnership building.

A new dawn

The Government's 2006 'Fraud Review', conducted to measure the impact and prevalence of fraudulent activity within the UK, changed everything for the City of London Police. The findings recognised that attempts to tackle fraud were being undermined by the lack of a joined-up approach to reporting, recording and analysing financial crime. The response was the implementation of a new three-pronged national approach to tackling fraud:

- the setting up of an umbrella government organisation to oversee the tackling of fraud
- establishing a lead force on fraud investigation to provide education, expertise and advice to both police forces and industry nationwide
- setting up instruments to report, collate and prevent fraud activity.

The practicalities of this approach meant that the City of London Police become the national lead force for fraud in 2008. The National Fraud Authority (NFA) was set up in 2009, the Action Fraud reporting centre launched in 2009 and the National Fraud Intelligence Bureau (NFIB) came into being in June 2010. All are still in operation, with government funding confirmed for at least the next two years. Collectively, they have already made a significant impact on the fraud landscape.

A national lead force and the Centre of Excellence

After becoming the national lead force for fraud, the City of London Police started taking on

investigations involving multiple law enforcement agencies at home and abroad. Between the inception of the force and July 2011, 216 cases had been taken on and, in conducting those investigations, partnership working had gone from preferable to necessary. Evidence of this can be seen in the long list of police forces, counter-fraud agencies and public and private sector bodies that the force has engaged with while acting under its new remit.

At the same time, the Centre of Excellence was set up to enhance the professionalism and capabilities of fraud investigators in UK police forces and law enforcement agencies and within the wider financial community. Located within the ECD, it delivers training, accreditation and professional legislation, and prioritises fraud prevention and disruption. The focus of the Centre's work is driven by the strategic priorities for the national lead force and the NFIB, namely: money laundering, organised crime groups, payment card fraud, professional enablers, share purchase fraud, and technology-enabled crime.

The National Fraud Intelligence Bureau

The NFIB is the most advanced police analytical system in the world, driven by public and private sector partnerships and designed to collect and review millions of previously unconnected reports of fraud to find patterns in offending. This intelligence is used as the catalyst for fraud investigations, both at the City of London Police and at forces around the country. The data is also the source of fraud alerts circulated to public and private sector partners and, through the media, to the general public.

Over the next year, all reports of fraud, from large multi-jurisdictional cases to small, local-level crime, will first be sent to the NFIB for assessment and dissemination. This information will be set alongside the streams of data that are continually being made available by new partners.

A key function of the NFIB – providing public protection and facilitating police action – is delivered in tandem with Action Fraud, the national centre at which individual victims can report fraud, either online or over the phone, or receive advice. The victim is given a crime reference number and the report is transferred overnight to the NFIB, where it is analysed to decide if immediate police action is required.

In April the City of London Police became the first UK force to refer victims of fraud to the national reporting centre. As long as the person is not vulnerable, there are no known suspects and there is not a need for immediate police action, he or she can be advised to report the crime to Action Fraud. This should save many hours of staff time recording fraud.

Feeding the NFIB

For the NFIB to function and thrive requires different organisations to continue to provide and share different types of data for analysis. Current providers include CIFAS (the fraud prevention service), UK Payments Administration, the NHS Counter Fraud Agency, the Insurance Fraud Bureau and Vodafone. Alongside this, the NFIB has seconded partner organisations into the bureau to work with each other. These secondments include the Serious Organised Crime Agency (SOCA), the Solicitors Regulation Authority (SRA), the NFA, FSA and SFO – and international colleagues from Immigration and Customs Enforcement (ICE). Along with improving knowledge of fraud issues and improving how organisations can work together, this arrangement has directly led to operational benefits for a number of major investigations.

Friends at home and abroad

The City of London Police's success in tackling complex multi-jurisdictional cases is in part due to the well-established relationships that officers have developed over time with key counter-fraud agencies, government departments and businesses both domestically and internationally. This is further facilitated by the unique demographics of its beat, hosting the world's leading business and financial centre with over 450 international banks

and 300,000 daily workers. Relationships born in the City travel with the detectives, who in the past 12 months have conducted joint operations with the SFO, FSA and SOCA, and worked with police forces across the regions.

The nature of fraud means an increasing number of investigations are cross-border and involve law enforcement from abroad. In particular, the force has worked extensively with the Spanish authorities to combat 'boiler room' fraud, a crime committed outside the UK that targets some of the most vulnerable people inside the UK. In May 2011, ECD officers were on hand to assist Spanish police with the arrest of 15 UK citizens suspected of being involved in a criminal operation believed to be orchestrating a number of large boiler rooms. In March 2011, a joint investigation with US authorities led to a UK citizen pleading guilty to an £80 million boiler room fraud operating out of Spain that accounted for more than 2,300 victims.

The new reality is that continuous advances in technology are making it easier for criminal gangs to operate from multiple locations and move money to accounts all over the world. An example of this is recent evidence of boiler rooms starting to appear in the Far East. The challenge for the force is to use established international partnerships to maintain the pressure on known criminal hotspots, while using new alliances to identify and tackle new threats in new locations.

Public sector partnerships

Of the estimated £38 billion worth of fraud in 2010, £21 billion was believed to have occurred in the public sector. As part of the drive to tackle this problem, the City of London Police is focusing on increasing the engagement between the NFIB and key organisations such as the Department for Work and Pensions and HM Revenue & Customs. It is currently leading initiatives to improve the analysis, provision and dissemination of intelligence on public sector fraud.

The City of London Police is also at the forefront of a development project to prevent a single fraud from affecting several government departments. A pilot has been launched with the objective of delivering a system of fraud alerts to different departments, with the NFIB being used as a central hub of intelligence.

Private sector partnerships funding a new policing

It is important to recognise how the financial sector is already making a contribution to tackling financial crime. The best example of this is the Dedicated Cheque and Plastic Crime Unit, which was set up in partnership with UK Payments Administration and the British Bankers' Association in 2002 and in eight years has saved the industry up to £370 million. City of London Police and Metropolitan Police officers work with case support staff provided by the banking industry to identify and disrupt the organised crime groups who are behind much of this crime.

In July 2011 the insurance industry followed suit and agreed to fund its own specialist police unit to tackle insurance fraud – a crime valued at £2 billion per year. The unit, located in the ECD, will consist of 35 specialist fraud detectives and police support staff and will provide a dedicated response to threats posed to the insurance industry by both organised gangs and opportunist fraudsters.

Members of the Association of British Insurers (ABI) will fund the unit for three years, and a strategic board containing representatives from the City of London Police, ABI, NFA and the Insurance Fraud Bureau (IFB) will set priorities informed by an annual threat assessment and analysis of insurance fraud trends.

The City of London Police is also working closely with the NFA and partners from industry on developing a unit to tackle mortgage fraud, particularly concentrating on the problem of professional enablers. The attacks on lenders can involve many instances of fraud spread across the country, making it difficult to identify connections between the crimes and to get a single force to take the lead in investigating. This also affects the speed of the response and therefore the losses

incurred. With losses to the industry estimated at £1 billion, the new unit cannot come soon enough.

What will tomorrow bring?

The political and economic climate means no one in the counter-fraud community should be resting on their laurels. The City of London Police's capability in fighting economic crime has improved dramatically in the space of a few years, in which time the future of the national lead force and the NFIB has been secured.

But with new criminal threats continuing to emerge and a National Crime Agency on the horizon, we cannot take a step back or sideways. As a force, we need to be leading the reform of the national policing response to fraud to ensure that our capability in combating economic crime continues to evolve.

Closer to home, we must consolidate the NFIB as the UK's intelligence hub for all economic crime and develop the Centre of Excellence into a national and international academy that will set new standards for training. This is all achievable, but to be realised will require even closer alliances with old friends and new projects forged with new friends from around the world. The nature of the threat we face demands nothing less.

BETTER POLICIES FOR BETTER LIVES

OECD work on exchange of tax information

Global Forum on Transparency and Exchange of Information for Tax Purposes: Peer Reviews

The Global Forum is a multilateral framework within which work in the area of tax transparency is carried out and information is exchanged among its member jurisdictions. It is charged with in-depth monitoring and peer review of the implementation standards of transparency and exchange of information.

Global Forum publishes peer reviews assessing countries' performance

Andorra 2011, Phase 1
Anguilla 2011, Phase 1
Antigua and Barbuda 2011, Phase 1
Aruba 2011, Phase 1
Australia 2011, Phases 1 & 2
Austria 2011, Phase 1
Bahamas 2011, Phase 1
Bahrain 2011, Phase 1
Barbados 2011, Phase 1
Belgium 2011, Phase 1
Bermuda 2010, Phase 1
Botswana 2010, Phase 1
British Virgin Islands 2011, Phase 1
Canada 2011, Phases 1 & 2
Cayman Islands 2010, Phase 1
Curaçao 2011, Phase 1
Denmark 2011, Phases 1 & 2
Estonia 2011, Phase 1
Former Tugoslav Rep. of Macedonia 2011, Phase 1
France 2011, Phases 1 & 2
Germany 2011, Phases 1 & 2
Ghana 2011, Phase 1
Guernsey 2011, Phase 1
Hungary 2011, Phase 1
India 2010, Phase 1
Ireland 2011, Phases 1 & 2
Isle of Man 2011, Phases 1 & 2
Italy 2011, Phases 1 & 2
Jamaica 2010, Phase 1
Jersey 2011, Phase 1
Liechtenstein 2011, Phase 1
Luxembourg 2011, Phase 1
Mauritius 2011, Phases 1 & 2
Monaco 2010, Phase 1
New Zealand 2011, Phases 1 & 2
Norway 2011, Phases 1 & 2
Panama 2010, Phase 1
Philippines 2011, Phase 1
Qatar 2010, Phase 1
San Marino 2011, Phase 1
Saint Kitts and Nevis 2011, Phase 1
Singapore 2011, Phase 1
Switzerland 2011, Phase 1
Trinidad and Tobago 2011, Phase 1
Turks and Caicos Islands 2011, Phase 1
United Kingdom 2011, Phases 1 & 2
United States 2011, Phases 1 & 2

Find out more at **www.oecd.org/tax/transparency**

All titles can be purchased at **www.oecd.org/bookshop** and are also available at **www.oecd-ilibrary.org**

OECD

4

Inter-agency and international co-operation in the fight against financial crime

Brian McAuley, Policy Adviser
The Organisation for Economic Co-operation and Development

Money laundering, corruption, terrorist financing, tax crimes and other financial crimes can threaten the strategic, political and economic interests of both developed and developing countries. The common factor in these types of crime is that they all thrive in a climate of secrecy, inadequate legal frameworks, lax regulation, poor enforcement and weak inter-agency co-operation. Countering these activities, therefore, requires greater transparency and improved efforts to harness the capacity of different government agencies to work together to deter, detect and prosecute these crimes.

The OECD has consistently promoted the benefits of globalisation for citizens around the world. But in a global economy with integrated financial markets, new opportunities have opened up for all forms of illicit activity. Fighting this is a shared concern of developed and developing countries, and the risks attached to these flows can only be dealt with effectively by improving international co-operation and removing the bureaucratic obstacles between the different parts of government that deal with money laundering, terrorist financing, bribery and tax evasion.

Oslo dialogue

The link between tax crimes and other financial crimes is increasingly recognised. There are substantial similarities between the techniques used to launder the proceeds of crimes and to evade taxes. Greater transparency and enhanced co-operation between different government agencies are the key ingredients in countering these criminal activities. For these reasons, the OECD launched a platform to fight financial crime at a conference on tax and crime held in Oslo in March 2011.

The event was the first of its kind, bringing together governments from developed and developing countries, non-governmental organisations (NGOs) and business. Participants expressed a strong interest in collaborating further on this issue, and agreed to continue the 'Oslo dialogue' with a view to improving inter-agency co-operation in fighting financial crime and illicit flows at all levels.

The OECD has set the standards on tax measures to combat bribery, and on greater co-operation and better information sharing between the different government agencies involved in the fight against financial crime both domestically and internationally. Two OECD Recommendations to governments

contain the detail: the 2009 Recommendation on Tax Measures for Further Combating Bribery of Foreign Public Officials in International Business Transactions, and the 2010 Recommendation to Facilitate Co-operation between Tax Authorities and Other Law Enforcement Authorities to Combat Serious Crimes.

An example of how all this works in practice is the Australian cross-agency taskforce Project Wickenby, which also co-operates with international partners. Set up in 2006, it has already recovered well over A$500 million (US$535 million) and secured a number of convictions, setting a strong deterrent in the process.

Civil society and business can also play an important role in the fight against financial crime through heightened alertness and contributing to improved systems.

Tax administrations as a means to fight corruption

Countries have put in place, and are reinforcing, a range of tax-related measures to strengthen both the legal framework and practical administrative efforts to counter corruption. The combined effect of these measures is increased deterrence, detection and prosecution of corrupt activities.

On the policy side, countries have explicitly prohibited tax deductions for bribes to foreign public officials, as required by the OECD 2009 Recommendation.

Such legislation raises the overall level of awareness within the business community of the illegality of bribery and increases the cost of doing so. It also highlights the need for tax administrations, during their audits, to seek to detect any deductions for payments of bribes, and to report suspicious payments to the appropriate domestic law-enforcement authorities for possible prosecution of bribery.

Policymakers have recognised that sharing tax information with domestic law enforcers can improve the detection and punishment of serious crimes like corruption. On the international side, more and more tax treaties allow information provided by a treaty partner for tax purposes to be used to combat serious crimes if certain conditions are met.

Tax administrations are now stepping up their training of tax examiners to identify the types of payment that constitute bribes and the action to take when their suspicions are aroused. Such training is usually based on the *OECD Bribery Awareness Handbook for Tax Examiners*, which includes practical tips such as indicators of bribery, interviewing techniques and examples of bribes identified in tax audits.

Tax crime and money laundering

In a recent international survey, anti-money laundering experts identified tax crime as one of the top three sources of dirty money that criminals seek to hide in the financial system. Tax administrations can therefore play an important role in detecting and deterring money laundering, and at the same time tackle tax crimes.

Criminals accumulate significant sums of money by committing crimes such as drug trafficking, human trafficking, theft, investment fraud, extortion, corruption, embezzlement and tax fraud. Money laundering is a serious threat to the legal economy and affects the integrity of financial institutions. It also changes the economic power in certain sectors. If left unchecked, it can corrupt society as a whole.

In the majority of countries, tax crime is a predicate offence for money laundering. In May 1998 the finance ministers of the G7 encouraged international action to enhance the capacity of anti-money laundering systems to deal effectively with tax-related crimes.

In July 2009, the G8 leaders called for further efforts in combating illicit financing, and acknowledged the progress being made by the Financial Action Task Force (FATF), the inter-governmental body, in improving the standards for combating money laundering and the financing of terrorism, and by the OECD on international standards of transparency. The OECD's Committee on Fiscal Affairs, working with FATF,

has developed some new tools to help improve co-operation between tax and anti-money laundering authorities.

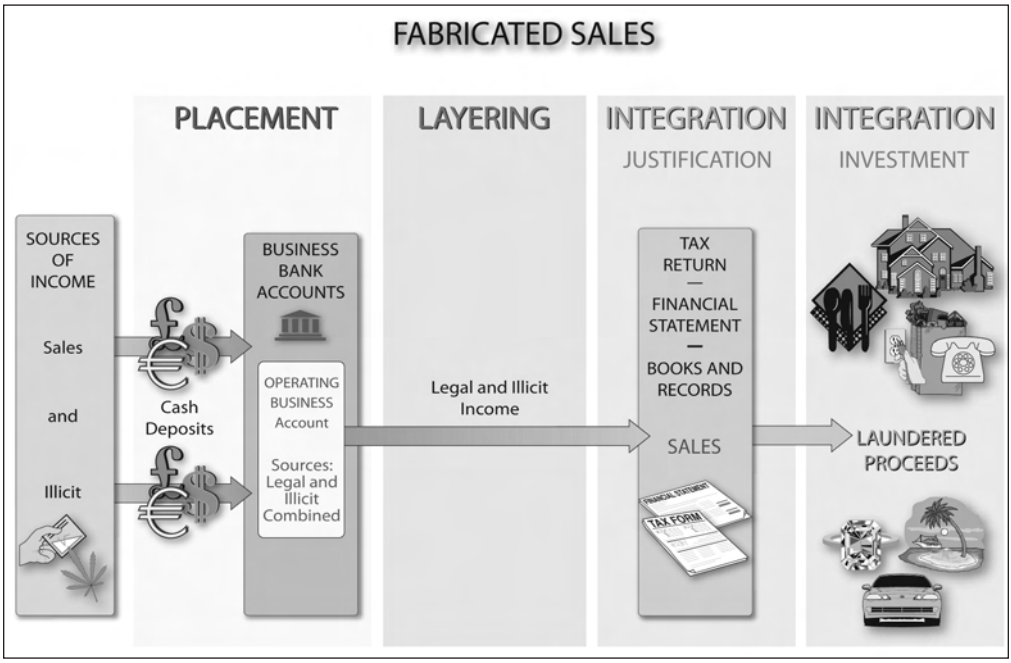
In the past 20 years, crimefighters have sought to deter criminals by paying more attention to the confiscation of proceeds of crime. More recently, with the regulated sector reporting unusual or suspicious transactions, it is often the flow of money or goods that is investigated even before a criminal offence has been detected. If criminals are arrested or taxed on the proceeds of crime, they will try to avoid having the proceeds traced back to their origin and confiscated.

In order to be able to spend money openly, criminals will seek to ensure that there is no direct link between the proceeds of crime and the actual illegal activities. They may also seek to construct a plausible explanation for the origin of the money, and thus seek to 'launder' their proceeds of crime before spending or investing it in the legal economy.

'Money Laundering Awareness Handbook'

Tax administration staff need to be aware of the nature of money laundering and how they may recognise the indicators that point to a need for further investigation. The OECD has produced the *Money Laundering Awareness Handbook*, which provides guidance in identifying money laundering during the conduct of normal tax audits. It is now available in a range of languages.

Tax administrations can adapt the handbook to suit their particular circumstances, taking account of the varying roles they have in relation to reporting unusual or suspicious transactions, receiving such reports and investigating money laundering offences. The handbook can help tax administrations and law enforcement authorities to:



- identify tax crimes
- identify other crimes and criminals
- locate and confiscate criminal assets.

Money laundering methods

The traditional methods of money laundering have centred on the use of cash-based businesses and this remains an important area. However, criminals will continue to seek out innovative methods to exploit weaknesses in financial systems and to try to keep ahead of the investigators. Real estate, loans, international trade and professional service providers (lawyers, accountants and others) are now preferred vehicles for criminals in laundering the proceeds of crime and tax fraud. The handbook contains graphic examples of these methods and describes the traces of crime that can be used to detect them.

One area where tax auditors can apply their expertise is in detecting money laundered through a normal business. A traditional method involves the fabrication of sales. Here the criminal is depositing the illicit funds into the business bank account along with funds from genuine sales. The illicit funds are recorded in the books and records as if the money came from genuine turnover and the overstated income is reported in the tax returns. The company may not have to pay tax on this increased income if the company has trading losses available or where false deductions are also created. The auditor's checks on purchases and sales may reveal the fraudulent activity.

Money laundering through the football sector

In the past two decades, football has changed from a popular pastime into a global industry. The investment of money in the sector has increased exponentially, and some of this has criminal connections. The FATF, with assistance from the OECD, recently completed a study, 'Money Laundering through the Football Sector', to determine what makes the sport attractive to criminals. The report provides case examples identifying the methods used. One case exposed the

diversion of signing-on and other fees to supposed 'image rights' that had been transferred to a company registered in a tax haven. The club conceded that the image rights were in fact part of the employment contract and had to pay an additional tax bill of over £1.3 million (US$2.1 million).

Charity abuse

Another channel for money laundering and tax crimes can be the abuse of charities, either by establishing fake charities or targeting one of the many bona fide organisations. Charities may be perceived as not subject to the kind of tough accounting vigilance afforded to regular businesses. Yet some of them handle vast amounts of money and, just like major corporations, often have to move those finances across borders. As a result, the privileged status of a charitable organisation is sometimes abused, whether by taxpayers, donors or preparers of tax returns.

A 2008 OECD survey identified a range of common methods and schemes used to exploit charities to commit tax crimes and launder money. For instance, a bogus company might pose as a registered charity and solicit contributions, which end up in the pockets of its directors. There are registered charities that sell charity receipts to preparers of tax returns for a commission. Taxpayers and preparers of returns might counterfeit the receipts of real charities. Or terrorists might use charities to raise or transfer funds for their organisations.

Detection is improving, thanks to a combination of intelligence gathering, data matching, and risk profiling and analysis to uncover charity frauds. In-depth audits of a charitable organisation's bookkeeping can also help verify the tax status of the donors. The report suggested that valuable tax information could come from domestic intelligence agencies such as financial intelligence units (FIUs), customs and immigration agencies, or foreign tax authorities. Informants can also provide leads. Many countries have passed Bills to exclude 'remunerated donations', where the 'donor' gets something of value in exchange for their 'donation', while others have made it obligatory to report suspicious transactions to their FIU. Several countries have set up special taskforces and audit teams to combat the abuse.

International seminars

To help tax administrations implement their awareness programmes, the OECD has developed a 'train the trainers' seminar that is being offered in a number of centres around the globe. The seminar also covers bribery awareness for tax auditors. Fifty-seven participants from 22 countries attended the first seminar in Washington DC in June 2010, and they have been rolling out the training in their own tax administrations. Further events are planned for the Latin American, Southern African, Eurasian and Asia Pacific regions.

Conclusion

OECD work in this area continually seeks to reach all countries and to bridge the gaps in organisations. Work continues on examining the methodologies used by criminals, providing advice on detection and prevention, offering opportunities for sharing knowledge and experiences, developing policy recommendations and enabling better inter-agency and international co-operation. The Oslo dialogue will enable the OECD's work to reach a wider audience. Finding synergies and addressing loopholes in regulatory and standard-setting activities remains a priority in the OECD's work.

The mission of the European Anti-Fraud Office (OLAF) is to combat fraud and corruption affecting the budget of the European Union.

To save the taxpayer's money, OLAF investigates in many areas such as:

- illegal perception of grants
- fraudulent public procurement
- embezzlement of aid
- non-payment of import taxes
- contraband cigarettes
- euro counterfeiting

In 5 years, OLAF helped to recover 900 million €uros

OLAF

OFFICE EUROPÉEN DE LUTTE ANTI-FRAUDE

EUROPEAN COMMISSION
EUROPEAN ANTI-FRAUD OFFICE

For more information: http://olaf.europa.eu

5

Fraud prevention by the European Commission: how the lessons from OLAF's administrative investigations are used to stop irregularities and fraud

J Khouw, Head of Unit Fraud Prevention and Intelligence, and
W Kleinegris, Head of Sector Intelligence Direct Expenditures
The European Anti-Fraud Office

The European Anti-Fraud Office (Office Européen de Lutte Anti-Fraude – OLAF) is the service of the European Commission responsible for fighting fraud and other illegal activities against the European Union's budget. OLAF has a hybrid status: it carries out its administrative investigations in full independence from the EU's institutions and member states, but OLAF's policy directorate, which deals with the development of policies and methods to prevent irregularities and fraud, falls under the responsibility of the European Commissioner for taxation, customs, audit and the fight against fraud.

The European Anti-Fraud Office

OLAF was set up as a successor to UCLAF, the directorate in the EC's General Secretariat that co-ordinated the fight against irregularities and fraud. The establishment of OLAF was accelerated as the result of the crisis, amid allegations of fraud and nepotism, that led to the resignation of Jacques Santer's Commission at the beginning of 1999. In the same year, under a decision[1] adopted by the Commission and regulation[2] adopted by the European Parliament and European Council, the Office came into being with the following objectives and tasks:

- to exercise the powers of investigation conferred on the Commission by EU rules and agreements in order to step up the fight against fraud, corruption and any other illegal activity affecting the financial interests of the EU
- to organise and co-ordinate the activities of the member states to protect the financial interests of the EU, and to contribute to the design and development of methods of fighting fraud and any other illegal activity affecting the financial interests of the EU
- to conduct administrative investigations – within the institutions, bodies, offices and agencies established by, or on the basis of, European treaties –

for the purpose of fighting fraud, corruption and any other illegal activity, as well as investigating serious matters relating to the discharge of professional duties.

Before 1999, the Commission already had a certain number of powers to carry out administrative investigations. It was authorised, for example, to perform on-the-spot checks in the member states in order to verify whether economic operators had complied with all their obligations arising from contracts or grant agreements concluded under the programmes and projects that were co-financed under the EU's structural actions or the common agricultural policy. The new element, however, in the regulation adopted in 1999 was the setting up of an Office with powers of investigation that could be carried out with full independence – without interference from member states, EU institutions or the EC's own commissioners.

The protection of the EU's financial interests

This is OLAF's main task, with 'financial interests' covering the revenues, expenditures and assets of the institutions, bodies, offices and agencies set up by EU treaties.

Revenues

For 2011, the total revenues of the EU amount to €126.5 billion (US$178.4 billion). These revenues originate from four different sources:

- customs duties (€16.7 billion, or 13.3 per cent)
- agricultural levies (€123.4 million, 0.1 per cent)
- a percentage of the national VAT levied on goods and services (€13.8 billion, 11 per cent)
- a percentage of the gross national income (€94.5 billion, or 75 per cent).

A further category, 'other revenue' (such as fines imposed on cartels or illicit commercial agreements), accounts for an additional €1.4 billion.

The Office's mandate only covers 'traditional own resources' (TOR – customs duties and agricultural levies), which now account for 13.4 per cent of the EU's revenues.

Expenditures

The EU cannot have a budget deficit: the total amount of payments must equal the total amount of revenues. The EU's budget also identifies 'commitments', referring to interventions that the EU agrees to finance at a later stage. The total amount of commitments approved by the European Parliament and European Council for 2011 amounts to €141.9 billion and is higher than the EU's revenues because the payments can be spread over several years and because the commitments are in practice never fully utilised.

Most of the EU's expenditures relate to interventions carried out under the structural policies and the common agricultural policy under shared or decentralised management, which provides that the implementation tasks for the budget are delegated to the member states or to third countries. These headings account for more than 80 per cent of the EU's budget.

The expenditures for which the EU itself manages the implementation ('direct expenditures') account for less than 20 per cent of the budget. They mostly consist of research expenditure, external assistance to third countries, or pre-accession aid and administrative expenditure.

Direct expenditures are allocated over a vast number of contracts, grant agreements, subsidies, salaries, pensions and administrative outlays that are mostly managed by the Commission or one of the executive agencies.

Assets

OLAF's mandate does not only cover the EU's budget but also its financial interests. The latter include the assets that the EU has acquired over the years – for example, when one of its institutions purchases real estate, office equipment or research facilities. All these assets can be exposed to theft or embezzlement, which varies from the illicit use of office facilities to the theft of

computers, cars or expensive equipment used by the EU's Joint Research Centre.

The Office achieves its objectives and tasks by undertaking the following activities, which are different but closely linked:

- it carries out independent administrative investigations
- it contributes to the design and development of methods of fighting fraud and any other illegal activity.

Administrative investigations

It is the director of the Office who decides on the opening and the closure of investigations. In this capacity, he is fully independent from the Commission, the EU institutions and the member states. He cannot and will not accept instructions to open or close an investigation.

The administrative investigations consist of inspections, checks and other measures to establish the regularity and legality of activities that OLAF has to investigate. An investigation starts with information received by OLAF from internal or external sources.

Internal sources consist, for example, of auditors or Commission officials who have noticed irregularities during the implementation of a contract. External sources tend to be whistleblowers, informants or the media.

Upon receipt, the information is assessed in order to determine whether or not an investigation should be opened. OLAF has a discretionary power in that irregularities for which another body is better placed to investigate are transmitted to that body. For instance, minor wrongdoings by staff are dealt with by the Investigation and Disciplinary Office of the Commission (IDOC). Irregularities for which the estimated financial impact remains below a certain threshold are not investigated (the de minimis rule). Information on issues falling outside OLAF's competence lead to 'non cases' or 'non cases prima facie'.

OLAF's administrative investigations are broken down into external and internal inquiries.

External investigations

These relate to activities or behaviour involving persons and/or entities that are outside the Commission or any of the EU institutions. They examine irregularities or suspected frauds that have occurred during the preparation or implementation of contracts and/or grants agreements awarded by any of the EU institutions, bodies, offices or agencies within the framework of, for example, the EU's external assistance to third countries or its research programmes.

OLAF carries out investigations into irregularities in the performance of research grant agreements where contractors have falsified documents, such as timesheets, with a view to claiming expenditures that have not been made or that cannot be justified. The annual research budget of more than €7 billion is distributed over many beneficiaries and (small) grants, which makes it practically impossible to rule out any irregularities or fraud.

The EU's annual external-assistance budget amounts to more than €10 billion and is largely dedicated to funding infrastructure projects in third countries. Examples of investigations in this area relate to irregularities with the certificates of origin for certain goods; the underperformance or low quality of infrastructure works; bid rigging in procurement; and falsified invoices.

External investigations also take place in the areas of structural actions, agriculture, the EU's own resources revenues, and customs, where OLAF has been successful in uncovering smuggling (cigarettes) and fraud schemes to avoid custom duties (garlic and sugar).

Internal investigations

These relate to serious wrongdoing by staff members of any of the EU institutions, bodies, offices or agencies in violation, especially, of the provisions of the Staff Regulations. These regulations provide, for example, that staff shall act impartially and be objective and loyal, and that they shall not disclose information or accept gifts, payments, favours or decorations. There are several

Table 1

Number of opened and closed cases, clearance rate, per year, 2005-2009

	2005	2006	2007	2008	2009
Opened cases	214	195	210	204	220
Closed cases	233	217	232	187	188
Clearance rate (opened/closed)	0.92	0.90	0.91	1.09	1.17

Source: Annual Report, European Anti-Fraud Office

categories of employees, such as permanent officials, temporary agents, contract staff or seconded staff. OLAF investigates situations, for example, where staff members are suspected of having conflicting interests or of leaking information to third parties in order to help the latter secure contracts at the expense of other competitors.

Some figures on investigations

OLAF opens and closes around 200 internal and external investigations per calendar year (as shown in Table 1). To these must be added the cases that are considered 'non cases' or 'non cases prima facie', where OLAF has no competence to investigate or where it considers that the financial impact of the alleged irregularity does not exceed a minimal threshold. It also considers cases where the allegation can hardly be specified, or where the allegation turns out to be libel or downright nonsense, as non cases.

OLAF also acts as a co-ordinator between national law-enforcement organisations.

Follow-up

Once the Office has closed the investigation stage, it decides on the follow-up to be given to a case. There are several ways it can do this. OLAF can recommend, for example, that undue payments be recovered from the wrongdoer (financial follow-up), but the investigation could also reveal the need to change internal procedures and/or rules in order to address a vulnerability, to which the EU is exposed, that has been uncovered during the investigation (administrative follow-up). The outcome of internal investigations into allegations made against staff who have not complied with their statutory obligations could make it necessary to transmit the file to the disciplinary office of the institution concerned (disciplinary follow-up). And in case the investigation reveals criminal facts, OLAF transmits the findings to the national judicial authorities (judicial follow-up).

The follow-up activities may take a long time, particularly if a case has to be dealt with by the judicial authorities in a member state, in which case OLAF has to monitor a number of procedural requirements under national criminal law, such as prescription periods or provisions in relation to evidence gathering.

The activities of the Office generate revenues to the extent that the financial follow-up allows for the recovery of large amounts of undue payments. In 2009, a total of almost €250 million was recovered. That consisted of around €197 million recovered by the member states within the framework of shared management interventions. Another €43 million came from customs operations and the remainder from undue payments made under the EU's direct expenditures interventions. Table 2 shows the recovered amounts between 2005 and 2009, which largely exceeded OLAF's operating costs in most of the years. More importantly, this is a clear signal that the EU is determined to recover undue payments.

Policy development

OLAF does not only carry out investigations, but "contributes to the design and development of methods of fighting fraud and any other illegal activity affecting the financial interests of the European Community".[3] OLAF is subordinate to

Table 2

Recovered amounts by sector and year, 2005-2009, in € million

Sector	2005	2006	2007	2008	2009	Open amounts
Agriculture	14.2	1.2	0.9	2.0	148.2	23.0
Customs	63.0	0.1	3.3	14.2	43.4	144.9
Direct expenditures	0.2	0.2	0.5	0.5	0.9	0.8
EU institutions and EU bodies	0.0	2.2	0.1	0.2	0.2	1.7
External aid	31.8	3.7	0.9	2.3	7.7	1.5
Structural funds	98.1	17.2	197.7	128.0	49.1	16.9
Total	**207.3**	**24.6**	**203.4**	**147.2**	**249.2**	**188.8**

Source: Annual Report, European Anti-Fraud Office

the Commissioner for this second activity. In other words: it is independent in relation to its operational, investigative activities, but it falls under the political responsibility of the Commission when it comes to policy development and implementation. OLAF bears responsibility for several policy areas, such as the Commission's anti-fraud strategy, fraud prevention and the protection of the euro coins.

The prevention of irregularities and fraud is a responsibility of the Commission services and member states' authorities that are responsible for the financial management of the EU funds. Fraud prevention, detection and reparation (recovery) of irregularities and suspected fraud are essential elements of sound and efficient financial management. OLAF contributes to these activities through three different instruments:

- a 'dynamic approach' to fraud proofing
- raising awareness of fraud
- strategic and tactical intelligence analyses.

At the end of 2007, the Commission adopted a 'Communication': 'Prevention of fraud by building on operational results – a dynamic approach to fraud-proofing'. This approach relies on OLAF's operational experience, which allows for the identification of the specific threats and vulnerabilities to which the EU is exposed. These findings are made available to other Commission departments and to EU institutions and bodies as well as the member states via non-binding recommendations, compendia of common cases and ad hoc instruments. The approach focuses on identifying potential weaknesses in the EU's legislation, implementation instruments, management/control systems, and practices.

In the area of structural fund interventions, OLAF has invested substantially in increasing the awareness among financial managers of irregularities and suspected fraud. These activities have been undertaken in close co-operation with the Commission services responsible for regional policy and employment in the framework of the Joint Fraud Prevention Strategy of the European Regional Development Fund (ERDF), the European Social Fund (ESF) and the Cohesion Fund (for reducing social and economic disparities between member states).

Together with these services, OLAF has implemented an action plan, which addresses issues such as risk assessments and raising fraud awareness. In 2009, for example, it organised

Table 3

Distribution of new information by source and sector per year, 2005-2009

	2005	2006	2007	2008	2009	Total	%
Source							
European Commission	246	251	251	305	305	1,358	30
Freephone	40	26	42	48	58	214	5
Informants	345	398	419	431	456	2,049	46
Member states	119	107	132	147	111	616	14
Other EU institutions	23	20	20	73	33	169	4
Others	29	20	14	25	6	94	2
Total	**802**	**822**	**878**	**1,029**	**969**	**4,500**	**100**

	2005	2006	2007	2008	2009	Total	%
Sector							
Agriculture	100	107	136	201	173	717	18
Cigarettes	9	9	10	13	10	51	1
Customs	60	65	56	54	36	271	4
Direct expenditures	73	50	102	152	109	486	11
EU institutions and bodies	235	232	207	293	305	1,272	31
External aid	168	205	206	179	140	898	14
Structural funds	157	154	161	137	196	805	20
Total	**802**	**822**	**898**	**1,029**	**989**	**4,500**	**100**

Source: Annual Report, European Anti-Fraud Office

seminars for auditors and desk officers within the services responsible for the implementation of structural fund interventions. The Office has the ambition of building an anti-fraud culture among financial actors, including control bodies.

Notifications and risk analyses

An important instrument in this respect is the Irregularities Management System (IMS), a database with information identified by the member states, which have to notify the Commission of any irregularities and fraud cases they discover in the management of interventions in the area of structural actions, as well as the common agricultural policy. The same applies to pre-accession countries that receive financial support from the EU in order to prepare for membership.

When a member state, for example, discovers irregularities in a training programme for the long-term unemployed that is funded by the ESF (one of the structural funds), its competent authorities have the responsibility to take the necessary measures to prevent, detect and repair the irregularities. The member state has to notify OLAF of the type of irregularity, the duration, the amount involved, the modus operandi and the persons involved. This obligation also applies to expenditures made under the other structural funds, such as the ERDF or the Cohesion Fund,

as well as the expenditures made under the financial instruments created under the common agricultural and fisheries policies.

These notifications are processed and analysed by OLAF and they have started to provide a wealth of information on the number of irregularities and suspected fraud cases, along with the typical schemes used by fraudsters and their modus operandi. The results of these analyses are now made available to the Commission's authorising officers, who oversee the shared management interventions in order to strengthen the relevant sector legislation against irregularities, fraud and shortcomings in the EU interventions.

The analysis of OLAF's investigations has generated important findings that feed into the Commission's efforts to boost fraud prevention. These reviews have demonstrated, for example, the importance of external information sources in the opening of investigations: in certain areas, more than half of OLAF's inquiries have been opened on the basis of information originating from sources outside the 'chain of control' (see Table 3), such as internal and external officers or the desk officers in the Commission who carry out verifications.

It is important to note that investigations opened on the basis of external information relate to cases having a substantial financial impact. The analyses of OLAF's operations have revealed that falsification of documents and incorrect declarations are among the most common modus operandi in cases of irregularity and fraud. But the information has also allowed identified shortcomings in the management of the EU-funded interventions.

OLAF has presented these findings to the member states during its annual, bilateral control and co-ordination meetings, within the framework of the Joint Fraud Prevention Strategy. This co-operation between the states and the Commission can generate valuable information for both partners in the effort to fight fraud and improve the implementation and management of structural funds interventions.

OLAF's intelligence activities make use of its own operational experience, the information from the Irregularities Management System, the Commission's financial databases, as well as 'open source' data. The analyses allow a better understanding of the circumstances and conditions under which the EU's financial management is vulnerable to irregularities and suspected fraud. They lead to the identification of 'red flags' and risk indicators for fraud.

Several intelligence analyses have now been carried out and have generated useful findings for recommendations to internal and external stakeholders, such as the Commission's authorising officers and the relevant authorities in member states. Interestingly, some of the findings identified throughout all the areas and analyses have been very similar, such as the most common modus operandi being theft, embezzlement and falsified documents, and the need for a greater knowledge among officials of fraud and fraud schemes.

OLAF's future

OLAF is a small organisation compared with the law-enforcement and investigation bodies in the member states. It employs fewer than 200 investigators. They are supported during their inquiries by a wide range of professionals, such as IT and intelligence specialists, lawyers, and administrative and budget staff, but the headcount at the Office does not exceed 500.

An increase in the number of investigators would certainly contribute to the achievement of OLAF's tasks and objectives, but even if that figure were doubled or tripled, it would remain a relatively small body. It has to be borne in mind that the subsidiarity principle applies to OLAF, which only intervenes where it is able to add value on top of the activities undertaken by similar organisations within the member states. OLAF also provides co-ordination support to the different law-enforcement organisations but is not in a position to investigate all the irregularities and suspected frauds perpetrated against the EU's

revenues, expenditures or assets. This underlines the need to use the lessons that can be drawn from OLAF's operational experience in order to prevent irregularities and fraud from occurring. Preventing fraud is, of course, always better than cure, even if the quantification of the benefits remains a difficult and arbitrary exercise when compared with the quantification of costs.

OLAF's future will also depend on the outcome of certain developments. For example, the European Commission tabled a proposal to amend OLAF's legal base, Regulation 1073/1999, providing for changes to the investigation procedure and the investigative powers of the Office. These changes incorporate the case law of the Court of Justice, whose rulings have had an impact on the way OLAF carries out its investigations. Meanwhile, the Treaty of Lisbon provides for the possibility of creating a European Public Prosecutor. Even though this function will probably not be created at short notice, preparatory activities will have an impact on OLAF's own role and responsibilities.

The Court of Auditors has also indicated a need for OLAF to speed up its investigations and focus on more serious irregularities, while the Commission is working on an anti-fraud strategy that will highlight the need to strengthen its own fraud-prevention and intelligence activities at the level where they have the greatest impact: the financial and authorising officers. These developments will clearly affect the priorities and allocation of resources within the Office itself.

But it must be borne in mind that prevention is part of a cycle that begins with information on suspected irregularities, and is followed by investigation, detection and sanctions, before leading to the prevention activities themselves, which are based on the lessons from OLAF's operational experience and its identification of the EU's most vulnerable areas and sectors of expenditure. The prevention activities provide important input for the improvement of the financial management of new policies and programmes.

All elements in this cycle help to create a sufficient level of deterrence to protect the EU's financial interests. Clearly, both OLAF's investigations and its fraud prevention activities contribute to that mission.

6

Transparency International and the fight against corruption

Chandrashekhar Krishnan, Executive Director Transparency International UK

Corruption hurts in many ways. Transparency International (TI) estimated in 2008 that the cost of attaining the UN Millennium Development Goals relating to water and sanitation was likely to increase by as much as US$48 billion by 2015. Of course, the financial cost is only one dimension of the tragedy. In many parts of the world, corruption and poor governance undermine both democracy and development. The poor are disproportionately hurt – the mother who cannot afford to pay a huge bribe to get medical attention for her dying child; the family who will only be able to have safe drinking water if it pays a bribe; and the unemployed who remain jobless because public works projects are not implemented since corrupt officials have pocketed the funds that were allocated for them.

Unless greater progress is made in reducing corruption and improving governance, it will be that much harder to achieve the UN Millennium Development Goals. For example, research by TI in 42 countries shows that the increased practice of paying bribes is associated with a lower literacy rate among 15- to 24-year-olds.

In the UK, we believe there should be zero tolerance for corruption both at home and in Britain's business dealings with the rest of the world, especially in developing countries. It is crucial that UK companies behave ethically, particularly in high-risk overseas environments, and that they do not become complicit in making the problem of corruption worse. The British financial system should not allow the corrupt to find a safe haven for their illicit wealth in the UK and its overseas dependencies and territories. The UK government must honour its international obligations, particularly under the 1997 OECD Anti-Bribery Convention and the UN Convention against Corruption.

The government's 2011 White Paper on Trade and Investment for Growth quite rightly points out that bribery and corruption are barriers to trade and growth, because they hinder development, distort competition and perpetuate poverty.

The UK currently conducts about a quarter of its foreign trade with developing countries and most of this is with emerging economies where the risk of corruption tends to be greater, as demonstrated by their low scores on TI's Corruption Perceptions Index (see Table 1 over page). It is in the UK's strategic interests to see anti-corruption reforms implemented in these

Table1: TI Corruption Perceptions Index 2010

TOP 40			BOTTOM 40		
Rank	Country/ territory	CPI 2010 score	Rank	Country/ territory	CPI 2010 score
1	Denmark	9.3	134	Sierra Leone	2.4
1	New Zealand	9.3	134	Togo	2.4
1	Singapore	9.3	134	Ukraine	2.4
4	Finland	9.2	134	Zimbabwe	2.4
4	Sweden	9.2	143	Maldives	2.3
6	Canada	8.9	143	Mauritania	2.3
7	Netherlands	8.8	143	Pakistan	2.3
8	Australia	8.7	146	Cameroon	2.2
8	Switzerland	8.7	146	Côte d´Ivoire	2.2
10	Norway	8.6	146	Haiti	2.2
11	Iceland	8.5	146	Iran	2.2
11	Luxembourg	8.5	146	Libya	2.2
13	Hong Kong	8.4	146	Nepal	2.2
14	Ireland	8.0	146	Paraguay	2.2
15	Austria	7.9	146	Yemen	2.2
15	Germany	7.9	154	Cambodia	2.1
17	Barbados	7.8	154	Central African Republic	2.1
17	Japan	7.8	154	Comoros	2.1
19	Qatar	7.7	154	Congo-Brazzaville	2.1
20	UK	7.6	154	Guinea-Bissau	2.1
21	Chile	7.2	154	Kenya	2.1
22	Belgium	7.1	154	Laos	2.1
22	US	7.1	154	Papua New Guinea	2.1
24	Uruguay	6.9	154	Russia	2.1
25	France	6.8	154	Tajikistan	2.1
26	Estonia	6.5	164	Dem Republic of Congo	2.0
27	Slovenia	6.4	164	Guinea	2.0
28	Cyprus	6.3	164	Kyrgyzstan	2.0
28	UAE	6.3	164	Venezuela	2.0
30	Israel	6.1	168	Angola	1.9
30	Spain	6.1	168	Equatorial Guinea	1.9
32	Portugal	6.0	170	Burundi	1.8
33	Botswana	5.8	171	Chad	1.77
33	Puerto Rico	5.8	172	Sudan	1.6
33	Taiwan	5.8	172	Turkmenistan	1.6
36	Bhutan	5.7	172	Uzbekistan	1.6
37	Malta	5.6	175	Iraq	1.5
38	Brunei	5.5	176	Afghanistan	1.4
39	Korea (South)	5.4	176	Myanmar	1.4
39	Mauritius	5.4	178	Somalia	1.1

countries because this will be beneficial to economic growth and trade.

The UK needs to be at the forefront of international efforts to tackle corruption. But it will be accused of hypocrisy if it does not first put its own house in order. Research published by TI-UK in June 2011 ('Corruption in the UK – Overview and Policy Recommendations') suggests that there is a more acute problem in Britain than is currently recognised. There are serious issues in relation to specific institutions and sectors, notably political party funding, parliament, sport and prisons.

A particularly shocking finding is the increasing reach of organised crime in areas, such as prisons, where criminal activity and corruption are inextricably linked. More action is needed by the government to understand and combat these growing threats through a robust, coherent and co-ordinated response. Since there are links between corruption outside and inside the UK, it would be desirable to extend the remit of the government's current overseas 'anti-corruption champion' (the Secretary of State for Justice) to cover corruption within the UK.

The Bribery Act 2010

The effective enforcement of the Bribery Act, which came into force on July 1, 2011, should be a key element of a UK strategy to combat corruption, both overseas and domestically. After a decade of procrastination, the UK has finally become fully compliant with the OECD Anti-Bribery Convention, which requires all its parties to criminalise the bribery of foreign public officials. Prosecutors will have a legal framework for prosecuting bribery that is fit for purpose.

However, there is a danger that implementation of the new law may be weakened because of budgetary cutbacks and uncertainties about the future organisation of the machinery of law enforcement against economic crime. This would be tragic because there has been a significant improvement in the UK's efforts in recent years. TI's 2011 assessment of the OECD Convention's enforcement by 37 countries shows that, for the second successive year, the UK is one of seven countries to be actively enforcing the Convention (see Table 2 over page). It has recorded 17 prosecutions and has 26 ongoing investigations. This is a huge improvement because, in 2007, it had not brought a single prosecution of foreign bribery.

The Bribery Act should send a strong message to British business: it will be used to punish unethical companies that pay bribes to gain an unfair advantage, and it will make it easier for honest UK companies to resist demands for bribes and facilitation payments when operating in high-risk environments. Hopefully, it will also strengthen their hand in requiring their business partners to observe high ethical standards.

The Bribery Act, through its extra-territorial application to foreign companies that have or conduct a part of their business in the UK, ought to help to create a level playing field for companies that are committed to zero tolerance of bribery. However, it is unfortunate that parts of the UK government's guidance to commercial organisations on procedures for preventing bribery, in relation to Section 7 of the Act, have unnecessarily created some uncertainty in this area.

In 2010, TI-UK published 'UK Bribery Act Adequate Procedures – guidance on good practice procedures for corporate anti-bribery programmes'. This is designed to help companies adopt and apply sensible, practical measures consistent with the Act's requirements.

Our guidance is based on the principle that a company's anti-bribery systems are more likely to be regarded as constituting 'adequate procedures' if they are based on good practice rather than an approach that solely uses compliance with laws to determine the structure of the programme.

Zero tolerance of bribery is the best policy

A company's best defence against bribery and corruption is a policy of zero tolerance – especially when operating in high-risk environments. The TI guidance to companies stresses six basic requirements:

Table 2: foreign bribery enforcement in OECD Convention countries

Country	Enforcement[I]				Share of world exports % for 2010[II]	Share of foreign investment % for 2009 (outward)
	Total cases		Investigations under way			
	2010	2009	in 2010	in 2009		
Active enforcement						
Denmark	14[III]	14[III]	1	1	0.8	0.9
Germany	135	117	22	24	8.2	8.4
Italy	18	18	2[IV]	3[IV]	2.9	4.6
Norway	6	6	1	1	0.9	0.6
Switzerland	> 35	30	0[IV]	0	1.6	2.6
United Kingdom	17[V]	10	26	24	3.5	13.3
United States	227	169	106	100	9.8	15.7
Moderate enforcement						
Argentina	2	2	0[IV]	0	0.4	0.1
Belgium	4[VI]	4[VI]	0	0	2.0	2.5
Finland	6	5	3	5	0.5	0.4
France	24	18	5	10	3.5	11.3
Japan	7	7	0[IV]	0	4.5	3.7
Korea (South)	17	17[VII]	0	1	2.9	0.8
Netherlands	9	7	3	0	3.3	1.6
Spain	11	11	0	1	2.0	6.0
Sweden	2[IV]	2[IV]	4	5	1.2	1.9
Little or no enforcement						
Australia	1	1	3	4	1.4	1.2
Austria	0	0	5[IV]	4[IV]	1.1	1.6
Brazil	1	1	8	4	1.3	0.4
Bulgaria	4	3	0	1	0.1	0.1
Canada	2	2	23	1	2.5	2.7
Chile	2	0	2	0	0.4	0.2
Czech Republic	0	0	0	0	0.8	0.2
Estonia	0	0	0	0	0.1	0.1
Greece	0[IV]	0[IV]	0[IV]	0[IV]	0.3	0.3
Hungary	27	27	2	0	0.6	0.2
Ireland	0	0	0[IV]	0[IV]	1.1	1.0
Israel	0	0	0	0	0.4	0.4
Luxembourg	2	-	Some	-	0.5	0.5
Mexico	0	0	0	0	1.7	0.4
New Zealand	1	0	1	2	0.2	0.1
Poland	0	0	0	0	1.0	0.2
Portugal	4	4[VII]	6	0	0.4	0.3
Slovak Republic	0	0	1	1	0.4	0.4
Slovenia	0	0	2	2	0.2	0.1
South Africa	0	0	5	1	0.5	0.2
Turkey	0	0	5	4	0.9	0.1

I. Case numbers are cumulative, starting from Convention entry into force; investigation numbers are those ongoing in the year listed. II. Numbers from the OECD Working Group on Bribery 2010 Annual Report. III. Cases all related to UN oil-for-food programme. Some of these cases may have been brought for sanctions violations. IV. Number unknown or based on media reports. V. Includes 2011 cases. VI. Belgium has brought ten additional cases on behalf of EU institutions. VII. Number corrected from last year's report.

- first, the tone from the top – at the board level – is crucial in establishing zero tolerance of bribery and corruption as the foundation for a company's anti-bribery systems
- second, a proper, thorough assessment of risk is essential. The assessment should be seen as a continuous process because corruption challenges are not static and can change quite quickly
- third, detailed policies and procedures need to be developed and the key areas to cover include: facilitation payments; promotional expenditure and gifts; political and charitable contributions; due diligence on business partners; and operational functions such as contracting and purchasing
- fourth, sufficient resources and high-level attention are needed to ensure proper implementation of policies and procedures. There is no point in developing good policies if mechanisms for implementation are weak
- fifth, due diligence must be applied to business partners. This is particularly important in relation to agents, contractors and suppliers
- finally, companies should monitor and review their anti-bribery systems continually. It also helps to seek external assurance that a company's systems are functioning properly.

Facilitation payments

Companies operating in high-risk environments are often exposed to demands for so-called facilitation payments (FPs), which are banned under UK legislation.

Although the OECD Convention does not require parties to criminalise FPs, a majority of them have done so. Others, like the US, allow them but on the basis of strict conditions. None of the parties give companies carte blanche to make such payments. The OECD's 2009 Anti-Bribery Recommendation calls on governments to control the problem, recognising that the payments are generally illegal in the countries where they are made.

FPs are a form of bribery and TI therefore urges all companies to work towards their complete elimination. There is no dividing line between a facilitation payment and a bribe. The influence of pervasive FPs can be insidious and provides a climate for wider systemic corruption. Such payments can place a heavy burden on the poorest citizens of developing countries.

We recognise the challenges companies face at a practical level. Those that have banned these payments tend to be the large multinational companies that may have a lot of clout. Smaller companies may find it more difficult to resist demands for such bribes. However, despite the practical difficulties, there are good reasons why they should be eliminated. Once a company starts making them, it becomes vulnerable to demands for larger payments. Furthermore, if a company allows FPs, this can be misunderstood by employees or abused by some of them to pay bribes in the guise of FPs.

Companies that have adopted a zero-tolerance approach to FPs have actually found that it is good for their business. They say their employees are not bothered for demands for these payments because it is widely known in the high-risk countries where they operate that their corporate policy is not to pay them.

If enough companies collectively refused to make FPs, and demands for them were publicised and reported to the host government, this would make it difficult for those demands to be sustained. But for that to happen, it will also be vital for UK embassies and high commissions to give UK companies advice and support on the ground. It is good to see that this issue is now receiving more attention from the UK government.

Creating a level playing field

TI is increasingly concerned about the lack of enforcement efforts among other parties to the OECD Convention. Our 2011 annual assessment report (see Table 2) shows that as many as 21 parties are laggards that need to face greater diplomatic pressure from the OECD's secretary-

general and its Working Group on Bribery. We have recommended that the OECD should publish a list of these countries and monitor their enforcement efforts more closely.

Questions have been raised about whether a truly level playing field for bribe-free international business can be created as long as some major players remain outside the OECD Convention. Particular concerns have been expressed about Russia, China and India. Companies from these countries are significant players in global markets.

There have been some positive developments. Russia has decided to accede to the OECD Convention later this year. China and India have introduced legislation that criminalises foreign bribery, and India has finally ratified the United Nations Convention against Corruption. Of course, it would be even better if India and China could also be persuaded to join the OECD Convention, and it remains to be seen how they will actually enforce their new laws against foreign bribery. But we should not underestimate the significance of these developments because they augur well for international diplomatic efforts to level the playing field for bribe-free international business.

United Nations Convention against Corruption (UNCAC)

Companies that are committed to conducting their international business ethically often ask what more can be done to tackle corruption on the 'demand side' in the difficult environments where they operate.

UNCAC, which has been ratified by 152 countries, is very relevant in this context because it is the international community's most comprehensive, legally binding instrument to combat bribery and corruption.

It has provisions that cover prevention, enforcement and international co-operation to prosecute bribery and return financial assets looted by corrupt politicians and officials. It provides the best framework to pursue anti-corruption reforms in countries and will create a more congenial environment for attracting foreign direct investment, enabling companies to conduct business without pressure to pay bribes.

In 2009, the parties to the UN Convention agreed the outline of a mechanism to review its implementation. Since the agreement of more than 100 countries was required, what emerged was perhaps not as robust as TI and other organisations would have wanted. However, we now have a framework to press for anti-corruption reforms in countries where governance is weak, public institutions are fragile and corruption levels are high. And over time, we hope it will be possible to strengthen the review mechanism. For this purpose, TI and several other non-governmental organisations (NGOs) have formed a coalition that is pressing for changes, especially to ensure transparency in the monitoring and review process.

While legally binding international instruments like the UN and OECD Conventions are crucial, we should not ignore the important role of non-binding international initiatives in promoting transparency and anti-corruption reforms.

Extractive Industries Transparency Initiative (EITI)

A good example of voluntary international initiatives is the EITI, which aims to improve transparency in the payment and reporting of revenues in extractive industries, notably oil, gas and mining. The basic underlying principle is that if citizens in certain countries – those that are rich in natural resources but socio-economically poor because of corruption and economic mismanagement – had access to accurate information about government revenues from extractive industries, they could demand greater accountability. This would help to promote more productive uses of those revenues for the wider public good.

Since it was launched in 2002, the EITI has grown into a unique coalition among

governments, companies, civil society and international organisations. Under the initiative, which is independently audited with oversight by country multi-stakeholder groups, companies disclose their payments of tax and royalties, and governments disclose their corresponding receipts. Currently, there are 24 so-called 'candidate countries', whose governments have, in the view of the EITI's International Board, committed to implementing its principles and meeting five 'sign up' indicators. Ten countries are deemed by the board to be compliant with the EITI 'standard'.

More than 50 of the world's largest oil, gas and mining companies, and 80 institutional investors (managing over US$16 trillion), support the EITI. And about 300 NGOs worldwide – represented by the Publish What You Pay (PWYP) coalition, of which TI was a founder member – are involved in the implementation of the initiative, internationally and nationally.

A TI project to promote revenue transparency in the oil and gas sector is helping to reinforce the EITI. TI's 2011 report on the oil and gas industry rates 44 companies on the public availability of information on their anti-corruption programmes and how they report their financial results in all the countries where they operate. The companies evaluated represent 60 per cent of global oil and gas production.

Legislation for revenue transparency

The EITI will also be strengthened by a provision in a new US law passed in July 2010 that is expected to have a huge impact in terms of promoting transparency. Under the Cardin-Lugar provision in the US Financial Reform Act, oil, gas and mining companies that report to the Securities and Exchange Commission will be required to publish payments to foreign governments on a country-by-country and project-by-project basis.

It would be good to see measures equivalent to the Cardin-Lugar provision enacted in the UK, as well as other major financial centres where extractive companies are listed. It is important to have a level playing field and this could be achieved through co-ordinated action at the level of the EU and the G20. The PWYP coalition is actively campaigning for this, and we have seen some encouraging indications of growing support among key EU members like the UK, Germany and France.

Tackling illicit financial flows

The UK and other major financial centres need to strengthen their defences against money laundering since the ability to launder the proceeds of corruption facilitates the commission of bribery as well as terrorism and other criminal activities.

It has been estimated by the World Bank that corrupt leaders of poor countries steal as much as US$40 billion each year and stash these looted funds overseas. UK financial institutions have been used as repositories for stolen funds from several countries. Money launderers find it easier to mingle their dirty funds in a large financial centre like London.

Worldwide, the poorest people in the poorest countries are the main victims of bribery and corruption. When leaders in these countries are able, with impunity, to loot public financial resources and launder this illicit wealth in the financial centres of developed countries like the UK, the poor suffer even more. Instead of funding health, education, clean water and sanitation, corrupt kleptocrats lead obscene, extravagant lifestyles.

The UK's defences against money laundering should be sufficiently robust to prevent corrupt money from finding a safe haven. If those defences are breached, the UK must co-operate promptly to enable stolen assets to be repatriated to victim countries.

An assessment by TI-UK of the UK's anti-money laundering regime ('Combating Money Laundering and Recovering Looted Gains – Raising the UK's Game', June 2009) showed that although considerable improvements have

been made in recent years, there is a particular need to:

- strengthen regulatory capacity in vulnerable UK overseas territories
- enhance due diligence on politically exposed persons
- make transparent the beneficiaries of trusts
- improve the regulation of trust and company service providers.

Conclusion

The fight against corruption has to be waged on several fronts. Civil society, governments and companies can work together to change policies, attitudes and values in ways that will help to tackle corruption effectively at the national and global levels. We need more international trade and economic growth but within an ethical framework based on transparency, accountability and integrity. Most UK companies want to conduct their business in an ethical manner and will actually benefit from a strong stance against bribery.

If the UK enforces the Bribery Act and its other laws against serious economic crime effectively, it will be in a far stronger position to encourage other countries, particularly emerging economies, to raise their standards. And as anti-corruption standards improve over time in a larger number of countries, we are bound to see positive impacts on growth, development and the reduction of poverty.

Transparency International (TI) is the world's leading non-governmental anti-corruption organisation. With more than 90 Chapters worldwide, TI has extensive global expertise and understanding of corruption.

Transparency International UK (TI-UK) is the UK chapter of TI. We raise awareness about corruption; advocate legal and regulatory reform at national and international levels; design practical tools for institutions, individuals and companies wishing to combat corruption; and act as a leading centre of anti-corruption expertise in the UK.

www.transparency.org.uk

World Bank Integrity Vice Presidency

Integrity for Better Results

The World Bank Group is committed to ensuring its projects are of highest integrity

Please report concerns of fraud and corruption to:

Call 1-800-831-0463 inside the US
Call 1-704-556-7046 outside the US

Operated by an independent third party Open 24 hours a day Interpreters available Anonymous calls accepted
Or email: investigations_hotline@worldbank.org

For companies interested in INT's Voluntary Disclosure Program contact: phaynes@worldbank.org

For more information, please visit www.worldbank.org/integrity

7

The reality of fighting global corruption: a World Bank perspective

Leonard Frank McCarthy, Vice President, Integrity World Bank Group

Taking aim at corrupt influence, revolutions across the Middle East and North Africa (MENA) and elsewhere have become a self-fulfilling prophecy. The demand for integrity and enforcement around the world is clear evidence that economic and social progress can stumble in the face of corruption despite the best intentions of the international development community.

In many countries, the global public has begun to demonstrate immense energy and increasingly low tolerance of corruption by governments and the private sector. Major corporations are taking note of a new international force that is spreading across countries in Africa, the Middle East, Asia, Europe, and North and Latin America. The encouraging reality is that many of these companies are currently refining their checks and balances, to ensure that their integrity in the public eye is unquestionable. It matters for their profits and share in global markets, including the development market and the international private sector.

Meeting public demand for integrity: a daunting reality

Governments, on the other hand, face a different challenge in the new reality of public demand for integrity, as it features today on their economic, social and political horizons. Those authorities that paid little or no attention to their integrity score in the public eye can no longer afford to do so. Empowered by advancing information technology with unprecedented global reach, a growing body of interconnected young people and a flourishing media, today's world is demanding accountability in ways that challenge governments every day.

At a meeting convened by the World Bank in December 2010, members of the International Corruption Hunters Alliance confirmed that in their – once-restricted – world, information sources and co-operation avenues were now opening up that were never part of their tradition as crimefighters. Civil society organisations have made a significant investment in the past few years in drawing upon public frustration and the need for a stronger accountability standard that can be used anywhere and be applied in any context.

At the World Bank, our engagement with civil society leaders in different parts of the world has been very valuable in connecting us with the reality on the ground, and the dire need for accountability and transparency in

Bank-financed projects. We have launched a number of transparency initiatives, including Access to Information Policy and Open Data, which put free information on projects, and all the knowledge that Bank teams generate, at the disposal of a global public – to improve accountability to the public.

This, however, is not the end of the story. As an international development institution, we also recognise that societies, governments, national companies and small enterprises need to be able to grow and compete on an equal footing – and to take account of the circumstances of the poor and vulnerable. Economists and social scientists at the World Bank will argue that fighting corruption is a cornerstone in driving growth and human resource development, creating jobs and securing a level playing field for private sector development, particularly in emerging and transitional economies.

A mission to deliver results

For corruption fighters in the international development arena, the World Bank's global positioning and regional reach offer an array of opportunities that must not be passed up. In every part of the world where we operate, there is a clear picture of what the stakes are and a less clear picture of what it takes to fight corruption. International investigators can face some complex and high-risk challenges on the ground, yet it is our mission to deliver the types of result that set back the cause and course of corruption.

As part of the World Bank's overall governance and anti-corruption strategy, the Integrity Vice Presidency (INT) investigates allegations of fraud and corruption in Bank-financed activities. Where Bank staff may also be involved, we act.

Beyond investigations, we make a rigorous effort to analyse what we do right and to share that knowledge with colleagues in operations and state authorities. This is why the Bank has invested in new Preventive and Forensic Services Units, as part of our integrity agenda. We refer our investigative findings to governments and other institutions, so that they can pursue prosecutions or take other action. In 2010, for the first time ever, we included a list of all our referrals in our department's annual report, with the objective that it would bring greater pressure to follow up on these referrals.

Since 2008, the World Bank has concluded 553 external and internal investigations, and generated close to 200 combined sanctions applications and debarments, to deter wrongdoing and protect public funds. Most of INT's investigative findings in 150 substantiated cases have been referred to the relevant authorities to take charge of affairs in their own countries and institutions.

INT defines integrity results in terms of the deterrent effect of investigations, delinquent companies interdicted, the impact of preventive precautions and forensic audits, and effective legal actions taken by national authorities. And it defines progress in terms of the co-operation underlying the success of its investigations, the lowering of governance risk, and international coherence in the anti-corruption arena.

Debarment, voluntary disclosure and compliance monitoring: integrity in action

The World Bank's early response to the financial crisis, which translated into a US$72 billion lending portfolio to reduce poverty and assist growth in countries that suffered in the crisis, has increased the potential for private sector companies to engage in Bank-financed projects. With that, the Bank has also been charting new territory in its fight against corruption.

Since 1999, the World Bank Group (WBG) has been using debarment both to protect its funds and as a way of holding fraudulent or corrupt firms accountable for their misconduct. Publicising the debarments deters potentially wayward businesses from participating in Bank-financed projects, increasing the likelihood of fair competition among bidders and protecting the misuse of development resources. In 2009, the WBG began using negotiated resolutions as a means of resolving cases fairly and equitably,

removing corrupt firms from projects and encouraging others to acknowledge their misconduct sooner.

Brought to book

One of the early milestones for the World Bank's integrity agenda was the 'Siemens settlement' in 2009. Following an agreement to pay more than US$1.3 billion in the US and Germany after being charged with accounting offences, the German manufacturer reached a comprehensive settlement with the World Bank. This included a commitment to pay US$100 million to support governance interventions in developing countries, a debarment of the company's Russian subsidiary for four years and a voluntary two-year shutout on bidding for Bank business.

In April 2010, the WBG debarred UK publisher Macmillan for six years. The debarment was part of a negotiated resolution that followed Macmillan's admission that it had paid bribes in an attempt to win a multimillion-dollar contract in an education project in Southern Sudan.

Macmillan had been a major supplier of educational materials for WBG-financed projects, winning more than US$35 million in contracts since 1999. Acting upon information it had received, an INT investigation uncovered evidence that Macmillan made a series of questionable payments in an effort to influence the procurement process – and ultimately the company was not awarded the contract. Underscoring the Bank's commitment to working closely with governments to pursue corruption, INT collaborated with national authorities in the Macmillan investigation, which accelerated the resolution of the case.

Under the terms of the agreement, Macmillan agreed to co-operate with the World Bank efforts to combat fraud and corruption in WBG-financed projects. The company also agreed to implement a compliance programme that will be monitored by a third party to ensure its adequacy. In recognition of Macmillan's early acknowledgement of its wrongdoing, the WBG agreed to a six-year debarment – a reduced term.

In December 2010, the World Bank debarred the Italian company Lotti in the wake of the company's acknowledged misconduct in a Bank-financed public works project in the water sector in Indonesia. Under the negotiated resolution, the company committed to pay US$350,000 in restitution to Indonesia – an innovative settlement marking the first time that the World Bank had included restitution payment in resolving an investigation into fraud. The US$350,000 represented the unjustified payments received by Lotti and its partners as a result of fraudulent invoicing. The firm was debarred for a minimum period – until March 2013 – but can be released from debarment if it adopts certain remedial and preventive measures, such as implementation of an acceptable corporate compliance programme.

Working with the Indonesian authorities paid off, and it can also reap rewards in other countries.

Taking responsibility

Instituting corporate compliance programmes as a condition of settlements is one way in which the WBG is encouraging the private sector to take responsibility for curbing corruption. In September 2010, the World Bank released new compliance monitoring guidelines and appointed a new integrity compliance officer to oversee the implementation of the programmes by companies on the World Bank's debarred list. And in the same year it launched a revised version of the Voluntary Disclosure Program (VDP), a mechanism under which firms undertake internal investigations, disclose misconduct to INT and implement suitable compliance programmes. In exchange for full co-operation, they remain anonymous and avoid the reputational damage of public debarment. The level of co-operation shown by companies will affect the steps then taken by INT, which can include the initiation of sanctions proceedings.

This first generation of settlements, the enhanced VDP and the move towards compliance monitoring are major steps in the right direction. One option that has been put forward by a number of experts to further this is the concept of an anti-

corruption fund, which revolves around managing restitution and compensating societies for the damage they suffer as a result of corruption and crime. This concept has a number of complex implications, including how to calculate awards and how payments due will be determined, but these issues are not beyond our capacity, and that of our partners, to identify and resolve.

An international enforcement alliance: a reality in progress

In April 2010, the World Bank signed a benchmark agreement with four other multilateral development banks (MDBs). This sent out a clear signal that where corruption has an impact on development resources, companies stand to lose more than they gain.

Since the agreement, the World Bank and its partners have jointly recognised the cross-debarment of 31 companies and individuals across different regions. This accord has given new momentum to the anti-corruption effort following years of negotiation and hard work among MDBs in terms of harmonising both investigative processes and practices that can be punished through sanctions. Those practices covered by the agreement include fraud, corruption, coercion and collusion. The next level of progress will be defined by a new generation of preventive services, capacity-development products, investigation and prosecution outcomes and international crimefighting benchmarks.

The corruption hunters

The first meeting of the International Corruption Hunters Alliance (ICHA) in December 2010 demonstrated the convening power of the World Bank in making a difference in the corruption arena. It included 286 high-level prosecution and enforcement officials from 134 developing and developed countries, and was sponsored by the governments of Australia, Denmark and Norway.

The ICHA brought together a diverse range of enforcement and crimefighting experiences, which showed the commitment that exists to partner the World Bank in its fight against corruption. The Bank has a sanctions process that is effective, but it must be supported by resilient prosecutions that reduce crime and corruption. With the help of the Alliance, we will able to sharpen the impact of our investigations and sanctions so that prosecution mandates can be carried out where national laws have been violated. And courts can be called upon to deliver judgments.

The ICHA brings a powerful sense of what it means to have a global connection that can be activated in the face of international and regional corruption crimes. The experiences of the members of the Alliance reveal that many governments have developed laws but that, without enforcement, legislators' anti-corruption efforts are in vain. "Laws cannot walk without legs."

What constitutes an effective enforcement vision?

The World Bank's experience in 187 countries reveals that institutions, human capacity and political commitment are key to a strong enforcement effort that can extend its reach without bias and achieve the credibility needed to maintain integrity with the public. The Bank has convened a number of meetings where law-enforcement and financial experts meet to discuss their efforts to deal with questionable money flows, which often fuel violence and conflict. Through these networks, and the global dialogue between countries and international organisations, we are building up a global momentum that will ultimately take the issue of asset forfeiture to the next level.

The rule of law is equally vital – a point that has been brought home by our experience with projects, technical assistance, policy dialogue and public engagement. In the past, we have encountered voices arguing that development can happen while a blind eye is turned to corruption. Today, those voices are silent, after experiencing the harsh reality of a public denied equal opportunities to jobs, services and participation. The World Bank's governance and anti-

corruption strategy, adopted in 2007, paved the way for putting accountability, transparency and public access to information in the mainstream of many Bank projects, through a variety of tools and mechanisms including e-procurement and community watchdogs. These interventions empowered communities to become part of informed decision-making and inspired a stronger public advocacy for accountability.

The Declaration of Principles for Effective Global Enforcement to Counter Corruption, announced at the Global Enforcement Roundtable convened by the World Bank during its 2011 spring meetings, encourages reciprocal disclosure of information, spontaneous reporting mechanisms for suspicious transactions, and investigative assistance. But equally important, we are seeking partnerships with global enforcement agencies to respond to some of the pertinent questions on the radar of clients and the public. One of the questions is how to deal with criminality at the very top. This is not easy in all countries, where criminality can often be linked to captured power and structures that are difficult to unravel. Working with enforcement entities nationally and internationally, we are leveraging knowledge and experience on the best strategies to clean up corruption, and are seeing the change that accompanies success.

Improving perceptions

Through the International Corruption Hunters Alliance and dialogue with international enforcement agencies, the World Bank is also strengthening the link between enforcement action and public perception of justice, so that we can reduce conflict, violence and other crimes that exacerbate poverty. An important question that the World Bank has raised with the Alliance is what can we do collectively to make sure that law and integrity take hold in states affected by fragility and conflict. An important message in the Bank's 2011 World Development Report is that the achievement of justice is a significant priority alongside jobs and security.

In terms of enforcement capacity, the challenges are complex but not impossible to overcome. A fast track to progress starts with a blunt recognition of the powerful and bureaucratic bottlenecks that obstruct justice, and then a committed effort to reduce their influence, while ultimately aiming for their substitution with processes that can enhance credibility, transparency and accountability.

Investigating and prosecuting authorities need to lead the way in applying those standards, to maintain their credibility and earn their rightful status in the public eye. An important outcome of the ICHA's first meeting was guidelines for measuring the performance of anti-corruption authorities. In addition, a number of co-operation agreements were signed with several authorities, including the UK Serious Fraud Office, the International Criminal Court, the United States Agency for International Development, the United Nations Development Programme, and Australia's Overseas Aid Program – in addition to prosecuting authorities in South Korea, Thailand, Mongolia, Southern Sudan, Indonesia and Uganda, among others.

These agreements and guidelines are important in upholding the rule of law and cementing the performance of criminal, investigative and prosecutorial authorities around the world. In 2010, the WBG launched a series of risk-prevention and investigative-training exercises to advance 'red flag' detection, evidence management and witness-interviewing techniques.

Is corporate compliance a reality or a myth?

In the wake of the global economic downturn, the private sector has been turning its interest to multilateral development banks that provide project financing for private investment in developing countries. In the past two years, countries have sought financial assistance from MDBs to invest in infrastructure projects, while private international banks and capital markets pursue their recovery process. In 2010, the WBG committed more than $72 billion to addressing

poverty and promoting economic growth and private sector development in countries hit by the financial crisis.

On the integrity front, the WBG also brought in a new set of compliance standards that were accepted by all major shareholders representing donor and borrower countries. As part of the institutional efforts to enhance this regime, debarment with conditional release has become the default or 'baseline' WBG sanction for cases initiated under its revised sanctions procedures. In future, the establishment (or improvement) and implementation of an integrity compliance programme satisfactory to the WBG will be a principal condition for ending a debarment.

As mentioned earlier, the World Bank appointed an integrity compliance officer (ICO) in 2010, whose primary responsibility is to monitor compliance by sanctioned companies (or codes of conduct for individuals). In addition, the ICO will decide whether the compliance conditions – and/or others established by the sanctions board or a WBG evaluation and suspension officer as part of a debarment – have been satisfied. Other conditions might include remedial actions related to the relevant misconduct.

A primary purpose of these recent revisions to the WBG sanctions regime is to place greater emphasis on corporate rehabilitation and encourage sanctioned companies and individuals to adopt adequate and meaningful policies and measures that can help prevent, detect and reduce incidences of fraud, corruption, collusion and other forms of misconduct – and ultimately to change the governance landscape where it matters most.

Compliance as a catalyst

While the execution of Bank-financed projects lies in the hands of borrower countries, the World Bank – through enhanced supervision and stringent procurement policies – is in a stronger position today to define the accountability boundaries within which its investments can be better protected, to ensure they reach the intended beneficiaries. In recent years, the Integrity Vice Presidency has ramped up its investigative capacity, preventive services and forensic accounting resources, with regional teams working closely with projects teams in the field. Now that a stronger sanctions regime is in place, compliance is emerging as a more viable catalyst for a private sector that is keen to engage in development business with the World Bank and to gain a solid reputation in new and emerging markets.

Getting back on the right road

In June 2011, INT's Preventive Services Unit released its first review of the global roads sector, assessing the vulnerability of the sector to corruption based on international and Bank experiences.

While roads projects supported by the WBG have had consistently positive development results, the dangers of fraud, corruption and collusion plague the sector worldwide. This is a problem for both developed and developing countries; yet it is much more costly in terms of opportunity costs and lost economic growth for developing countries.

To help our clients safeguard their roads projects, the World Bank must be innovative and learn more systematically from both our experiences and those of our development partners and client countries. The report by INT supports this effort, by turning the results of its investigations, and the experiences of developed and developing nations, into practical advice about a range of measures to stem collusion in tenders for roads contracts, and fraud and corruption in contract execution.

One important conclusion in the report is that when collusion or corruption is systemic, change requires breaking the cycle of abuse by bringing in someone from the outside – a prosecution service, anti-corruption agency, competition law authority, supreme audit institution, or, in the case of a local authority, the national government. If senior officials are involved, introducing an outsider can be particularly challenging. When corruption is deeply ingrained, short-term palliatives, such as an independent procurement

Combating collusion by changing the procurement process

The World Bank's experience with the Bali urban infrastructure project

World Bank staff became suspicious when only three bids were submitted for one of the first contracts on the Bali urban infrastructure project. Suspicions were heightened when, despite wide variations in labour and materials prices on the bidders' bills of quantity, the prices submitted by all three were within 0.02 per cent of the engineer's estimate. When additional investigation confirmed the existence of a bid-rigging cartel, the Bank made a number of changes to the procurement process to increase competition:

- procurement notices were widely publicised in both national and provincial papers in prominent places and in large typefaces
- the attempts of local authorities to limit eligible bidders to local firms were rebuffed
- bidders' qualifications were evaluated after, rather than before, the tender
- mandatory participation in pre-bid meetings, which had given colluders an opportunity to agree on prices and intimidate firms not part of the ring, was ended
- a complaint-handling mechanism was introduced that allowed contractors and community members to anonymously report fraud, collusion, corruption and intimidation.

The impact of the changes was dramatic. As the table below shows, bids dropped from amounts virtually identical to the engineer's estimate to amounts 35 to 40 per cent less. Overall, the project team estimated savings of 15 to 30 per cent on contracts let after the changes.

Bids for US$50,000 contract: best three bids as percentage of engineer's estimate

Original	*Post-changes*
98.9%	58.0%
99.7%	67.6%
100.0%	68.0%

evaluator or technical auditor, may be the answer. However, more drastic measures may also be required, and the report reviews three: the use of bid ceilings, competitive negotiation, and turning procurement over to an independent agent.

Not all corruption is systemic, and thus not all reforms require such significant steps. In the Bank-supported Bali urban infrastructure project, for example (see above), a local bidding ring was defeated through the circulation of tender notices to firms in other provinces. In the Philippines, civil society monitors uncovered corrupt schemes in a variety of government contracts, and in the second phase of the country's national road improvement and management project, civil groups were called on to monitor all phases of the work. This shows that clients working with us can make the sector relatively safe.

The next level of action

Where the World Bank has enforced sound administration through rigorous financial disclosure, tough audit rights and stringent reporting obligations, the effect on wrongdoing has been chilling. This holds true at a national level, where those countries that make information about budget decisions easily accessible to the public greatly reduce opportunities for corruption and greatly increase private sector interest.

Until recently, the definition of loss as a result of corruption was restricted to resources that ended in the wrong pockets. Today, public voices are redefining the reality of the social and associated costs of failures in development through their challenging experiences, their expectations of a better future and legitimate demands for opportunity and justice. These will be important keywords in shaping the present and future of corruption and fraud crimefighting.

Without a doubt, the moment has arrived for anti-corruption work; its advocates are shifting the political sway and interplay around the globe. For those of us who have been in this fight for the long haul, we can feel the lifting of a great burden. We no longer have to struggle to be heard when we talk about corruption, and we no longer have to pretend we can fix the failures of development, while ignoring the fact that many of these failures are the consequence of corruption run amok.

The fruits of our labour are the results of hard work, straightforward strategies and a desire to assure our shareholders and beneficiaries that every development dollar, especially in times of fiscal restraint, is spent to overcome poverty and boost growth and opportunity. This is a recipe for winning.

• *The findings, interpretations and conclusions expressed in this paper do not necessarily reflect the views of the executive directors of the World Bank or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work.*

8

Co-ordinating the fight against fraud and corruption: agreement on cross-debarment among multilateral development banks

Stephen S Zimmermann, Director of Operations of the Integrity Vice Presidency, Frank A Fariello Jr, Lead Counsel, Operations Policy, in the Legal Vice Presidency
World Bank Group

The fight against fraud and corruption took a major step forward in April 2010 when the heads of five leading multilateral development banks (MDBs) – the African Development Bank Group[1] (AfDB), Asian Development Bank (AsDB), European Bank for Reconstruction and Development (EBRD), Inter-American Development Bank Group[2] (IDB) and World Bank Group[3] (WBG) – signed the Agreement for Mutual Enforcement of Debarment Decisions (the Agreement).

At the time of writing, the Agreement has become effective for four of the five signatories – the AsDB, EBRD, WBG and IDB – after they put the required changes to their respective policies and procedures into place. It is anticipated that the AfDB will soon be in a position to begin implementation of the Agreement.

In this chapter, we examine the policy rationale behind the Agreement, the developments that led up to it, its principal provisions and some key issues and challenges faced by MDBs in crafting the Agreement. We also look at the prospects for deeper and wider harmonisation in the near to medium term.

Setting a standard for sanctions

In principle, aggressively tackling fraud and corruption in development projects should be a central part of the common agenda of MDBs. The 'cancer of corruption' undermines efforts to combat poverty and wastes the scarce resources of the international aid community. But until relatively recently, a number of obstacles had made it difficult for international organisations to move forward.

For many years, corruption was seen as primarily, if not exclusively, a political problem with little or no relevance to economic development. Moreover, work on corruption was felt to contravene the so-called 'political prohibition' that is hard-wired into the constituent documents of most (but not all) MDBs, barring them from interfering in the political affairs of their members.[4]

More recently, however, the close nexus between corruption and other governance issues on the one hand, and development, including economic

development, on the other, has become clear.[5] And it has also become clear that, if done right, governance issues may be addressed without violating the political prohibition.[6]

Moreover, when it comes to sanctions, the MDBs owe a fiduciary duty to their stakeholders, enshrined in their constituent documents, to safeguard the proper use of their funds.[7] It is this duty that underlies sanctions, which operate as a key disincentive against the misuse of MDB funds. While the MDBs will never be able to investigate and punish every instance of misuse, sanctions in a relatively small number of cases can create broader deterrence.

Application of this tool is not always straightforward. On a political level, for example, the MDBs face challenges due to their co-operative governance structures, in which their shareholders (member countries) may face pressures if their private sector 'champions' are subject to MDB sanction. And although sanctions are not aimed at government, the investigations leading up to them often uncover wrongdoing by government officials, which can be a sensitive issue for the member countries.

Early progress

Notwithstanding these challenges, by the early 2000s, the leading MDBs had established mechanisms to investigate and possibly penalise fraud and corruption in the projects they financed. Although similar in purpose and with generally common goals, these mechanisms were each developed separately, drawing on the distinct institutional cultures and political tolerances of the individual MDBs. While the banks had similar business models, little effort had been made to harmonise the specific provisions of these fairly novel programmes.

Certain core elements were common to most of these sanctions mechanisms. Rather than rely on local law in each country, all the MDBs had decided to create a level playing field by adopting a single set of anti-corruption policies applicable in all of their projects. They had set up 'integrity' offices to investigate allegations of violations, along with adjudicative mechanisms to determine when the policy had, in fact, been violated. And, finally, each MDB had settled on ineligibility – in other words, debarment – as the most likely sanction to be imposed.[8]

As the sanctions mechanisms were implemented, it became clear that the devil was in the detail. How should fraud and corruption be defined? What rules should govern the investigative process? How much due process should be afforded to an accused party?

Collectively, the MDBs came to realise that uniformity would allow them to set the standard for best practice. Each bank would then be able to point to the policies of the others as a basis for how to proceed. Moreover, while the MDBs did often compete for business on price and product among their client countries, there was recognition that flexibility on issues of integrity should not be used to win business. Setting a single standard would allow the MDBs to draw a line that none should cross.

Rationale and background for the Agreement

In February 2006, a Joint International Financial Institution Anti-Corruption Task Force (IFI Task Force) including the AfDB, AsDB, EBRD, IDB and WBG, as well as the European Investment Bank (EIB) and the International Monetary Fund (IMF), was formed to work towards a "consistent and harmonised approach to combat corruption in the activities and operations of the member institutions".[9] It was recognition that "a unified and co-ordinated approach is critical to the success of the shared effort to fight corruption and prevent it from undermining the effectiveness" of their work.[10]

As that work got under way, the members of the IFI Task Force agreed that consensus needed to be reached on harmonised definitions of the types of illicit conduct they would consider punishable by sanctions. Each of the member institutions had already established four such offences: corrupt, fraudulent, collusive or coercive

practice. The task ahead was therefore to align their respective definitions of these practices. After much debate, the IFI Task Force agreed on those definitions, so creating a single set of violations applicable in every project financed by participating institutions.[11] The adoption of these harmonised definitions would not only provide uniformity for governments and firms executing development projects financed by different international financial institutions, but also create a single benchmark by which all of the IFIs could judge whether a punishable practice had occurred.

The search for unification

Attention then turned to the creation of a unified set of principles and guidelines to govern how the integrity offices of the respective MDBs would execute their investigative mandates. Starting with the investigative guidelines adopted by the Third International Investigators Conference,[12] the IFI Task Force was able to agree on a set of core elements: definitions of misconduct and the standard of proof; the rights and obligations of witnesses and subjects, and of investigative staff; procedural guidelines on sources of complaints, receipt of complaints, preliminary evaluation, case prioritisation and investigative activity; investigative findings; referrals to national authorities; review and amendment; and publication.

During the final meetings of the IFI Task Force over the summer of 2006, discussion turned to whether institutions were prepared to recognise and enforce each other's sanctions decisions. It became clear, however, that the work to reach agreement on definitions and guidelines had expended the then available political will; the MDBs were not yet willing to surrender the independence and 'sovereignty' of decision-making that would be implicit in accepting recognition of each other's debarment systems. Each firmly believed that they had to maintain control over whom their institution would sanction and the terms of the sanction.

It would be necessary to allow these initial agreements to take root before further agreement could be reached. Indeed, the initiatives agreed to by the IFI Task Force still required the approval of both the respective heads and, in some matters, the boards of the MDBs.

In September 2006, the heads of each of the institutions represented on the IFI Task Force met at the annual meetings of the World Bank and IMF in Singapore and signed the Uniform Framework for Preventing and Combating Corruption, laying down the cornerstone for future harmonisation among the banks in the area of fraud and corruption. The Uniform Framework included not only an agreement on harmonised definitions and investigative guidelines but also a placeholder for future discussions on cross-debarment, by stating that the institutions would "explore further how compliance and enforcement actions taken by one institution can be supported by the others". It was an undertaking predicated on the understanding that "mutual recognition of … enforcement actions would substantially assist in deterring and preventing corrupt practices".

Over the next few years, each of the MDBs won approval from their governing bodies for the definitions and implemented the Uniform Framework. This new partnership fostered closer ties in responding to integrity issues and due diligence in private-sector financing activities as well. Constant communication and frequent contacts led to an increase in trust and confidence between the maturing integrity offices – a sense of community that was further supported by the movement of staff from one office to leadership positions in others.

'A bridge too far'

Harmonisation took another step forward when, in early 2009, some of the MDBs that had comprised the IFI Task Force in 2006 expressed an interest in reopening a dialogue on the possibility of setting up arrangements for the mutual enforcement of sanctions.

The first proposal on the table, advocated principally by the World Bank, was the establishment of a Joint Sanctions Board (JSB).

Under this proposal, the JSB would act as an autonomous body to hear sanctions cases from each of the participating MDBs using a uniform set of procedures. The internal procedures for the initial vetting of cases would be left to each MDB to work out, although some expressed an interest in an arrangement like the WBG's evaluation and suspension officers.[13] The proponents of the JSB believed that it would play an important role in facilitating a unified approach to reducing fraud and corruption in MDB-supported projects.

However, the JSB idea quickly ran into a number of stumbling blocks, primarily the wide variance in adjudicative mechanisms employed by the MDBs.[14] The WBG sat at one end of the spectrum with a quasi-judicial, two-tier system that included an oral hearing, an appeals mechanism and detailed procedures. None of the other MDBs were employing systems as elaborate as the WBG's and none were prepared to move significantly in that direction. While all recognised the need to provide adequate notice and some due process to the accused parties, each also believed that their own mechanisms were sufficient. Moreover, each institution continued to feel strongly that it should have sole control over who the decision makers would be.

The debate also raised some fundamental issues on which the MDBs diverged. For example, should the sanctions process of each bank be viewed simply as a decision over whom the MDB chose to do business with, or, given that the focus was on acts of fraud and corruption, should it be treated as a judicial or quasi-judicial action requiring more robust due process? Were anti-corruption policies more akin to due diligence by traditional investment banks, or had the MDBs taken the responsibilities of an international regulator?

Underlying the questions was a more fundamental point: did firms and individuals have a right to do business with the MDBs under the 'open procurement' principles that each of them had embraced? If so, then it followed that those firms and individuals should not be deprived of their rights without robust due process. If not, then the decision to debar was essentially a unilateral business decision by the MDB, and the only due process required was one sufficient to ensure that the decision itself was not arbitrary. A JSB would therefore have made good sense under the former view, but been excessively burdensome under the latter.

Each of the MDBs addressed these issues indirectly, through the manner in which they had chosen to implement the anti-corruption programmes. And while all the MDBs' systems relied on the same central precepts, none were yet ready to sacrifice the nuances and policy assumptions of their own decision-making mechanisms in favour of the others.

The road to cross-debarment

In light of these thorny issues, the banks agreed that the JSB was a 'bridge too far', and that the most logical next step in the harmonisation of sanctions processes would be the creation of an effective cross-debarment regime. Therefore, during the course of 2009 and 2010, representatives of the MDBs[15] met to discuss the key elements of a regime based not on common rules or procedures, but on common 'core principles' of due process.

It was expected that cross-debarment would serve many of the same purposes as a JSB while still preserving each MDB's autonomy in policy- and decision-making. As stated in the Uniform Framework, cross-debarment among the banks would greatly enhance deterrence and thus the prevention of corrupt practices, so strengthening integrity efforts and safeguarding development resources from corrupt participants. Cross-debarment would also significantly enhance the deterrent effect of sanctions by any one MDB, effectively multiplying the impact of a debarment on a firm or individual by foreclosing the possibility of their winning contracts with the other MDBs.

Cross-debarment would also address some of the significant fiduciary and reputational risks associated with the financing of contracts with

firms and individuals on which sanctions had been imposed by other MDBs.

Apart from the EBRD,[16] none of the MDBs had previously had a process in place for cross-debarment. Thus, under the 'open procurement' principles adopted by each of the banks, firms and individuals sanctioned by one development bank were free to continue doing business with others, potentially engaging in further misconduct.[17]

This situation exposed the MDBs' borrowers and donors – and, most importantly, the beneficiaries of the projects they financed – to further prejudice, while at the same time leaving the MDBs themselves open to serious reputational risks for continuing to engage with firms and individuals found by a sister institution to have committed acts of fraud or corruption.[18]

In addition, although each MDB would retain its own sanctions process and standards within the core principles, it was hoped cross-debarment would encourage deeper harmonisation among the MDBs, leading to greater consistency of sanctions. It was also felt that smaller, regional MDBs might be more willing to take part in a cross-debarment regime than a JSB, for the same reasons that made the proposal problematic for the larger MDBs. Similarly, it was hoped that the desire to join the cross-debarment regime would serve as an incentive for regional MDBs to put in place the core principles.

Key terms of the Agreement

The Agreement is based on mutual representations by each of the signatory MDBs that its sanctions regime meets certain common core principles:

- that the MDB has adopted the four harmonised definitions of fraud and corruption in the Uniform Framework
- that the MDB follows IFI Principles and Guidelines for Investigations
- that the MDB has sanctions processes with certain key due process elements, including an internal investigative authority and a distinct decision-making authority; written and publicly available procedures that require notice to accused parties and an opportunity to respond; a 'more probably than not' standard of proof or equivalent; and a range of sanctions that take into account the principle of proportionality, including aggravating and mitigating factors.

In reliance on these representations, each signatory MDB agrees to recognise and enforce any debarment decisions of the other signatories that meet the following criteria:

- the debarment is for fraud and corruption under one or more of the four harmonised definitions: fraudulent, corrupt, coercive or collusive practices
- the debarment is made public
- the debarment period exceeds one year
- the conduct that gave rise to the debarment occurred no more than ten years prior to the debarment decision
- the decision to debar is taken after the Agreement takes effect with respect to that MDB.

If the debarment decision meets these criteria, cross-debarment by the other MDBs is essentially automatic. There is no review by the other banks of the underlying decision or the reasons for it, and the original debarring MDB determines the period of debarment. However, each of the MDBs has reserved a right to 'opt out' if they determine that the debarment is inconsistent with 'institutional or legal considerations'.

The Agreement provides that other international financial institutions[19] can join if they sign a letter of adherence and meet the core-principles standards, and all existing signatories consent to their adherence. Signatories are also free to leave the arrangement by written notice.

Key issues and challenges

Why is cross-debarment automatic?

The MDBs considered but rejected a system whereby each bank would be able to engage in a

de novo review of each sanctions decision before agreeing to cross-debarment in a particular case. The working group concluded that allowing de novo reviews would not only be costly and laborious, but could well result in inconsistent decisions among participating banks, exposing both the original debarring MDB and the non-cross-debarring MDB to reputational risks. Moreover, inconsistent results might encourage litigation by entities or individuals against the organisation that had imposed the sanction on the same facts.

It was agreed that the more effective form of cross-debarment would be one that was triggered automatically, subject only to the specified criteria and the 'opt out'.

Why insist on cross-debarring public debarments only?

The MDBs agreed it was essential that only public debarments would be cross-debarred, even though this effectively excluded most sanctions imposed by one of them: the AsDB.[20]

There were several reasons for this approach. Among these, although not stated explicitly as a core principle, was that most MDBs believed a degree of transparency was an essential element of due process. The duty to cross-debar a non-public debarment would oblige the other MDBs to adopt non-public debarments themselves – something they were not willing to do on policy grounds, and also on practical ones: it is through publication that the MDB borrowers' implementing agencies and other interested parties are made aware of debarments so that they may enforce them in their own procurement decisions.[21]

Moreover, public debarments increase the deterrent impact, and an insistence on publicity reinforces this effect.

Was the creation of 'safe harbour' for debarments of one year or less the right thing to do?

The MDBs recognised that some cases might not warrant the onerous impact of cross-debarment. After all, for firms that are heavily reliant on MDB-financed business, cross-debarment could put them out of business. While this would most certainly be a strong deterrent, it might also be seen as disproportionate for lesser offences.

In an effort to balance these competing concerns, the Agreement allows for a 'safe harbour' in that cross-debarment is only applicable to debarments exceeding one year. It is hoped that this 'safe harbour' will provide an incentive for firms under investigation to co-operate with the MDBs with a view to mitigating their sanction.

The 'opt out' clause: a giant loophole or a necessary escape valve?

The MDBs wanted to allow for exceptional situations in which individual MDBs might need to opt out of the cross-debarment regime if there were overriding 'legal or other institutional considerations'. For example, the WBG would normally not apply sanctions to a firm participating in its Voluntary Disclosure Program (VDP).[22] Similarly, the WBG would not be able to enforce a sanction through cross-debarment against a firm with which the WBG had resolved a case through negotiation, if the terms of the negotiated resolution related, in whole or in part, to the conduct for which the other MDB debarred the firm.

Given the current lack of common sanctioning guidelines among the MDBs, this opt-out right also allows the banks to decline enforcement of a debarment decision that may be egregiously sweeping in scope or duration, significantly impairing the development missions of the other MDBs. It also allows for 'one off' exceptions where a debarred party is playing a crucial development role, particularly in emergency situations.

Any decision to opt out would not affect the decision of the other participating MDBs to cross-debar in the same case. If an MDB chooses to exercise this clause, it is required to provide written notice to each of the other participating banks. While MDBs do not have to supply the reasons for

their decision, which would be based on 'sovereign' matters of internal policy, this notification requirement alone should provide an incentive only to use the clause in exceptional circumstances. In any event, the participating MDBs know that anything other than very limited recourse to the opt-out would endanger the credibility of the system as a whole, to the detriment of all the banks. At the time of writing, in fact, none of the MDBs has invoked its opt-out right.[23]

In the absence of an opt-out clause, an MDB confronted with a legal or institutional matter that would preclude the imposition of a particular cross-debarment would be faced with the Hobson's choice of either committing a breach or perhaps having to withdraw from the Agreement. Given this alternative, the opt-out can be seen as the lesser of two evils.

A special challenge for the World Bank: applying cross-debarment to existing projects

MDB cross-debarment required a change in World Bank procurement policy, which in turn necessitated amendments to the relevant legal framework for the World Bank's loans and grants, including the Procurement, Consultant and Anti-Corruption Guidelines, as well as the General Conditions.[24] Unlike other MDBs, the World Bank customarily applies changes in policies only to new loans and grants. The existing portfolio – even if there is new procurement – is not affected by changes in policy unless the Bank and its borrowers agree otherwise.

The Bank has traditionally taken this position essentially on fairness grounds. Once the Bank and its borrower have agreed to apply a certain set of policy-based rules to govern a particular project, it has been felt that it would not be fair if the Bank could unilaterally change the 'rules of the game' in mid-course.

In the case of MDB cross-debarment, however, this stance posed at least two problems:

- the other MDBs intended to apply cross-debarment to new contracts in both new and existing projects. At least one other MDB found it unacceptable that the Bank would not do the same and viewed non-application of the regime to the Bank's existing projects as a potential 'deal breaker' because it violated the principle of reciprocity that was central to the Agreement
- the Bank itself faced major reputational risk, since it would have been hard-pressed to explain to the press and public why it was continuing to finance contracts with cross-debarred firms on some – and, in the short term, most – of its projects.

A consensus formed that the World Bank needed to find a way to apply cross-debarment to its existing portfolio. Its lawyers concluded that the only legally valid way to do this was by amendment of all existing legal agreements with the Bank's borrowers. International legal principles did not allow it to do this unilaterally, but the task of undertaking individual amendments to literally hundreds of agreements, co-signed by borrowers, seemed onerous at best. The Bank therefore adopted a somewhat novel approach: 'omnibus' amendments of the legal agreements with each borrower on an 'absence of objection' basis, so that unless the borrower objected within a defined period, the Bank would consider the amendment to have taken effect automatically.

This approach aroused some controversy. A relatively small number of borrowers did, in fact, object or ask for more time to consider the amendment. The Bank granted these requests and actively engaged with those borrowers that had stated their opposition; at the time of writing, only a handful of objections were still outstanding.

This issue brought out an interesting point: none of the other MDBs needed to go through this exercise in order to put in place the policy changes required to implement the cross-debarment regime. In some cases, the other MDBs' policies themselves were broadly enough stated to allow for cross-debarment without a change in procurement

policy. In other cases, changes were automatically applied to existing projects because their legal agreements incorporated their policies 'as amended from time to time'.

This experience has led some of us at the World Bank to question why we take such a different approach from our sister institutions. The 'fairness' argument that underlies the Bank's current practice is open to challenge, and not simply because other MDBs do not share the practice. Bank policies are only adopted after extensive consultation with member countries and other stakeholders. Moreover, the Bank, like its sister MDBs, is a co-operative institution – its borrowers are also its member countries, represented in the Bank's governing bodies. Any amendments to Bank policies require the approval of those bodies, and it is not immediately obvious that the changes should always be assumed to redound to the detriment of the Bank's borrowers.

More often than not, in fact, the opposite is true, which is why many borrowers agree with the Bank, either formally or informally, to apply new policies to ongoing projects. The Bank's position that the loan agreement requires formal amendment, however, means that there is often a mismatch between the formal legal framework for a project and the reality 'on the ground'. And, ironically, even if the Bank's approach to policy changes is fairer in substance, it does not always appear so to the borrowers. In this case, for example, the Bank was believed by some borrowers to be imposing a change, when it was actually asking borrowers to consent to a change that other MDBs were implementing automatically.

What is the likely impact of cross-debarment on the private sector?

There is some concern that cross-debarment could have a 'chilling effect' on bidders in MDB-financed procurement. However, it is our belief that this effect would apply mainly to those firms and individuals whose practices are already questionable. In this sense, the chilling effect is just another way of talking about deterrence. Honest firms with effective integrity compliance programmes should have nothing to fear from cross-debarment.

The risk of cross-debarment should provide firms with an incentive to re-evaluate their governance and compliance systems in an effort to mitigate the risk of sanction and cross-debarment. In the wake of the adoption of model compliance principles as part of the reform of its own sanctions process, the WBG intends to engage in outreach with the business community and other stakeholders to explain the cross-debarment regime and what steps they can take to mitigate the risk.

Cross-debarment should also encourage company management to come forward voluntarily as soon as they learn of misconduct in their operations, leading to expansion of the Voluntary Disclosure Program and the use of negotiated resolutions.

And while it is difficult at this point to assess the impact on corporate behaviour overall, debarment decisions by MDBs are also beginning to have an impact outside the development arena: private firms have begun to include a review of debarment decisions in their traditional integrity research.[25]

Experience with cross-debarment so far

At the time of writing, the Agreement has become effective with four of the five signatory MDBs. The AsDB and EBRD became the first signatories to implement the cross-debarment regime in June 2010, and the WBG followed a month later and the IDB in May 2011. Implementation by the AfDB is anticipated.

As of February 2010, the World Bank had cross-debarred 15 firms and individuals, all of which were originally debarred by the AsDB. The AsDB, in turn, had cross-debarred 13 entities originally debarred by the World Bank. The EBRD had recognised 10 of the debarments issued by the World Bank and 12 issued by the AsDB. In line with expectations, no debarment by any of the signatories has been subject to an opt-out by another signatory.

Next steps for harmonisation among the major MDBs and beyond

Further harmonisation among the major MDBs

Cross-debarment should serve to embed still further the MDBs' role as leaders in the global effort to combat corruption. By encouraging the banks to work together, cross-debarment should reinforce the momentum behind their anti-corruption efforts and provide an 'enabling environment' for overcoming the challenges outlined at the start of this chapter.

Already there are discussions under way among the participating MDBs on harmonising their sanctioning guidelines, as well as on finding a common approach to the scope of sanctions when dealing with corporate groups.[26] Moreover, cross-debarment has underscored the need for closer co-operation and exchange of information among the banks. Parallel or joint investigations between MDBs and with national authorities have already become more common.

While it is probably premature at this juncture to talk about an established droit commun (general law) among the MDBs, these developments certainly open up that possibility in the future. Already there is significant congruence among the MDBs in the forms of misconduct they consider punishable by sanctions, and shared due-process principles for the adjudication of cases. The upcoming publication of sanctions decisions by the WBG will begin to create a jurisprudence to fill out the detailed contours of these general principles. To the extent that other MDBs choose to rely on such jurisprudence or may be willing to follow suit and publish their own decisions, one day we may indeed see the emergence of a common body of law in this area.

Harmonisation beyond the major MDBs

The Agreement also opened up the possibility of broadening the harmonisation efforts to other international financial institutions. The WBG and other participating MDBs have already started working with smaller, regional MDBs to help them develop and implement anti-corruption programmes that will conform to the core principles.

Some of these banks have expressed interest in participating in a cross-debarment regime and have indicated that they may recognise cross-debarment decisions unilaterally. Others have made participation a specific goal for their institution. While work remains to be done before additional MDBs can be added to the cross-debarment regime, this would be a positive development that would further strengthen deterrence, harmonisation and collaboration – all key components in the fight against fraud and corruption.

There are also inchoate efforts to extend a degree of harmonisation beyond the IFI community. In February 2008, at the first Roundtable of the Legal Harmonization Initiative (LHI Roundtable), sponsored by the World Bank, the concept of common approaches to fraud and corruption among major MDBs, several United Nations (UN) agencies and bilateral aid agencies was floated for the first time.

While the LHI Roundtable participants expressed openness to the idea in principle, they also agreed that reaching this level of harmonisation would require considerable discussion and effort, given the wide disparities in institutional governance structures, operational models, policies and practices, including the basic question of how they defined 'corruption'.

Since then, harmonisation has proceeded along a number of parallel 'paths of least resistance'. As outlined in this chapter, the major MDBs, which share similar business models and had roughly similar sanctions regimes, found common ground in cross-debarment, largely outside the LHI framework. At the same time, as part of the LHI, the MDBs and key bilateral aid agencies successfully negotiated a framework for operating sector-wide approaches and co-financing situations, which included some basic common understandings on the handling of fraud and corruption issues. And the UN[27] has launched a process to harmonise sanctions, which we understand is at a fairly advanced stage.

In November 2010, the G20 issued an Anti-Corruption Action Plan, which called for increasing international co-operation. While the details of implementation remain under discussion, the Action Plan provides an important additional impetus for harmonisation among MDBs and beyond.

Notwithstanding the significant challenges that would need to be confronted, as the MDBs, UN and bilateral aid agencies deepen their own harmonisation, and the broader international community develops stronger approaches to fraud and corruption more generally, there remains scope to open up a dialogue on a yet more comprehensive approach to harmonisation among international actors. The importance of the fight against corruption, and the logic of harmonisation, demand it.

• *The authors would like to thank Roman Majtan, consultant in the Legal Vice Presidency of the World Bank, for his valuable assistance in the preparation of this article.*

World Bank Integrity Vice Presidency

Integrity for Better Results

The World Bank Group is committed to ensuring its projects are of highest integrity

Please report concerns of fraud and corruption to:

Call 1-800-831-0463 inside the US
Call 1-704-556-7046 outside the US

Operated by an independent third party Open 24 hours a day Interpreters available Anonymous calls accepted
Or email: investigations_hotline@worldbank.org

For companies interested in INT's Voluntary Disclosure Program contact: phaynes@worldbank.org

For more information, please visit www.worldbank.org/integrity

Don't Face Compliance and Ethics Issues Alone

Join the Society of Corporate Compliance and Ethics and enjoy the support of over 2,200 compliance and ethics professionals worldwide

Declining budgets, increased regulation, and heightened enforcement are all making compliance and ethics more challenging, and more important, than ever.

SCCE can help you manage your compliance and ethics program—and your career—through these times. As an SCCE member you will enjoy a host of services informed by the shared knowledge of our membership, such as conferences, certification, a bimonthly magazine, a weekly e-newsletter, and SCCEnet, our online social network.

Join SCCE today and tap into a vast network of information and resources to help move your ethics and compliance program forward, no matter how difficult the times.

To learn more about SCCE and how we can help, visit us online at **www.corporatecompliance.org/join**

SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

JOIN THE DISCUSSION

SCCEnet

The Official Social Network of the Society of Corporate Compliance and Ethics

Over **7,000** professionals connect on SCCEnet to discuss compliance and ethics issues

JOIN FOR FREE AT community.corporatecompliance.org

ALSO CONNECT WITH SCCE ON THESE SOCIAL NETWORKS

Find us on Facebook
corporatecompliance.org/Facebook

FOLLOW US ON twitter
twitter.com/SCCE

JOIN OUR GROUP LinkedIn
corporatecompliance.org/LinkedIn

9

An alternative to adding more rules, laws and regulations for preventing serious economic crime

Roy Snell, Chief Executive Society of Corporate Compliance and Ethics

Many industries have struggled to prevent, find and fix their problems. As a result, society thinks the business community needs more rules, laws and regulations. Some of us are tired of the bureaucracy because it is onerous, expensive, complicated, vague and generally very frustrating. But if we want to stop the onslaught of regulations, we do have to prevent, find and fix our own problems. We have to take away society's reason for adding more rules. Internal compliance and ethics programmes are an alternative to the rule-based enforcement model. I spoke at a UN meeting in Warsaw about this. The international frustration with business and business leaders was palpable. We need to do something different.

Compliance prevents an explosion in bureaucracy

There is a common misconception that compliance and ethics programmes add rules. I have been in the compliance profession for 16 years and I can tell you that it is just not true. Most dictionaries define compliance as 'meeting the expectations of others'. And regulations, laws, ethics, values and principles are grouped together as 'a set of expectations'. I think people take these definitions and apply them to the programmes, which in reality add no rules, laws, principles or values to an organisation. What they do is help to prevent, find and fix problems with the rules; they ensure that rules are followed. If organisations do that, it is less likely that society and the government will think we need more rules. Compliance programmes are a superior alternative to adding further laws to fight serious economic crime.

The programmes move finding and fixing problems from an external methodology, the enforcement community, to an internal methodology – a compliance officer. These officers work with their colleagues to prevent, find and fix problems associated with rules, laws, regulations, ethics, values and principles. They help to fix problems as they are happening, or before they happen. They help their fellow employees understand and follow laws and meet the ethical expectations of the company's leadership. Ironically, if more businesses followed the law and met the ethical expectations of society, then society would add fewer rules to deal with poor behaviour.

Compliance programmes not only add no rules, they can reduce the number of rules a country imposes on its companies. Businesses and

industries that do not implement a programme, and run into problems, cause governments and society to insist on more laws.

Trust is the goal, not the control

The global economy is upon us. Some countries succeed in winning business abroad because they are trusted. Compliance and ethics programmes can help build that trust, boosting the economies of those countries, while untrustworthy countries suffer economically.

In the past, some companies were advised not to deal with their ethical and legal problems and 'deny and defend' if caught. This does not work, except for those selling 'deny and defend' services, and the road is littered with companies that have proved this point.

In the past, many organisations wanted to use ethics, values and principles to guide employees and encourage proper behaviour. That was helpful but it didn't succeed in actually getting all employees to follow the law. Compliance programmes stress values, principles and ethics but take the process a step further by finding problems and disciplining poor behaviour. Trust is not a control. Trust is a goal. Trust doesn't find all problems. Trust doesn't fix all problems.

When companies get into legal trouble, audit, legal or risk personnel are often interviewed. When asked why they did not fix the problem, they say it was not their job. Compliance programmes are responsible for finding and fixing legal and ethical problems. They are often the missing link.

Compliance and ethics programmes are the future. Deny and defend is passé. 'Fixing the problem was not my job' is passé. Telling your employees your company values, principles and ethics, and hoping it all works out, is passé. The future is: trust but verify. The future is prevention, not waiting for your government to do it.

A leap forward

There is a worldwide explosion of compliance and ethics programmes. South Africa, Australia, the United States, Ireland and other countries now have professional associations dedicated to compliance officers. Our association, the Society of Corporate Compliance and Ethics (SCCE), and its sister body, the Health Care Compliance Association, have 9,400 members in over 30 countries. Membership is growing rapidly. We have social networks with over 50,000 participants, from approximately 50 countries. We are connecting compliance professionals on Twitter, Facebook, LinkedIn and YouTube. We have our own social network, SCCEnet, which is open to anyone in the world.

The growth of these networks is significant. The growth of compliance and ethics programmes is significant for a civilised society and the success of the global economy. Those of us who want to move from a government enforcement model with ever-increasing regulations are excited. Those of us who were tired of the same old failed approach to finding and fixing our problems are excited. Those of us who are interested in restoring society's trust in business and business leaders are excited.

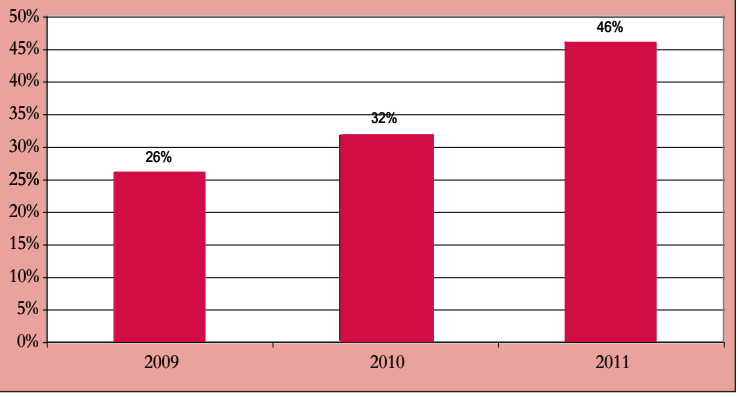
The Organisation for Economic Co-operation and Development (OECD) has a coalition of 38 countries that support the implementation of compliance and ethics programmes. The South Africans have published the King II Report, which encourages activity in this area. The United States Sentencing Commission has instructed the enforcement community to give significant breaks to companies that have made a mistake but had a compliance programme in place. US sentencing guidelines also suggest that penalties be significantly increased for companies that made little effort to prevent, find and fix problems. There are other countries moving in this direction. They are all tired of the failures of the past and they are tired of all the talking. They want an effective methodology for preventing wrongdoing.

What makes a compliance programme effective?

The tools that compliance programmes use are auditing, monitoring, investigations, incentives, anonymous reporting mechanisms, education,

Percentage of compliance professionals reporting year-on-year budget rises

The SCCE surveyed its 2,400 members in 25 countries on the growth of their compliance budgets. While many of the companies are US based, a large number are multinationals This survey shows an increased commitment to the implementation of compliance programmes.
2011 figures are forecasts



policies and procedures, ethics, risk assessments and reporting to the board or leadership. These are tools that have been around for years but they haven't been effective in the past because they weren't used in a balanced fashion and in concert with each other, and no one wanted to fix the problems they found. Managing a compliance programme is more challenging than just using the tools. There are many personalities to deal with. Sometimes problems are difficult to solve because someone has a conflict of interest. You have to know which tools to use and when; and you have to finish.

Some people beat to death the use of one tool, such as endless audits that aren't followed up on. Others conduct 18-month risk assessments that are so detailed you couldn't find a problem if your life depended on it.

Risk assessments point to where a problem might be. Audits point to a problem. Neither tool fixes problems. People are tired of all the analysis and finger pointing; they want problems fixed. But most do not know how to run a balanced and effective compliance programme.

To be effective, compliance officers need to know what is not worth fighting over and when to throw themselves in front of the train. They need independence, authority, and responsibility for preventing, finding and fixing problems. Good compliance officers do not take away the authority of other departments, such as audit, legal or risk, but form partnerships with them whenever possible. They just make sure that the compliance tools are being used properly, in a timely fashion, and that problems are dealt with rather than being swept under the rug.

The keys to success are simple. The compliance officer needs independence from all those who may be conflicted and the support of the leadership. There must be a balance between, on the one hand, encouraging people to have values and principles and to behave ethically – and, on the other, looking for, finding, fixing, enforcing and disciplining infractions. The compliance department needs adequate resources and strong, talented and respected people. It needs authority.

The principles of compliance

I have seen 700-page descriptions of what a compliance programme is. These have been put together by people who do not know what is important – so to them, everything is important. When a programme works, it is because it is a simple methodology. Everyone wants in on the act because it is a hot new topic.

Some seek to complicate it because they seek to make money from it. The more complicated compliance programmes are, the more people need help, and the more money there is to be made. But

Generally accepted compliance principles

Expectations	Ethics, values, principles, policies etc		Regulations, laws etc	
Prevention	Education	Incentives	Code of conduct	Internal controls/ policies/procedures
Look for problems	Auditing	Monitoring (conflict of interest/ background check)	Anonymous reports/hallway conversation	Risk assessment
Evaluate	Investigation		Measure programme effectiveness	
Fix and follow up	Corrective action		Discipline	
Report	Report to board a summary of all relevant compliance activities		Disclosure programme	

the truth of the matter is, they do not need to cost a lot of money; much of what you need already exists in your organisation.

I got tired of those 700-page descriptions and decided to see if I could describe a compliance programme in one page, with one diagram. Above is the result of this effort. The words along the left side of the diagram describe the general flow of a compliance programme. The boxes describe the tools used. Longer explanations than those provided below can be helpful, but what matters is that all employees and leaders know how compliance programmes work. Misinformation is plentiful in the world of compliance; a simple explanation is all we need.

As seen on the left side of the diagram, the general flow involves: determining the expectations, prevention, looking for problems, evaluating the problems you find, fixing the problems, following up, and then reporting to the board or leadership.

Determining the expectations is a fairly simple process of extracting the company values, principles and ethics. It also involves determining the laws and regulations that apply to your industry. This can be a lot of material, so in a later step we will talk about prioritisation.

Prevention has long been the focus of a lot of people. Most methodologies for stopping wrongdoing are focused on talking and hoping, which won't be enough. Prevention includes educating people about your expectations, particularly your ethical expectations. Education on applicable and commonly broken laws is also important. Good compliance and ethics programmes will include incentives for those who prevent, find and fix problems, tying them to bonuses and the annual employee review process.

A code of conduct is a summary of a company's ethics, values, principles, and key laws that affect its industry. It is often signed by all employees and visibly supported by leadership. Internal controls, policies and procedures are tools long used by the audit community. But this is

another area that is often beaten to death. One must be careful not to fall into the trap of sitting in an office and writing policies all day. Get out and look for problems.

The keys to success

Looking for problems is an important step and often not done well. As simple as it sounds, this is where we start getting into the key determinants of success or failure.

Auditing and monitoring are well-known tools used in finance. Risk assessment is another tool that has been around for some time; it can be used to prioritise the numerous potential problems that an industry may be facing. But many risk managers get lost in the detail, with hundreds, if not thousands, of line items in their assessments. Most settlements and prosecutions fall into a few high-risk areas. A good compliance and ethics professional will talk to peers in their industry and check recent settlements to help them focus on a few things rather than everything.

When I was a compliance officer, I found most of my serious problems by walking around. Although you should have an anonymous reporting mechanism, many people will not call the hotline. However, they are often dying to be asked if they have seen any ethical or legal infractions. When asked if they are aware of any problems, most people won't lie. When asked to call an anonymous reporting mechanism, they would rather not turn someone in voluntarily. They need to be put on the spot. They need to be asked. They want to be asked.

A good compliance and ethics professional is always asking questions, and it should help that most problems are known by more than one person. The trouble is, most problems will not be fixed by most people who are aware of them. They feel that, 'It's not my job to fix other people's problems.' And they have a very good point. That is why we need one person in every organisation who is responsible for fixing ethical and regulatory problems: a compliance and ethics officer.

A job for specialists

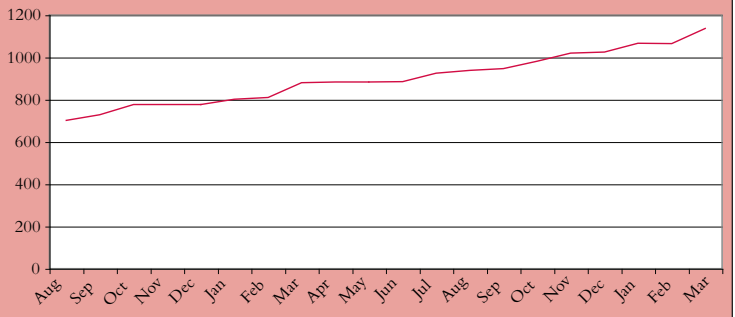
Evaluation is where the leading compliance and ethics professionals can really make a difference. Many people can get us to this point in a programme, but few can actually finish from here. Compliance and ethics professionals cannot under-react or over-react to a problem. The key is to uncover the facts through investigation. Legal help is often required but the mistake most people make is that they use legal experts with a general legal background, rather than a sub-specialist. We wouldn't go to a general practitioner for brain surgery, so why do we go to a general legal professional for a complex, specific issue that could cost our organisation a great deal of money? Good compliance and ethics professionals insist on one or more opinions from experts. It's appropriate to involve the legal department and counsel but not to delegate the compliance process to anyone else. Many problems have not been resolved until it is too late because some department insisted on control but not on fixing the problem – as discussed below.

Compliance and ethics programmes should also be evaluated for effectiveness. This can be a self-review or done from the outside. I would only ask for outside help if you can find someone who has been a compliance professional before. Everyone who has ever done legal work, conducted a risk assessment or audited something thinks they are a compliance expert. But these are the people who don't know what is important, and so everything is important; they get lost in the details. The tools – audit, risk, codes of conduct and education – are all simple if very valuable concepts in themselves and give inexperienced people the idea that they can evaluate a compliance programme. In reality, measuring the effectiveness of a programme is the most difficult compliance-related task there is.

Fixing and following up on problems is where most people have failed. Corrective action has been the step that few have managed to take in the past. Plenty of people are happy to audit, assess risk, write policies and talk about the legal

Growth in the number of compliance professionals: Aug 2009 to April 2011

The SCCE has conducted certification training in the US, Canada, Belgium, Brazil, Switzerland and the UK. Each event has been attended by compliance professionals from many different countries. The rapid growth in certified compliance and ethics professionals mirrors the rapid growth in compliance budgets.



implications of a problem, but in terms of actually fixing a problem, these people have often been found under the table. The leaders of an organisation under scrutiny for a serious legal infraction have either tended to deny and defend, or to claim that fixing the problem is not their job.

After the enforcement process is complete, audit, legal, risk and many other departments are often asked a simple question: did you know about the problem, and if so, why did you not fix it? The answer has often been the same: 'Yes, I knew of the problem and I did not fix it because it was not my job.'

Compliance professionals are charged with resolving a problem to the satisfaction of legal or ethics experts who have no conflict of interest. They do not walk away. They do not have a conflict. They are independent. They have authority. This is what is different from all the failed attempts of the past.

Enforcing discipline

If discipline is in order, compliance and ethics professionals help the appropriate individuals to determine and implement that discipline. This is what those who came before compliance failed to do. This is the difference between the compliance department and all other departments. Many other people in an organisation are able to point to the problem, but few can fix it and few want to deal with discipline. This is why compliance programmes are difficult to manage: it is easy to avoid conflict and bury your head in the sand, much harder to fix problems. Compliance professionals finish the job.

Not all your employees will always do what you expect, but everyone will do what you enforce. They won't do what you expect all the time because there are those who don't know that what they are doing is wrong. Some won't always do what you expect because they don't think they will get caught – or if they do, all they will get is a slap on the wrist. They can either rationalise their behaviour or are so conflicted that they can't help themselves. But there is no one who won't do what you enforce. Most see that you are serious and will not contemplate doing the wrong thing.

Reporting to the board

The final step of a compliance programme is periodic reports to the board. The leaders of an organisation will need to be assured that the programme is working. They will need to know what's going on so they can support the programme. The board should be informed of general compliance activities such as education, audit and risk assessments. They may need to approve documents such as the code of conduct

and they should be appraised of major problems uncovered by the compliance programme.

Effective compliance should also incorporate a disclosure programme that outlines who in the enforcement community will be told, if anybody, that a problem has been discovered. Many countries have laws that require disclosure of some types of problem. Your programme, at a minimum, should cover those laws.

Seeing the big picture

I once gave a presentation to owners of small businesses in Brazil using the Generally Accepted Compliance Principles diagram. I was trying to get my audience, who had never seen this concept before, to understand the way in which a compliance programme works. They asked many questions, many associated with the onerous nature of the programmes. One person finally summed it all up: 'This makes people feel as though you don't trust them.'

I told them you can balance compliance programmes with actions that demonstrate your trust, but also that trust is a two-way street. By not dealing with problems effectively, you are avoiding short-term pain for long-term pain. If you don't find and fix the problems, your people will suffer. You company will suffer. Your country will suffer. Other countries will not trust you. That lack of trust will affect your economy, standard of living, and the safety of your people. As hard as it is to deal with these problems, you will have less pain in the long run if you deal with your problems when they occur.

Brazilians are very nice people and they are not alone in this concern about showing a lack of trust in employees. We all just need to look at the bigger picture. Frankly, I think that employees who see problems going unresolved are frustrated and understand any efforts to prevent, find and fix problems.

Conclusion

Many people want a less onerous process than compliance – but they have tried and failed for many years. Trust is not a control. The press, the government and the people of almost every country in the world are very disappointed in the business community – all because of wrongdoing. Many want to trust that telling people to do the right thing will work. Many do not like rule-based systems. Methodologies other than compliance work for 99 per cent of employees, but it is the 1 per cent of employees who will cause you millions of dollars in fines, set your reputation back, and cause your company to lose the confidence of customers and potential partners.

A compliance and ethics programme has the best chance of preventing, finding and fixing problems. Anything less leaves you vulnerable.

This page intentionally left blank

PART II

The main offences

10

The Bribery Act 2010: implications for global businesses and individual directors

John P Rupp, Partner, Robert Amaee, Counsel, and Alexandra Melia, Associate
Covington & Burling LLP

The message is stark: a commercial organisation that carries on a business or part of a business in the United Kingdom can be convicted of an offence under the UK Bribery Act 2010 if a bribe is paid on its behalf and the organisation is deemed to have failed to implement 'adequate procedures' to prevent bribery.

Commercial organisations that have adopted risk-reduction measures incorporating the recommendations of the US Department of Justice and Securities and Exchange Commission under the US Foreign Corrupt Practices Act (FCPA) already will have satisfied some of the obligations imposed upon them by the Bribery Act. But procedures built on the requirements of the FCPA will not necessarily be deemed to be 'adequate' under the Bribery Act. The reason, in short, is that the substantive requirements of the Bribery Act go beyond those of the FCPA.

In addition to describing the jurisdictional reach of the Bribery Act, this chapter focuses on the practical steps that commercial organisations – particularly those that have built their anti-bribery compliance programmes around the FCPA – will need to consider to take advantage of the 'adequate procedures' defence in the Bribery Act. Also discussed will be some of the key implications for individual directors.

The jurisdictional reach of the Bribery Act

Under Section 12 of the Bribery Act, the offences of bribing another person and being bribed apply to any person or entity having a 'close connection' to the UK, irrespective of whether the acts or omissions forming part of the offence occur in the UK or abroad. Under the Bribery Act, UK companies, UK partnerships, other UK commercial organisations, British citizens, British nationals and individuals who ordinarily are resident in the UK are deemed to have a close connection with the UK.[1]

The offences created by the Bribery Act also apply to non-UK companies, non-UK partnerships and other non-UK commercial organisations if they are carrying on a business, or part of a business, in the UK. In addition, individuals who are neither British citizens nor nationals are covered if an act or omission forming part of the offence takes place within the UK.[2]

Many commercial organisations will be subject to the Bribery Act because of the jurisdiction triggers described above. An even greater

number, however, will be within the Bribery Act's jurisdictional ambit because, under Section 7, they will be considered 'relevant commercial organisations' by virtue of the fact that they "carry on a business, or part of a business, in [some] part of the United Kingdom". Entities that are pursuing primarily or exclusively charitable or educational objectives – or that have a purely public function – will be deemed to be 'relevant commercial organisations' if they engage in commercial activities.

The Bribery Act does not specify what it means to carry on a business, or part of a business, in the UK. The Ministry of Justice's 'Guidance about procedures which relevant commercial organisations can put in place to prevent persons associated with them from bribing' says that, ultimately, it is for the courts to decide on this. The guidance then goes on, however, to describe the UK government's 'intention' in relation to the phrase "carries on a business, or part of a business" in the UK.[3]

The guidance suggests that commercial organisations lacking a demonstrable business presence in the UK will not be caught by the Bribery Act. It states in that connection, rather controversially, that the UK government "would not expect" a mere listing on the London Stock Exchange or, less controversially, possession of a UK subsidiary automatically to subject a non-UK parent to the Bribery Act. It is not at all clear, however, that the Serious Fraud Office (SFO) – the lead enforcement agency for the Bribery Act – will take as limited a view of the jurisdictional reach of the Bribery Act as the Ministry of Justice.[4]

The scope of the Bribery Act

The general offences

Offence of bribing another person

Section 1 of the Bribery Act prohibits a person – whether directly or through an agent – from offering, promising or giving a financial or other advantage to another whenever he or she:

- intends the advantage to induce a person to perform a relevant function or activity improperly
- intends the advantage to reward a person for improper activity
- knows or believes that acceptance of the advantage itself would be improper.

The test for 'improper performance' involves an assessment of whether the person performing the function or activity was expected to do so in good faith or impartially or to act from a position of trust and, in turn, whether that performance was in breach of the 'relevant expectation'.

A 'relevant function or activity' can be performed in the public or private sectors and has been defined broadly to include functions or activities of a public nature, connected with a business, performed in the course of a person's employment or by or on behalf of a group of persons. Such functions or activities can be carried out abroad and do not need to have a connection with the UK.

The 'relevant expectation' is what a reasonable person in the UK would expect. Consequently, when the performance of the function or activity is not subject to UK law, local custom or practice must be disregarded unless it is enshrined explicitly in local legislation, the governing constitution or case law.

Offences relating to being bribed

Section 2 of the Bribery Act prohibits a person from requesting, agreeing to receive or accepting a financial or other advantage:

- intending, as a consequence, that a relevant function or activity will be improperly performed (whether by that person or another)
- when the request, agreement or acceptance is itself improper
- as a reward for improper performance (whether by that person or another) of a relevant function or activity.

It also is an offence where, in anticipation of or in consequence of a person requesting, agreeing to receive or accepting a financial or other advantage, a relevant function or activity is performed improperly by that person or by another person at that person's request or with that person's assent or acquiescence.

The Section 2 offence expressly applies if an agent is used to request, agree to receive or accept a bribe. It is irrelevant whether the bribe is, or will be, for the benefit of the person who requests, agrees to receive or accepts it or for another person. Neither does it matter whether he or she knows or believes that the performance of the relevant function or activity is improper.

The 'relevant function or activity' criteria and 'improper performance' test are the same as those in respect of the Section 1 offence.

Bribery of foreign public officials

Under Section 6 of the Bribery Act,[5] an offence is committed when a person – whether directly or indirectly – offers, promises or gives any financial or other advantage to a foreign public official, or to another person at that official's request or with his or her assent or acquiescence, with the intention of:

- influencing the foreign public official in his or her professional capacity
- obtaining or retaining business or an advantage in the conduct of business, provided that the public official is not expressly permitted, as required by applicable written law, to be influenced in his or her capacity as a public official by the offer, promise or gift.[6]

For the purpose of the Section 6 offence, it is not necessary for the person offering, promising or giving an advantage to know or intend that the foreign public official might act improperly. An intention to influence is sufficient. Officials will be considered to have been 'influenced' if they fail to exercise their functions or seek to use their official position to a particular end, even if acting outside their authority when doing so.

Criminal liability of senior officers

If a commercial organisation commits any of the offences outlined above – and it is proved that the offence was committed with the consent or connivance of a director, manager, corporate secretary or other similar officer – then, under Section 14 of the Bribery Act, the senior officer can be prosecuted alongside the company. Individuals who purport to act as senior officers also may face prosecution under this provision of the Bribery Act.

The application of the Section 14 offence is, however, limited to those who have a close connection to the UK (in other words, individuals who are British citizens, British nationals or are ordinarily resident in the UK).

Failure of commercial organisations to prevent bribery

The Bribery Act creates a new offence for commercial organisations that fail to prevent bribes being paid on their behalf. The Section 7 offence will be committed if an 'associated person' bribes another person to obtain or retain business or an advantage in the conduct of business for a relevant commercial organisation.

An 'associated person' is someone who performs services for or on behalf of a relevant commercial organisation. There is a rebuttable presumption that an employee acts for or on behalf of his or her employer. In other circumstances, this issue will be determined by an assessment of all relevant circumstances, not merely on the nature of the relationship between the person and the organisation.

There is no need for a person performing services on behalf of a commercial organisation – for example, an employee, agent or subsidiary – to have been prosecuted for bribery provided they would be guilty of the offence of bribing another person or of bribing a foreign public official.

The 'adequate procedures' defence

A commercial organisation can defend itself against a charge under Section 7 if it can prove, on the balance of probabilities, that it had in place

'adequate procedures' designed to prevent persons performing services for or on its behalf from engaging in bribery. Unfortunately, the Bribery Act does not define the term 'adequate procedures'.

The guidance issued by the Ministry of Justice discusses the procedures that commercial organisations 'should consider' adopting to combat bribery. It focuses on six high-level principles that are described as being 'outcome focused' rather than 'prescriptive' – stopping short of providing commercial organisations with a detailed recipe for creating an 'adequate procedures' defence. The six principles are as follows:

Proportionate procedures

The guidance states that a commercial organisation's corruption-prevention procedures should be proportionate to the bribery risks that it faces as well as to the nature, scale and complexity of its activities. The guidance suggests that organisations should be permitted to decide whether to adopt standalone anti-corruption procedures or incorporate them into guidelines addressing particular business activities (such as managing a tender process involving a public entity, or recruiting new employees).

However, the procedures that are implemented should provide – according to the guidance – a practical and realistic means of achieving the objectives of the organisation's anti-corruption policy.

Top-level commitment

A commercial organisation's management – the board of directors, senior officers or owners – must be committed to preventing persons acting on the organisation's behalf from engaging in bribery and must foster a corporate culture in which bribery is never tolerated.

Risk assessment

The guidance suggests that organisations should assess the nature and extent of their exposure to the risk that those acting for the organisation – whether employees or others – will engage in bribery. The assessment should be 'informed' and 'documented' as well as be conducted periodically so that it accurately reflects the risks faced by the organisation as its commercial activities change over time.

Due diligence

The guidance urges commercial organisations to mitigate their bribery risk by adopting a proportionate and risk-based approach to the due diligence they undertake in relation to those who act on their behalf.

Communication

The guidance advises that bribery prevention policies and procedures should be "embedded and understood throughout the organisation". That goal should be achieved, according to the guidance, by communicating those policies to employees, business partners and others who act for the organisation through training and other means. It is likely that the manner in which a commercial organisation chooses to communicate its policies will depend on the nature of the risks that it faces, the organisation's size, as well as the scale and nature of its activities.

The guidance also urges commercial organisations to provide a secure, confidential and accessible means for employees and others to request advice, suggest improvements to the bribery prevention regime and raise any compliance concerns.

Monitoring and review

The guidance states that a commercial organisation should monitor and review its bribery prevention policies and procedures periodically – or engage an external expert to conduct such an exercise – to evaluate the effectiveness of its bribery prevention programme and enable the identification and implementation of enhancements that are required to improve the effectiveness of the organisation's controls.

Corporate hospitality and other business expenditures

Concern had been expressed in some quarters that the offences created by the Bribery Act would have the effect of criminalising the provision or acceptance of corporate hospitality. The guidance emphatically rejects that concern, endorsing instead 'reasonable' and 'proportionate' hospitality that seeks to improve the organisation's image, present its products and services or establish cordial business relations. The guidance goes on to state that "it is not the intention of the Bribery Act to criminalise such behaviour".

In determining what is reasonable and proportionate, the guidance proposes taking into account "all of the surrounding circumstances", including "the type and level of advantage offered, the manner and form in which the advantage is provided, and the level of influence the particular foreign public official has over awarding business". It states that "the more lavish the hospitality or the higher the expenditure in relation to travel, accommodation or other similar business expenditures provided to a foreign public official, then, generally, the greater the inference that it is intended to influence the official to grant business or a business advantage in return".

While much of the advice in the guidance is already part of the compliance mantra, commercial organisations that are subject to the Bribery Act should ensure that their policies and procedures on gifts and corporate hospitality are compliant with the principles described above.

Facilitation payments

Facilitation payments will remain a criminal offence under the Bribery Act. While acknowledging the problems faced by commercial organisations in some parts of the world and in certain sectors, the guidance reiterates that there is no exemption – either in the Bribery Act or the laws that it has replaced – for facilitation payments. It cites the OECD's position that such payments are corrosive and that exemptions create artificial distinctions that are "difficult to enforce, undermine corporate anti-bribery procedures, confuse anti-bribery communication with employees and other associated persons, perpetuate an existing 'culture' of bribery and have the potential to be abused".

When a commercial organisation or individual has no alternative but to make a payment to "protect against loss of life, limb or liberty", the guidance states that "the common law defence of duress is very likely to be available". Further, it stresses that it is a matter for prosecutorial discretion whether to pursue an organisation for offering or making a facilitation payment.

Dealing with differential treatments of facilitation payments in the FCPA and the Bribery Act will be vexing for many commercial organisations. Demands for the payments are, of course, a fact of life in many countries – and a refusal to acquiesce to such demands can, in some circumstances, prevent a commercial organisation from doing business in such countries. Fortunately, both the guidance and senior officials at the SFO have recognised that fact. The SFO has announced as a consequence a nuanced policy on the making of facilitation payments while describing a series of steps that commercial organisations subject to the Bribery Act should take to reduce and ultimately eliminate the making of facilitation payments.[7]

Penalties

The Bribery Act increases the maximum penalties that can be imposed for the commission of a bribery offence to:

- ten years' imprisonment, coupled with an unlimited fine, for an individual
- an unlimited fine for a commercial organisation.

The UK courts increasingly are prepared to impose custodial sentences on corporate officers who become involved in corruption. For example, in passing sentence in the case of Charles Forsyth, David Mabey and Richard Gledhill, former

executives at engineering firm Mabey & Johnson, Judge Rivlin QC stated: "When a director of a major company plays even a small part [in a bribery scheme], he can expect to receive a custodial sentence." [8]

The decision of Lord Justice Thomas in *R v Innospec Ltd* (2010) also demonstrated the serious view of corruption taken by the UK courts. In his sentencing remarks, Lord Justice Thomas characterised the corruption of foreign government officials or ministers as "at the top end of serious corporate offending both in terms of culpability and harm".

He went on to state that while there may be reason for differentiating between the US and UK in the custodial penalties imposed for corruption, "there is every reason for states to adopt a uniform approach to financial penalties for corruption … so that the penalties in each country do not discriminate either favourably or unfavourably against a company in a particular state".

There is a real possibility that commercial organisations convicted under the Bribery Act will face mandatory exclusion from competing for government contracts within the European Union. The Public Contracts Regulations 2006 and the Utilities Contracts Regulations 2006 currently require companies convicted of, among other things, a corruption offence to be automatically and permanently debarred from competing for public contracts across the EU. Companies convicted of the corporate offence of failing to prevent bribery also may face exclusion, although this is discretionary.

Implications for insurance coverage

Companies and senior managers who routinely purchase director and officer liability insurance (D&O) should talk with their underwriter to ensure that their policies provide cover for any investigations, prosecutions or civil claims that may arise under the Bribery Act. Absent such discussions, commercial organisations may well find their D&O insurance does not cover bribery-related offences.

When D&O cover is obtained, it should address the possibility of a company's senior officers being found liable under Section 14 of the Bribery Act for consenting or conniving in the commission of a bribery offence.

Consideration also should be given to addressing the corporate offence of failing to prevent bribery. If a commercial organisation cannot prove that it had adequate procedures to prevent bribery, the directors may face civil claims by shareholders alleging a failure of corporate governance.

Underwriters are likely to respond to increased demand for D&O policies that insure against breaches of the Bribery Act by requiring commercial organisations to have implemented adequate compliance procedures before the policies can be issued or renewed. The absence of such procedures will, at the very least, increase the premiums demanded by underwriters. There also is a possibility that coverage would not be available at all.

Moving beyond the FCPA

Because the FCPA does not cover commercial bribery, many companies subject to the FCPA have not developed procedures that combat behaviour other than the bribery of foreign public officials.

So far as commercial bribery is concerned, the questions that will be presented include, among many others, whether more lavish hospitality can be provided to a representative of another business entity than to a government official. In relation to facilitation payments, many such companies have stopped well short of prohibiting them. Policies and procedures containing such limitations will be, almost by definition, inadequate under the Bribery Act.

Commercial organisations that are subject to the Bribery Act will need to grapple, sooner rather than later, with the practical implications of extending their anti-bribery policies and procedures to cover commercial bribery and deal appropriately with facilitation payments. Failing to do so will leave an organisation at risk of not being able to rely upon the 'adequate procedures' defence in the Bribery Act.

11

US Foreign Corrupt Practices Act versus the UK Bribery Act: a perspective from both sides of the Pond

Lista M Cannon, Partner (London), and Richard C Smith, Partner (Washington DC)
Fulbright & Jaworski LLP

Bribery was costing the world US$1 trillion a year during the last decade, according to figures from the World Bank, but in parts of the world the counter-offensive has been stepped up. The United States has been using the US Foreign Corrupt Practices Act (FCPA) to take increasingly significant enforcement action against global organisations that engage in corrupt activity. The UK has followed, with the introduction of the Bribery Act providing a potentially powerful new weapon in the armoury of the authorities. Behind the scenes, UK and US regulators are co-operating on an unprecedented scale.

Against this backdrop, while some key differences exist between the US and UK frameworks, businesses must adopt a global approach to compliance.

US anti-corruption legislation and enforcement

The FCPA is enforced by the US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC). Individuals and companies that violate the FCPA may be subject to civil and criminal liability.

FCPA anti-bribery provisions

These apply to: all companies listed on US stock exchanges or subject to SEC reporting requirements; all US companies, citizens or residents, whether they act within or outside the United States; all companies or individuals that execute any part of a bribery scheme from within the US; and all officers, directors, employees or agents of the above. Under the FCPA, an actual payment is not required to trigger the Act, whose essential anti-bribery provisions prohibit the payment, or offer, promise or authorisation of a payment:

- **of money or anything of value**. The term 'anything of value' is broad and may include: gifts – for example, a holiday; charitable contributions or donations, say to the charity of a foreign official's wife; in-kind services or goods; anything else of value, such as tuition, a loan, travel upgrades, dinner or entertainment
- **to any foreign official, any foreign political party or official, or candidate for foreign political office, or official of public international**

organisations. For the purposes of the FCPA, a 'foreign official' means an official of a non-US public body. An official may include: an officer or employee of any government, whether national, state, provincial or local; employees of any department or agency of a non-US government, such as an energy ministry or customs service; employees of any state-owned or state-controlled business, such as an oil company; employees of any public international organisation, such as the World Bank or United Nations

- **to any person while 'knowing' that the money, or thing of value, will be passed on to these officials or entities**. Such 'middle men' may include agents, consultants or other third parties. The word 'knowing' carries speech marks because actual knowledge is not required to trigger the Act. As long as the person offering or giving the item of value to the third party has a firm belief that ultimately it will be given to a foreign official or others identified above, that person acts knowingly under the FCPA
- **with corrupt intent**. There must be an aim to induce the official to misuse his or her position. The intent to make the payment is relevant; not the intent to violate the FCPA
- **to assist in obtaining or retaining business, or a business advantage or directing business to any person**. This could include reducing taxes or customs duties, so lowering a company's overall expenses in a particular market.

Accounting provisions

The FCPA's accounting provisions require companies that register securities or file periodic reports with the SEC – for example, non-US companies that trade American depositary receipts on US exchanges – to keep accurate books and records and maintain an adequate system of internal accounting controls.

Limited exception

The FCPA makes a limited exception for 'facilitating payments' made to secure 'routine governmental action'. However, these payments must be small, reasonable and well-documented. Facilitating payments are illegal under the laws of most countries. In practice, this exception is interpreted very narrowly by US enforcement authorities and, as a result, many US companies have either severely limited or expressly prohibited them in their compliance policies and procedures.

Affirmative defences

A payment, gift, or offer of something of value may be exempt if it was lawful under the written laws of the foreign country. It may also be exempt under the FCPA if deemed to be a 'reasonable and bona fide expenditure' (such as travel and lodging expenses) that is directly related to the demonstration, promotion or explanation of the company's products or services, or the execution of a contract with a foreign government or agency.

The US approach to enforcement

The DOJ and SEC are seeking increasingly large penalties for FCPA violations. In 2010, nearly US$2 billion was levied against companies for FCPA-related offences, primarily in the engineering and energy sectors. US regulators have also taken significant action against individuals, leading to large financial penalties and lengthy jail terms.

The FCPA is a top priority for the DOJ and SEC, and the number of actions in the past five years has increased exponentially. The US enforcement authorities continue to seek voluntary reports from companies, but have recently taken a more proactive stance, using wire taps and 'sting' operations in one recent high-profile case. They have also sent letters to companies following voluntary reports from suppliers or competitors in a given industry, an example being the investigation of the oil and gas sector.

Whistleblowers have also contributed to increased enforcement. In 2010, the US government passed the Dodd-Frank Act, which

Top 10 corporate FCPA penalties

Sector	Company HQ	Penalty	Year
Transport	Switzerland	$81.8m	2011
Pharmaceutical	US	$70m	2011
Defence/ aerospace	UK	$400m	2010
Energy	Netherlands/ Italy	$365m	2010
Engineering	France	$338m	2010
Engineering	Japan	$218.8m	2010
Automotive	Germany	$185m	2010
Telecoms	France	$137m	2010
Energy	US	$579m	2009
Engineering	Germany	$800m	2008

Source: SEC

includes provisions to protect and incentivise whistleblowers who report potential violations of US securities laws, including the FCPA. In particular, the Dodd-Frank Act:

- protects whistleblowers from retaliation by employers
- rewards whistleblowers "who voluntarily provided original information to the [SEC] that led to the successful enforcement" of securities laws
- entitles whistleblowers to a maximum of 30 per cent of monetary sanctions exceeding US$1 million that the government recovers as a result of the assistance.

In May 2011, the SEC adopted final rules implementing the Dodd-Frank whistleblower programme. The rules do not require whistleblowers to report potential violations internally before reporting to the SEC, but whistleblowers may be eligible for a larger award if they report first through internal company procedures.

The DOJ and SEC continue to stress the importance of co-operation and the benefits of self-reporting potential FCPA violations. According to the enforcement authorities, a company's co-operation can lead to decreased monetary penalties, a non-prosecution agreement or deferred prosecution agreement, and/or the ability to enhance its compliance programme without the imposition of a monitor. Deferred prosecution agreements, long used by the DOJ, are a new tool for the SEC. It signed its first-ever corporate agreement in May 2011.

UK anti-corruption legislation and enforcement

The Bribery Act, which came into force on July 1, 2011, sets out four main offences:

- **giving, promising or offering a bribe**
- **requesting, agreeing to receive or accepting a bribe**. A bribe may be a 'financial or other advantage'. The Act targets circumstances in which the bribing party intends to bring about or reward improper performance of a function or activity
- **bribing foreign public officials**. Into this category fall officials from (non-UK) governments, public agencies, international organisations and the judiciary. An offence will be committed even if the bribe is paid to a third party at the request or direction of the foreign public official
- **the corporate offence of failing to prevent bribery by 'associated persons'**. It is a defence if a commercial organisation has 'adequate procedures' in place to prevent bribery and corruption by persons associated with the company.

A corporate body guilty of an offence will be subject to an unlimited fine. An individual found guilty of an offence will be subject to an unlimited fine or a jail sentence of up to ten years, or both.

Only eight weeks after the coming into force of the Bribery Act, the Crown Prosecution Service announced the commencement of the first

prosecution under the Act. A UK court administrative clerk is alleged to have requested and received a bribe in exchange for influencing the course of criminal proceedings.

Adequate procedures

Guidance published by the UK Ministry of Justice on March 31, 2011 states that businesses should adopt a 'risk-based approach' in establishing 'adequate procedures' that are 'proportionate to risk' to prevent bribery within their organisation. The guidance sets out six high-level, non-prescriptive principles, together with commentary and examples, which should inform organisations putting in place procedures to prevent bribery:

- proportionate procedures
- top-level commitment
- risk assessment
- due diligence
- communication (including training)
- monitoring and review.

Jurisdictional scope of the corporate offence

A relevant commercial organisation will be strictly liable where it fails to prevent bribery by a person associated with the organisation. The Bribery Act defines a 'relevant commercial organisation' as a body or partnership incorporated or formed in the UK irrespective of where it carries on a business, or a body or partnership that carries on a business or part of a business in the UK irrespective of the place of incorporation or formation.

The application of the corporate offence to overseas companies will depend on the extent to which organisations have a 'demonstrable business presence in the UK'. While the guidance suggests that the trading of a non-UK company's shares on the London Stock Exchange, or the simple fact of having a UK subsidiary, would not in themselves amount to carrying on business in the UK, it would be for the UK courts to determine whether an organisation 'carries on a business' in the UK, taking into account the particular facts of individual cases.

Associated persons

The liability of commercial organisations for the corrupt activities of 'associated persons' is a key theme of the Bribery Act, which defines an 'associated person' as one who 'performs services' for or on behalf of the relevant commercial organisation.

However, the guidance makes certain distinctions. In the context of joint venture arrangements, for example, it suggests that a commercial organisation benefiting indirectly, through its investment or ownership, from a bribe paid by an employee or agent of a joint venture entity on behalf of that entity is unlikely to be liable under the Act. Further, according to the guidance, "liability will not accrue through simple corporate ownership or investment, or through the payment of dividends or provision of loans by a subsidiary to its parent".

Hospitality and promotional expenditure

The guidance recognises that such expenditure is an established part of doing business, and states that the UK government will not seek to use the Bribery Act to prohibit 'reasonable and proportionate' hospitality and promotional or other similar business expenditure.

Facilitation payments

Unlike under the FCPA, facilitation payments – small sums paid to facilitate routine government action – are not exempt from prosecution under the Bribery Act. In determining whether to bring a prosecution for facilitation payments, the Serious Fraud Office (SFO) or the Director of Public Prosecution (DPP) will examine factors such as:

- the prevalence of large or repeated payments
- payments that are planned for or accepted as part of a standard way of conducting business
- payments that may indicate an element of active corruption of the official
- a clear breach of an organisation's procedures on facilitation payments.

The SFO/DPP will weigh these factors against those tending against prosecution, including where:

Anti-corruption enforcement by the UK authorities

Sector	Sanction	Date
Publishing	Civil recovery order: £11.2m, compliance monitor	July 2011
Insurance	£6.9m fine for anti-bribery systems and controls failures*	July 2011
Healthcare	Civil recovery order: £4.8m	Apr 2011
Engineering	£7m fine	Feb 2011
Defence/ aerospace	£500,000 fine (part of £30m global agreement)	Dec 2010
Energy	$12.5m fine (part of $40m global settlement). 3-year US/UK compliance monitor	Mar 2010
Engineering	Civil recovery order: £5m, compliance monitor	Oct 2009
Engineering	£6.6m fine, compliance monitor	Sep 2009
Insurance	£5.25m for anti-bribery systems and controls failures*	Jan 2009
Construction	Civil recovery order: £2.25m, compliance monitor	Oct 2008
Security	Employee and an official of Uganda: suspended sentence and 12 months' imprisonment	Sep 2008

Enforcement actions brought by SFO, except for

- there is a single small payment
- the payment(s) comes to light as a result of a genuinely proactive approach involving self-reporting and remedial action
- a commercial organisation has a clear and appropriate policy setting out procedures that an individual should follow
- the payer was in a vulnerable position arising from the circumstances in which the payment was demanded.

A prosecution will usually take place unless the prosecutor is sure there are public-interest factors tending against prosecution that outweigh those tending in favour.

The UK approach to enforcement

The Bribery Act provides a powerful new regulatory tool for the SFO. On the release of the guidance on March 31, 2011, Richard Alderman, director of the SFO, commented that the Act confirmed the UK regulator's "commitment to helping to eradicate bribery from business practices. The aim is to help ensure that ethical businesses do not lose out to others that use bribery and corruption to win contracts."

The SFO has also maintained that it remains "determined to go after senior corporate executives who break the law". While the level of fines lies far behind those imposed by US regulators, the SFO has already levied some significant financial penalties in a relatively short period, in particular in the engineering sector.

Significantly, there is no obligation under English law for a party to report incidents of bribery and corruption to the authorities, including the police or SFO. However, in July 2009 the SFO published guidance, 'Approach of the Serious Fraud Office to Dealing with Overseas Corruption', which signalled its intent to reach successful outcomes through a co-operative approach.

The SFO guidance recognises that self-reporting may not be appropriate in every case, but an active decision not to self-report may increase the prospect of a criminal sanction. The

guidance indicates that where possible an agreed civil solution will be extended to those who self-report, in preference to a criminal prosecution, although civil settlements will not be available where board members were involved personally in the corrupt activities. Once a satisfactory conclusion to an investigation has been reached, the SFO will consider the following factors in connection with civil proceedings:

- restitution by way of civil recovery
- independent monitoring, with an agreed and proportionate scope
- an agreed programme of culture change and training
- dealing with individuals involved in the wrongdoing
- the possible involvement of the SFO in settling with other domestic and overseas regulators
- a public statement agreed between the company and the SFO to provide public transparency.

In December 2009, the SFO's director advised that, in deciding whether to pursue criminal or civil proceedings in bribery and corruption cases, the SFO will consider factors including:

- the severity of the wrongdoing
- whether it is an isolated incident or there have been other examples
- whether the activity is systematic and part of an established business practice
- whether continuing board members have profited personally from the activity
- whether there have been previous warnings to the company about inadequate processes
- whether the company reported the issue within a reasonable time, and whether the report was sufficiently detailed and complete.

The SFO does not yet have the power to force the appointment of a compliance monitor as part of a settlement. However, the installation of a monitor has been a feature of a number of recent UK cases.

The SFO will consider factors including the 'genuine commitment' of a company to an anti-corruption culture, and public and market expectation. Where the issues are international, the SFO will engage with its counterparts in relation to the proposed appointment.

Compliance practicalities

While there are some key differences between the FCPA and the Bribery Act, commercial organisations should endeavour to create, operate and maintain effectively global compliance programmes, tailored to the risks associated with the jurisdictions and sectors in which they do business. The programmes should include:

- **procedures that reflect the full commitment of the organisation and its board to the eradication of corrupt activities**. These will include: strong and visible support and commitment from senior management; the vesting of responsibility for compliance and anti-bribery procedures with one or more senior board members, together with adequate autonomy, resources and authority; and mechanisms for the oversight of ethics and compliance procedures, including reporting to internal board committees
- **procedures to assess the risk of bribery in the light of a company's circumstances** with particular regard to foreign bribery risks in relevant geographical and industry sectors
- **procedures setting out the considerations that company personnel must take into account when engaging third-party representatives**. These could include a due-diligence questionnaire in relation to potential business partners, and a process by which the personnel responsible for managing a relationship with prospective partners review the due-diligence information and seek approval; a compliance certificate to be completed by company personnel concerning conduct during the course of a business

Material differences between the FCPA and the Bribery Act

- Unlike the FCPA, the Bribery Act does not allow 'facilitation payments'.
- The Bribery Act applies to corrupt dealings between private companies and private individuals, as well as dealings with governments and public sector entities. In the US, the enforcement authorities are using other laws – such as the Travel Act – to address commercial bribery.
- The Bribery Act extends criminal liability to the receiver of the bribe, as well as the giver of the bribe, unlike the FCPA.
- The Bribery Act does not include an FCPA-style 'books and records' offence, but UK businesses are subject to requirements for accurate accounting contained in other legislation, including the Companies Act 2006.
- The FCPA does not include a strict liability corporate offence of failing to prevent bribery and its related 'adequate procedures' defence.

relationship; a procedure for the approval of business courtesies, hospitality, travel and accommodation; an annual personnel questionnaire concerning conduct; and approved contractual provisions for the engagement of prospective partners, including anti-corruption representations and warranties, audit rights and termination rights

- **procedures to prevent and detect corruption** relating to: gifts; business courtesies, hospitality and expenses; travel and accommodation; political contributions; charitable donations; facilitation payments; goodwill payments and sponsorship – by the company and/or its personnel; solicitation and extortion; and record-keeping
- **procedures to implement company policy** throughout the corporate structure to all levels of employee
- **procedures to extend company standards**, where appropriate and subject to contractual arrangements, to third parties (such as agents, intermediaries, contractors and joint venture partners), including procedures as to how a company should go about seeking reciprocal commitments
- **procedures to ensure effective communication and training**, including: a properly articulated and visible corporate policy; proper training of personnel with appropriate reference to risk; the effective dissemination of the procedures throughout the organisation's businesses, including subsidiaries and joint venture entities; appropriate measures to encourage and provide positive support for the identification and reporting of bribery issues; effective measures to provide guidance for directors, employees and business partners; and the implementation, communication and use of appropriate disciplinary procedures for breaches of anti-bribery legislation and compliance procedures
- **procedures to monitor and review the proper implementation of the company's compliance efforts**, taking into account relevant developments in the field, and evolving international and industry standards.

The underlying reasoning behind the £6.9 million fine imposed on a leading insurance broker by the Financial Services Authority (FSA) in July 2011, while levied pursuant to a regulatory framework and not under the Bribery Act 2010, provides a number of important indicators as to how the SFO may assess whether procedures are 'adequate'. In short, the mere production of

policies and procedures, without effective implementation, monitoring, review, communication and oversight, will not suffice.

A common approach?

Key differences exist between the US and UK legislative regimes and regulatory frameworks (see the box opposite). That said, increasingly common approaches and enhanced co-operation between the US and UK regulators signal that businesses operating in global markets must pay close attention to both.

A number of common themes have emerged between the US and UK's regulatory approaches:

- proactive and significant enforcement against corporations and individuals
- the promotion of transparency and co-operation between businesses and regulators
- the development of new tools to assist enforcement activities.

The convergence of approach has been supported by unprecedented levels of co-operation between US, UK and international regulators. Cases are being passed from one to another, information and evidence is being shared, and methodologies are being discussed. The SFO and DOJ, for example, conduct regular meetings and have formalised their relationship in a memorandum of understanding.

Co-ordinated international raids, investigations and prosecutions are now a reality. Several high-profile global settlements have resulted, although companies must negotiate with each government agency or regulator.

This common approach, leading to common solutions, albeit with reference to differing legislative frameworks, is here to stay.

12

Cartels: competing within the rules, understanding the boundaries of fair competition

Nicole Kar, Partner, and Kirsten Donnelly, Associate Linklaters LLP

Under the Enterprise Act 2002, it is a criminal offence for individuals to dishonestly engage in cartel arrangements – legislation that was introduced in the UK to enhance deterrence by supplementing the civil prohibition regime under the Competition Act 1998. It was anticipated that the offence would provide both US-style prosecutorial muscle and enhance civil leniency programmes, encouraging whistleblowing in relation to unlawful cartel activity.

The UK's criminal cartel enforcement regime was built on an institutional structure in which the Office of Fair Trading (OFT) would manage initial investigative enquiries and the criminal immunity regime, and the Serious Fraud Office (SFO) would conduct investigations and prosecutions for cases falling within its acceptance limits. Where cartel arrangements are made involving individuals located outside the UK, criminal proceedings may be brought if the agreement has been implemented in whole or in part in the UK. Individuals outside the UK may be subject to extradition proceedings initiated by the UK government under the Extradition Act 2003.

Criminal cartel conduct

Overview of the offence

The cartel offence is set out in Part 6 of the Enterprise Act, with Section 188 establishing the elements of the offence. The section provides that an individual is guilty if he dishonestly agrees with one or more other persons that undertakings will engage in one or more of the following prohibited activities:

- price fixing
- limitation of supply or production
- market sharing
- bid rigging.

The activities must relate to the supply or production of a product or service in the UK and the cartel offence only applies to 'horizontal' agreements – that is, to undertakings at the same level of the supply chain. In addition, agreements

fixing prices, limiting supplies or limiting production must be reciprocal between at least two undertakings. The offence may be committed even if the agreement is not implemented or the individuals involved do not have the authority to act on behalf of their companies.

The test for dishonesty was established in England and Wales in the case of *R v Ghosh* (1982). This is a two-stage test involving both an objective and a subjective element. Juries will be required to ask themselves:

- whether what was done was dishonest by the ordinary standards of reasonable and honest people, and
- if so, whether the defendant realised his actions were dishonest according to those standards.

A person will only be dishonest if the jury finds beyond a reasonable doubt that the answer to both questions is in the affirmative.

Whether the common law criminal offence of conspiracy to defraud could extend to prosecuting individuals and companies involved in cartels was tested in 2008 in the *Norris* extradition case[1] and the *Goldshield Group plc* case (commonly known as the SFO's Generic Drugs Case). The House of Lords held that prior to 2003 (the coming into effect of the cartel offence) there was no "intrinsic unlawfulness and dishonesty merely in taking part in a secret cartel". Thus mere price fixing would not constitute a criminal offence. However, there could be a charge under conspiracy to defraud if the price fixing was accompanied by aggravating features such as fraud, misrepresentation, violence, intimidation or inducement of breach of contract. The focus of this chapter is on the application of the statutory offence.

Powers of investigation

The SFO and OFT may each bring prosecutions in respect of the cartel offence in England, Wales or Northern Ireland. No other body is permitted to commence proceedings, except with the consent of the OFT.[2]

Under the Criminal Justice Act 1987, the SFO has the power to investigate any offences involving serious or complex fraud. It will typically deal with prosecutions where there is likely to be widespread public interest, a significant international dimension and where highly specialised market or commercial knowledge is required. The SFO will only become involved in cases when the financial consideration is in excess of £1 million.

The OFT may commence a criminal investigation where there are reasonable grounds for suspecting that the cartel offence has been committed. However, it may only use its criminal powers of investigation for the cartel offence and not for any breaches of the civil prohibitions. Acting in excess of its powers could give rise to civil remedies against the OFT, and to the evidence gathered being excluded.

Where the OFT commences a criminal investigation, it may:

- require the person under investigation, or any other person who it has reason to believe has relevant information, to answer questions on any matter relevant to the investigation
- require the production of documents that appear to relate to the investigation
- seek to enter premises under a warrant.

The powers of the OFT when conducting criminal investigations do not extend to information and documents that are the subject of legal professional privilege. The SFO is also subject to the same restriction under Section 2 of the Criminal Justice Act.

Relationship between criminal enforcement under the Enterprise Act and civil enforcement under the Competition Act

The OFT's powers under the Enterprise Act operate in parallel with those under the Competition Act, which imposes civil sanctions on agreements that restrict, distort or prevent competition in the UK or the European Union

(the Chapter 1 prohibition and the prohibition in Article 101 of the Treaty on the Functioning of the European Union).

In practice the OFT will not generally know, when it receives a complaint or other information in respect of a potential cartel, whether it will ultimately take enforcement action against an individual under the Enterprise Act and/or an undertaking under the Competition Act.

In its guidance, 'Powers for Investigating Criminal Cartels', the OFT states that after gathering sufficient evidence, it will consider the possibility of instituting an administrative procedure under the Competition Act against companies at the same time as individuals are being investigated under the Enterprise Act. If the OFT wishes to pursue a Competition Act case where it (or the SFO) also wishes to commence proceedings under the cartel offence against any of the individuals involved, then the OFT will consult with the SFO on timing and will not commence administrative proceedings before speaking to the SFO.

In practice it is likely that any potential criminal prosecution will take precedence over any administrative action. The Competition Act case will be stayed pending either the conclusion of the criminal proceedings or a decision not to prosecute.

Parallel UK and EU investigations

In addition, the OFT may use its powers under the Enterprise Act to prosecute individuals involved in EU-wide cartels implemented in the UK. Potential infringements of Article 101 may be subject to investigation by the European Commission (EC) or by another national competition authority or by the OFT.

As Article 101 and the cartel offence under the Enterprise Act are aimed at different legal persons (the cartel offence at dishonesty by individuals and Article 101 at anti-competitive behaviour by undertakings), the OFT considers that the investigation or prosecution of an individual under the cartel offence would not oblige it to apply Article 101 as well, even where the cartel activity has cross-border effects within the EU.

However, in many cases there may be parallel investigations in relation to the UK cartel offence and Article 101. The OFT has stated in its guidance that it would work with the EC (and other national competition authorities) to co-ordinate the progress of their investigations. But the EC's jurisdiction only extends to the imposition of civil penalties on undertakings; it does not have the power to impose civil or criminal penalties on individuals.

Exposure to other potential criminal proceedings

As described above, where cartel arrangements are made involving individuals located outside the UK, criminal proceedings may be brought if the agreement has been implemented in whole or in part in the UK. The cartel offence may be subject to extradition proceedings initiated by the UK government, and prosecutors would have to demonstrate – say if they were seeking to extradite individuals in the US to the UK – that (among other things) there is 'probable cause' for believing that the person sought committed the cartel offence.

Similarly, where an individual engages in a cartel arrangement in the UK, it is possible that he may also commit an offence in other national jurisdictions where the cartel arrangement is implemented or gives rise to cross-border effects. For example, Section 1 of the Sherman Act in the US prohibits agreements that unreasonably restrain trade. Violation of Section 1 is subject to both criminal and civil enforcement by the Department of Justice (DOJ). In practice, criminal investigations generally focus on suspected collusive conduct among competitors, such as agreements to fix prices, rig bids or share markets.

The Antitrust Division of the DOJ will investigate and prosecute cartel arrangements affecting US markets. International cartels have accounted for the majority of the fines imposed by the DOJ: as of April 28, 2011, of the 82 companies that have paid fines of US$10 million or more, 94 per cent were foreign corporations. In the financial year 2010, 78 per cent of criminal cartel

defendants were sentenced to a term of imprisonment.

The US-UK Extradition Treaty permits extradition in relation to any offence, provided the conduct amounts to an offence both in the UK and in the US, and can be punished in both jurisdictions with a custodial sentence of at least one year. This encompasses the cartel offence under the Enterprise Act. In 2008, the House of Lords held that the fact that the criterion of dishonesty (a requirement for the UK offence) is not an element in respect of the US offence was not a bar to extradition.[3]

Prosecution history

Eight years after the introduction of the criminal cartel enforcement regime, two cases have come to court and others are under investigation.

The 'Marine Hoses' case[4]

The first criminal cartel prosecution under the Enterprise Act was the *Marine Hoses* case in 2008 involving a global cartel said by the prosecution to have involved UK contracts alone worth £17 million. Following an investigation, the EC concluded that, between 1986 and 2007, six producers of marine hoses operated a global cartel. It was alleged that the companies met regularly at several locations in Europe, East Asia and the US to fix prices, allocate bids and markets, and exchange sensitive information. (Marine hoses are used by customers in the oil and defence industries to transport oil and petroleum products between tankers and storage facilities.)

Marine Hoses was prosecuted by the OFT in co-operation with the DOJ, with whom the defendants had entered into a plea bargain arrangement. This was a controversial co-prosecution and plea arrangement that drew some critical comment from the Court of Appeal. The defendants had bound themselves not to ask for or appeal any sentence from the UK courts which was less than that imposed by the US courts. Lady Justice Hallett, in giving the judgment of the court, said:

"It follows that this court has not had the benefit of the kind of argument from counsel to which it is accustomed … we have our doubts as to the propriety of a US prosecutor seeking to inhibit the way in which counsel represent their clients in a UK court, but having heard no argument on the subject, we shall express no concluded view."

In *Marine Hoses*, three individuals were sentenced to between 30 and 36 months' imprisonment, reduced to 20 to 30 months on appeal. In its judgment, the Court of Appeal made it clear that the original and substitute sentences should not be treated as guideline sentences.

The BA case[5]

This case came to the OFT's attention when Virgin Atlantic Airlines (Virgin) blew the whistle on allegedly anti-competitive agreements that it said had been reached between certain of its employees and employees of British Airways (BA). Pursuant to the OFT's guidelines, Virgin secured immunity from the OFT in relation to civil and criminal penalties for its current and former employees. BA secured qualified leniency (a reduction in civil penalty) by admitting infringements of Chapter 1 cartel activity after the OFT's investigation had begun, but did not secure criminal immunity for its employees.

On 1 August 2007, the OFT announced it would impose a penalty of £121.5 million on BA for its participation in the alleged cartel. It indicated that it was continuing to investigate employees of BA using its criminal powers and froze the civil investigation prior to issuing a statement of objections so as to avoid prejudice to any criminal prosecutions. Four BA employees were charged with cartel offences on 7 August 2008.

All four defendants entered pleas of 'not guilty' on July 13, 2009, thus setting the scene for the first full criminal cartel trial in the UK.

After the commencement of the trial, however, it emerged that a large volume of electronic documentary evidence from Virgin's files (approximately 70,000 emails), which Virgin

had previously led the OFT to believe had been irreparably corrupted, could in fact be recovered. They were then disclosed to the defence.

One of the recovered emails revealed that at least one of the decisions taken by Virgin to increase its passenger fuel surcharge, which the OFT had said resulted from the alleged cartel, was actually made prior to the phone conversation during which the OFT alleged BA had suggested that Virgin should increase its surcharge. In light of the large volume of evidence that had been uncovered at such a late stage, the OFT took the view that it was unrealistic to seek an adjournment of the trial, and so on May 10, 2010, it indicated that it would offer no evidence against any of the four defendants. Accordingly, the jury acquitted the four men and so ended the first contested criminal cartel case in the UK.

Current cases

Despite the collapse of the BA case, the criminal prosecution of individuals involved in cartels remains very much alive. The OFT is currently investigating (publicly at least) two potential criminal cartels, one involving commercial vehicle manufacturers and one in relation to the automotive sector.

Proposed reforms

The OFT's powers to investigate cartels under criminal law appear to have survived a potential reallocation of prosecutorial responsibilities via the mooted (and now shelved) Economic Crime Agency. In terms of the substantive offence, the government is currently consulting on amendments such as the removal of the 'dishonesty' test, as part of wider reforms to the competition law regime in the UK. The consultation document lists a number of possible reform options, predicated on the assumption that the offence, as currently drafted, does not operate effectively.

Consequences of a breach: the sticks

Under the cartel offence, the main drivers of compliance include the risk of imprisonment, the imposition of disqualification orders, and orders for the recovery of the proceeds of crime.

Penalties

The cartel offence carries a maximum term of imprisonment of five years and/or an unlimited fine (depending on the court in which the case is heard). With regard to the conspiracy-to-defraud offence, Section 12 of the Criminal Justice Act provides for a maximum penalty of ten years' imprisonment and/or an unlimited fine.

Director disqualification

Where an undertaking has infringed any civil UK or EU competition law prohibitions, each of its directors could be served with a disqualification order (for a period of up to 15 years) where their conduct makes them unfit to be concerned in the management of a company. Such 'unfitness' may come from involvement in the cartel or negligent oversight of the relevant activities.

Although the OFT has had the power to impose competition disqualification orders (CDOs) since 2003, no orders have been imposed to date. In the *Marine Hoses* case, the defendants were each disqualified for a period of between five and seven years under the 'general' provisions of the Company Directors Disqualification Act (CDDA) 1986, which permit an order to be made as a result of an individual's conviction for an indictable offence (in this case the cartel offence), rather than the CDO provisions of the CDDA.

In June 2010, the OFT issued revised guidance on its powers to apply for CDOs under the CDDA. It said the new guidance was designed to maximise the deterrent effect of the orders, which includes expanding the circumstances in which they can be sought and increasing the likelihood that the OFT will seek a CDO in relation to directors who did not have actual knowledge of the breach of competition law in question but 'ought' to have known. In exceptional circumstances, it may apply for a CDO notwithstanding that a competition law breach has not been established by a prior regulatory

decision or court judgment, and also in cases where no fine has been imposed. In June 2011, the OFT released guidance for directors on their responsibilities under competition law.

Confiscation of proceeds

The Proceeds of Crime Act 2002 gives the crown court the power to make confiscation orders relating to offences committed after March 23, 2003. Where an individual has been convicted or sentenced, if the court believes it is appropriate to do so, on the balance of probabilities, it must determine whether the defendant has benefited from criminal conduct. If the court decides in the affirmative, it must determine the amount that can be recovered and make an order requiring the individual to pay it. If the victim(s) also intends to sue the defendant for damages or other loss in a civil claim, the court must treat this as a power rather than a duty.

Compliance: the carrot

The OFT may grant immunity from prosecution to individuals who inform competition authorities of cartel conduct and who then provide full co-operation in respect of any investigation. With regard to the cartel offence, immunity from prosecution will be granted in the form of a 'no-action letter' issued by the OFT under Section 190 of the Enterprise Act. The letter will prevent a prosecution from being brought against an individual in England and Wales or Northern Ireland in respect of the cartel offence, except in circumstances specified in the letter.[6]

In the context of criminal investigations, in addition to other factors, the extent to which the defendant's conduct was contrary to the guidelines laid down in a company compliance manual will be an important factor.[7] Best practice in competition law compliance includes obtaining management commitment and demonstrating this to staff; and identifying risks and appropriate compliance activities – for example, training, accessible legal advice and guidance, implementing mechanisms whereby employees are able to report concerns confidentially, and conducting compliance audits.

13

Insider trading: knowing the rules and remaining within them

Steven Francis, Partner, and Richard Burger, Partner
Reynolds Porter Chamberlain LLP

Insider dealing is not a modern phenomenon. For as long as there have been markets, there have been individuals taking advantage of their privileged access to information to make inordinate profits. Perhaps the most famous such example is the (much contested) claim that Nathan Rothschild was able to use his early knowledge of Wellington's victory at Waterloo to manipulate the stock exchange to his advantage, amassing substantial gains.

For all the attention paid to the offence of insider trading in recent years, it was by no stretch of the imagination the cause of the financial crisis and it is likely that, with takeover activity muted, insider dealing is probably far from being a prolific or regular activity. Indeed, a recent report published by the Financial Services Authority (FSA) suggested that the incidence of suspicious share price movements preceding takeover activity is now at an historic low. There are even some who doubt that insider dealing is damaging, arguing that it involves no obvious victim and actually assists in the rapid incorporation of information into price, which is essential for an efficient market.

As we will see, the criminal offence of insider dealing is notoriously difficult to prove. This has led to the introduction of a civil 'market abuse' regime, which, itself, is rarely utilised by the FSA. However, there is no doubt that politicians and regulators have become more aggressive in their pursuit of those who engage in insider dealing and, buoyed by recent regulatory successes, we can expect enforcement activity in this area to remain strong.

What is insider dealing?

Section 52 of the Criminal Justice Act 1993 (CJA) states:

> *(1) An individual who has information as an insider is guilty of insider dealing if, in the circumstances mentioned in subsection (3), he deals in securities that are price-affected securities in relation to the information.*
> *(2) An individual who has information as an insider is also guilty of insider dealing if:*
> *(a) he encourages another person to deal in securities that are (whether or not that other person knows it) price-affected securities in relation to the information, knowing or having reasonable cause to believe that the dealing would take the circumstances mentioned in subsection (3); or*

(b) he discloses the information, otherwise than in the proper performance of the functions of his employment, office or profession, to another person.

(3) The circumstances referred to above are that the acquisition or disposal in question occurs on a regulated market, or that the person dealing relies on a professional intermediary or is himself acting as a professional intermediary.

Breaking down this section of the 1993 Act, an offence is committed if:

- an insider deals in price-affected securities when in the possession of insider information
- an insider encourages another to deal in the price-affected securities when in possession of inside information
- an insider discloses inside information other than in the proper performance of his employment, office or profession.

The 'individual'

An 'individual', for the purposes of insider dealing, does not include a company. Given that businesses can commit, for example, theft, fraud, bribery and manslaughter, this is a clear gap in the law. However, a company could be guilty of aiding and abetting an insider dealing offence committed by a human being.

The 'insider'

Section 57 of the CJA states:

(1) A person has information as an insider if and only if:

(a) it is, and he knows that it is, inside information, and

(b) he has it, and knows that he has it, from an inside source.

(2) A person has information from an inside source if and only if:

(a) he has it through: (i) being a director, employee or shareholder of an issuer of securities; or (ii) having access to the information by virtue of his employment, office or profession; or

(b) the direct or indirect source of his information is a person within paragraph (a).

Primary insiders

These are people who have direct knowledge of inside information, such as those set out in Section 57. A basic case of insider dealing would be where a director of a company learns at a board meeting that it is to be subject to a takeover. In anticipation of the rise in the company's share price that an announcement of the takeover would trigger, the director increases his shareholding before the news is made public. When the announcement is made, the share price increases dramatically and the director sells his stake, making a handsome profit.

Recent FSA insider dealing cases have included staff in the reprographics department of a company and a university student on an internship. Quoted businesses must therefore take care to control the internal dissemination of information that may be price-sensitive.

Secondary insiders ('tippees')

This category is again provided for by Section 57 of the CJA. For example, the director described in the scenario above may disclose the takeover information to a friend, who then buys shares in the target company before the news is made public. Indeed, the director may be the ultimate beneficiary of the illicit trade if some or all of the profits are returned to him. Conducted in this manner, this is a cynical criminal enterprise, because while directors' dealings in the shares of their own companies are much scrutinised, this is not so obviously the case with respect to the dealings of others.

Secondary liability is much less certain in scope than primary liability. For example, a person might be told: "I hear from an inside source that company X is about to secure a major contract." The recipient of the information then deals. It is unclear whether these facts alone are sufficient to make the dealer liable or whether he needs to

FSA insider dealing prosecutions and convictions

Between January 2008 and August 2011 the FSA has prosecuted 13 individuals for insider dealing, securing 10 convictions, a conviction rate of 77 per cent
As of August 2011 the FSA is prosecuting a further 16 individuals for insider dealing, with the cases listed for trial between November 2011 and April 2012

Year	Prosecutions commenced/ pending	Convictions	Custodial sentences imposed including suspended sentences
2008	5	No cases	N/A
2009	4	4	4
2010	13	3	3
2011*	3	3	3

**Figures as of August 2011. Source: FSA*

know the precise identity of the source of the information.

Inside information

Section 56 of the CJA states:

> *(1) 'Inside information' means information which:*
> *(a) relates to particular securities or to a particular issuer of securities or to particular issuers of securities, and not to securities generally or to issuers of securities generally;*
> *(b) is specific or precise;*
> *(c) has not been made public; and*
> *(d) if it were made public would be likely to have a significant effect on the price of any securities.*
> *(2) Securities are 'price-affected securities' in relation to inside information, and inside information is 'price-sensitive information' in relation to securities, if and only if the information would, if made public, be likely to have a significant effect on the price of the securities.*
> *(3) For the purposes of this section, 'price' includes value.*

There is little guidance in the Act on the meaning of the expression "specific or precise" or on what might amount to a "significant effect on the price of the securities". It is clear, though, that the information does not need to be specific to a particular company. Indeed, inside information can relate primarily to another company. For example, in a sector dominated by two companies, a person may hear the unannounced news that company A has won a huge and lucrative contract. Rather than buy the shares in A, the person sells his holding in company B, A's competitor. This could amount to insider dealing.

With respect to what is or isn't a "significant effect on the price of the securities", this is rarely an issue as the prosecution will tend only to bring cases where the dealer has made a significant profit, which will mean there has been a big movement in price following the announcement of the information.

Under Section 56 of the Act, the information must be of a nature that would affect the price of securities if it were made public. What constitutes 'made public' is set out in Section 58:

> *(1) For the purposes of Section 56, 'made public', in relation to information, shall be construed in accordance with the following provisions of this section; but those provisions are not exhaustive as to the meaning of that expression.*
> *(2) Information is made public if:*
> *(a) it is published in accordance with the rules of a*

regulated market for the purpose of informing investors and their professional advisers;
(b) it is contained in records which by virtue of any enactment are open to inspection by the public;
(c) it can be readily acquired by those likely to deal in any securities (i) to which the information relates, or (ii) of an issuer to which the information relates; or
(d) it is derived from information which has been made public.
(3) Information may be treated as made public even though –
(a) it can be acquired only by persons exercising diligence or expertise;
(b) it is communicated to a section of the public and not to the public at large;
(c) it can be acquired only by observation;
(d) it is communicated only on payment of a fee; or
(e) it is published only outside the United Kingdom.

It is clear that, under the CJA, information can be public even if some extra steps or searches may be needed for an individual to acquire that information. It does not necessarily have to be common knowledge. This represents a real challenge for the FSA. In today's environment, information might be found in published but minority-interest websites, blogs and chat rooms. To what extent might this level of publication equate to 'made public'? One might also wonder what the fate would be of the trader who releases information in a barely read publication and then trades immediately after that release. These remain untested areas of law.

Price-affected securities

Schedule 2 of the CJA lists the securities covered by the offence. These include shares, debt securities, warrants, depositary receipts, options, futures and contracts for differences. The securities must also satisfy the conditions specified by the Treasury and secondary legislation under the Insider Dealing (Securities and Regulated Markets) Order, as amended in 1996. In a practical sense, the securities must be listed on an exchange in the European Economic Area (EEA) or be admitted to dealing on, or have their price quoted on, a regulated market.

Insider dealers nowadays will commonly trade through spread bets. These are exempt from stamp duty and the margin requirements of spread-betting firms allow for a significant bet to be made for a relatively small initial outlay.

The offences

We have considered the dealing offence that can be committed. Others are the 'encouraging offence' and the 'disclosing offence'.

The encouraging offence

Under Section 52, liability is imposed on a person who encourages another to deal while knowing, or having reasonable cause to believe, that the recipient will deal in securities so as to commit the dealing offence.

The disclosing offence

It is an offence to disclose inside information, otherwise than in the proper performance of the functions of the office held by that person.

Territorial scope

An offence will only be committed under the CJA if one of the essential elements of the offence takes place in the UK. Section 62 states:

(1) An individual is not guilty of an offence falling within subsection (1) of Section 52 unless:
(a) he was within the United Kingdom at the time when he is alleged to have done any act constituting or forming part of the alleged dealing;
(b) the regulated market on which the dealing is alleged to have occurred is one which, by an order made by the Treasury, is identified (whether by name or by reference to criteria prescribed by the order) as being, for the purposes of this Part, regulated in the United Kingdom; or
(c) the professional intermediary was within the United Kingdom at the time when he is alleged

to have done anything by means of which the offence is alleged to have been committed.
(2) An individual is not guilty of an offence falling within subsection (2) of Section 52 unless:
(a) he was within the United Kingdom at the time when he is alleged to have disclosed the information or encouraged the dealing; or
(b) the alleged recipient of the information or encouragement was within the United Kingdom at the time when he is alleged to have received the information or encouragement.

The UK government has a number of bilateral agreements in place with the governments of other states allowing for the exchange of information in insider dealing cases. The UK government will also co-operate with foreign regulatory bodies with regard to their investigations, and insider dealing is an offence that allows for extradition.

Defences

The burden of proof where there is an accusation of insider dealing lies with the defendant. The CJA sets out a series of general and special defences that could be relied upon.

General defences

Section 53 (1) (a) provides a defence if the accused can show that at that time he did not expect the dealing or encouraging to result in a profit (or the avoidance of a loss).

Section 53 (1) (b) provides a defence if the accused can show that he believed, on reasonable grounds, that the information had been disclosed widely enough to ensure that none of those taking part in the dealing would be prejudiced by not having the information.

Section 53 (1) (c) provides a defence if a defendant can prove that he would have done what he did even if he had not had the information. It may be the case, for example, that an individual was contractually bound to sell the shares at a particular time or there was some other overriding external pressure that made the individual buy or sell the securities when he did. This defence will often have real practical significance. For example, a director buying shares in his company could say it was not the inside information that caused his dealing but the general encouragement for people in his position to align their interests with those of the company's other shareholders by buying its stock. A day trader may be able to point to a research note, journal article are technical share price chart as being the true cause of his trade in the security. In most criminal cases, this defence will figure prominently.

It is a defence if the accused did not at the time expect any person, because of the disclosure, to deal in the relevant securities. It is also a defence if the individual did not expect a profit to be made or loss avoided, and that the change in price could be attributed to the information disclosed.

Special defences

The CJA provides three special defences to the dealing and encouraging offences:

- the market maker's defence
- the price-stabilisation defence
- the market-information defence.

The market-maker defence is available where an individual deals in securities or encourages another to deal and can show that he acted in good faith in the course of (a) his business as a market maker, or (b) his employment in the business of a market maker. In the City of London, market makers are used for dealing in many shares aside from those of the largest and most heavily traded companies, in which trading takes place via an automated system called SETS.

The price-stabilisation defence operates in favour of a person who can show that he committed the dealing or encouraging offences in conformity with the stabilisation rules made by the FSA under Section 144 of the Financial Services and Markets Act 2000. Price-stabilisation rules are designed to permit a manager of an

issuance of securities to enter the market and (usually) purchase the securities in order to maintain their market price.

The last of these special defences applies where the accused can show that the only information he had as an insider was market information – gained as a consequence of his involvement in the acquiring and disposing of shares – and that it was reasonable for a person in his position to deal in the securities despite having that information at the time of dealing. In determining whether it was reasonable for a person to deal in the shares, the courts will have regard to the content of the information, the circumstances in which he first had the information and the capacity in which he dealt.

The 'market abuse' regime

On December 1, 2001, in recognition of the fact that criminal insider dealing was very difficult to establish and, in any event, did not address all forms of illicit market behaviour, the FSA introduced a statutory prohibition on 'market abuse'. As a result of the effects of EU law, there are now seven types of behaviour that can constitute market abuse:

- insider dealing
- improper disclosure of inside information
- misuse of not generally available relevant information, not caught under the two provisions above, contrary to the standards of the regular user
- transactions or orders to trade that create false market impressions or artificially support prices
- transactions or orders to trade that employ "fictitious devices or any other form of deception or contrivance"
- disseminating false or misleading information
- behaviour creating false or misleading impressions or market distortion but not caught under the two points above relating to transactions, and contrary to the standards of the regular user.

The market-abuse offence creates civil liability, leading to unlimited fines or public censure by the FSA. The regulator is under a statutory obligation to publish a code giving guidance to those whose role it is to determine whether behaviour amounts to market abuse. This is known as the Code of Market Conduct and crucially it creates safe harbours – types of behaviour designated as not amounting to market abuse.

Also of relevance to this topic are the rules imposed on listed companies to publish promptly in a recognised way all information in their possession that might be price-sensitive.

The investigation and prosecution of insider dealing

Although historically prosecuted by the Department of Trade and Industry (now the Department for Business, Innovation and Skills), the FSA is now recognised as the lead investigator and prosecutor for the criminal offence of insider dealing. At the preliminary stages of an FSA investigation into market misconduct, it is very common for the regulator's Memorandum of Appointment of Investigators to cite both insider dealing and civil market abuse as being matters under investigation.

Insider dealing is essentially an offence involving the nefarious transmission and use of information. As such, criminal and market-abuse investigations focus on who has what information and to whom it may have been passed. The FSA and other investigators make substantial use of the authority afforded them under the Regulation of Investigatory Powers Act 2000 to obtain details of mobile telephone records. They can compel financial services firms to provide the recordings of conversations on the firm's telephone lines that might reveal the passage of inside information or, of less value as evidence but relevant when building a case, show an individual desperately keen to open a dealing account and buy or sell securities or make a spread bet. The FSA has recently conducted dawn raids, restrained those under suspicion from dealing in their assets, and worked hard to ensure that traditional broking

and spread-betting firms are alert to the indications of insider dealing and report their concerns promptly.

The imposition of custodial sentences on insider dealers over the past few years has, if anything, increased the pressure on the FSA. Establishing the criminal offence means that wrongdoers go to prison, and this means that the civil market abuse route is less attractive to the regulator. The case of Philip Jabré illustrates the point. The hedge fund manager was fined a record £750,000 in 2006 for committing market abuse. However, in phoenix-like fashion Jabré was free to establish himself as a multi-strategy fund manager in Switzerland. Had he been convicted of insider dealing and been imprisoned, his future would surely have been different.

Conclusion

In a bear market, with limited funds available for buyouts and acquisitions, opportunities for market misconduct are limited and egregious activities tend to stand out. It will be interesting to see how the reform of financial regulation in the UK affects the regulator's appetite for bringing insider dealing and market abuse cases. What is surprising is how rapidly and throughly the FSA has put its precious resources into insider dealing cases even though insider dealing is really only peripherally concerned with financial services regulation.

A new agency, the Financial Conduct Authority (FCA), will assume the role of markets regulator from the FSA, probably at the end of 2012 or early in 2013. In a speech on March 2, 2011 to the British Bankers' Association, Hector Sants, the chief executive of the FSA, said of the regulator's credible defence strategy and increasing focus on prosecutions and enforcement cases: "This strategy has shown particular success in relation to criminal prosecutions for insider dealing and it should be expected that the FCA will continue to vigorously pursue such cases in the future."

These are punchy sentiments. However, the FCA will be a complicated beast, being responsible not only for investor but also for consumer protection. The two are not obvious bedfellows, and if resources problems arise and there is a need for prioritisation, it may be hard for the FCA to display the same appetite for difficult, lengthy and expensive insider dealing investigations as its predecessor.

14

The main fraud offences prosecuted by the SFO

Harry Travers, Partner BCL Burton Copeland
Nicholas Yeo, Barrister Three Raymond Buildings
and Shaul Brazil, Barrister BCL Burton Copeland

Following a series of financial scandals in the City of London, the Serious Fraud Office (SFO) was established in 1988 in order to investigate and prosecute serious fraud. While the range of offences prosecuted by the SFO has expanded over the years, particularly in the area of overseas corruption, the vast majority of the prosecutions are still for generic fraud offences.

This chapter provides an overview of the main generic offences investigated and prosecuted by the SFO, namely the common law offence of conspiracy to defraud, and the statutory offences under the Theft Act 1968 and the Fraud Act 2006.

What is fraud?

Given how overwhelmingly obvious it seems, not least to a victim, that a particular type of conduct is fraud, it is extraordinary how difficult it has been to draft the substantive criminal law to define its scope effectively. Three larceny Acts through the 19th and 20th centuries failed adequately to achieve this goal.

The Theft Act 1968, which hoped finally to lay the matter to rest, got it spectacularly wrong (easy to say with the benefit of the sort of hindsight that a few decades and numerous House of Lords decisions brings). Most dramatically, the case of *Preddy* (1996) established that, after 28 years, the Act was unfit for the purpose of prosecuting the vast majority of mortgage frauds, as well as other frauds where the proceeds are wired from one bank to another.

Even the Fraud Act 2006 (which has so far proved glitch-free) stops short of defining fraud, preferring instead to describe three broad types of conduct that fall within its scope. The result is academically unsatisfying, but currently widely believed to be effective in practice.

Dishonesty

The test of 'dishonesty' derives from the 1982 case of *Ghosh*, held by the court to incorporate both an objective and a subjective element. The prosecutor must first satisfy a jury (and dishonesty is, in a Crown Court trial, *always* a question for the jury) that reasonable and honest people would consider the defendant's conduct to have been dishonest. The prosecutor must, then, satisfy the jury that the defendant was aware that his conduct

would be considered dishonest by reasonable and honest people.

Notably, subject to limited exceptions under the Theft Act 1968, which are addressed further below, it does not matter whether the defendant believed that he was entitled to do what he did (for example, the MP who over-claimed on his expenses because he thought his salary was too low), if, at the same time, he realised that the reasonable and honest person would regard what he did as dishonest.

While at first sight the *Ghosh* test may appear straightforward, in reality it is not always easy to apply. Take the example of a company director and majority shareholder who employs his wife as his personal assistant and pays her a salary that he considers can be justified but is above the market rate. It is by no means clear that a jury would consider his actions to have been dishonest. The problem is compounded in cases of commercial fraud where the 'ordinary' person may not be able to evaluate the honesty or otherwise of the activities.

The main offences

There are numerous discrete offences on the statute books that involve the commission of specific types of fraud such as misleading the market, cartels, tax crimes and corruption. This chapter, however, focuses on the main generic fraud offences of *conspiracy to defraud* and those under the Theft Acts, which together account for the vast majority of the prosecutions brought by the SFO. Consideration will also be given to the fraud offence under the Fraud Act 2006, which only applies to conduct committed wholly after January 15, 2007.

The common law offence of conspiracy to defraud

This can carry a punishment of ten years' imprisonment and remains a regularly used offence in the SFO's armoury. The definition of the offence derives from *Scott*, a 1975 case in which the court held that a conspiracy to defraud amounts to:

- "an agreement between two or more [persons] by dishonesty to deprive a person of something which is his or to which he is or would be or might be entitled, and an agreement by two or more [persons] by dishonesty to injure some proprietary right of his".

In other words, the offence is made out when two or more persons agree dishonestly to prejudice the rights of another.

The offence clearly encompasses an extremely wide variety of forms of fraudulent conduct. Its main advantage, over statutory offences, is said to be that it can be used to encapsulate, in a single charge, a course of conduct that might spread across years and incorporate numerous discrete examples of fraudulent behaviour. Examples of recent conspiracy-to-defraud cases brought by the SFO include:

- **RBG Resources plc** – a global metals-trading company with an advertised turnover in 2000 of more than US$1 billion that went into liquidation in 2002 with debts of over US$420 million. Its senior executives were prosecuted for creating phantom business transactions in order to secure substantial loans from commercial banks
- **Practical Property Portfolio Ltd** – a buy-to-let investment business that took in funds of £80 million from investors. The senior directors were prosecuted when it came to light that many of the investment properties were of a lower quality than represented, and that supposed rental income received by investors was in fact derived from new money put into the scheme by other investors
- **Independent Insurance Group plc** – a £900 million insurance company that collapsed with the loss of over a thousand jobs. Three of its directors were prosecuted for withholding insurance claims data and loss-making reinsurance contracts from the company's actuaries and others.

The offence of conspiracy to defraud does not

require an intention to deceive. In the case of *Scott*, the court was concerned with the sale of illegally copied films where there was no intention to deceive the real film owners or the intended customers of the copied films. The court held that no deception was needed; all that was required was that the parties to the conspiracy had acted dishonestly with a view to injuring the rights of another.

Generally, the 'rights of another' will constitute that person's economic interests. But this does not mean that actual loss must be incurred or that the parties to the agreement desired that any loss should be incurred. It is sufficient if the parties to the agreement realised that their agreement, if carried out as intended, would or might have the effect of prejudicing another's economic interests.

Conspiracy to defraud is therefore capable of capturing almost any dishonest conduct that has the effect of prejudicing a person economically in any way, hence its popularity with the SFO. However, the offence is by no means without its critics, who argue that its breadth creates uncertainty as to what is and what is not lawful conduct and that it is over-used in preference to statutory offences, particularly when it is used to sidestep difficulties in the proof of any substantive offence.

The stated intention of the Law Commission draft Bill on which the Fraud Act 2006 was based was to "eliminate the indefensible anomaly represented by the continuing survival of conspiracy to defraud". The government decided to retain the offence, but undertook to review the operation of the Act three years after its implementation (see below).

The main argument for the abolition of the offence of conspiracy to defraud is that it is ill-defined and too uncertain. In theory, the scope of the offence should by now be clear, and the courts are reluctant to extend the boundaries of the common law beyond its defined limits (*DPP v Withers* [1975]). However, as the case of *Norris* demonstrates, its limits remain sufficiently uncertain that even in 2008 the divisional court was found, by the House of Lords, to have been wholly wrong to hold that price fixing was necessarily within the scope of the offence.

On January 9, 2007, the Attorney General issued, to all prosecuting agencies, 'Guidance on the use of the common law offence of conspiracy to defraud'. The effect of the guidance is that the use of conspiracy to defraud should be limited to two classes of conduct:

- "conduct that can more effectively be prosecuted as conspiracy to defraud" – in other words, cases where various kinds of criminality are involved (possibly with a wide range of victims). The reasoning of the document was that prosecuting such cases under statutory provisions might lead to indictments with an unwieldy number of separate counts, and possibly to separate trials for separate parts of the conspiracy
- "conduct that can only be prosecuted as conspiracy to defraud" – in other words, conduct that is not covered by any statutory offence.

It is arguable, given that the Law Commission originally intended that the Fraud Act 2006 should cover all forms of fraudulent conduct, that some of the "conduct that can only be prosecuted as conspiracy to defraud" should not be criminal at all.

The guidance also requires that each time the common law offence of conspiracy to defraud is prosecuted, the prosecutor must consider whether a case would be better prosecuted under statutory provisions. Where conspiracy to defraud is charged, the prosecutor is required to make a written record justifying its use, which must include how much such a charge will add to the sum of evidence to be called at trial.

The purpose of collecting this information was so that it could be used in the government's review of the implementation of the Fraud Act 2006, referred to above. It is now understood that the review will be undertaken by the Ministry of Justice and that it will be published by the end of 2011. Its recommendations as to whether it is now

'safe' to abolish the offence of conspiracy to defraud are eagerly anticipated.

Theft and false accounting offences under the Theft Act 1968

The deception offences under the Theft Act 1968 were repealed by the Fraud Act 2006 for conduct taking place wholly after January 15, 2007. Theft and false accounting are the most important remaining offences under the Theft Act in the field of serious fraud.

Theft contrary to section 1 of the Theft Act 1968

Section 1 of the Theft Act 1968 provides that:

- "a person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it."

Theft is punishable with seven years' imprisonment.

The offence of theft is founded upon 'dishonest appropriation'. The House of Lords held in a famous triptych of cases (*Morris, Lawrence* and *Gomez*) that the word 'appropriates' in the definition of theft is no narrower than its statutory definition: "any assumption by a person of the rights of the owner …"; it does little to limit the scope of the offence. More recently, in *Hinks* (2001), this has been confirmed to extend even to circumstances in which the victim has made an indefeasible gift to the defendant, and could have no remedy in civil law.

This has left the concept of 'dishonesty' to 'do all the work'; in difficult cases, the question of whether conduct is or is not within the scope of the offence is entirely determined by the question of dishonesty. That is an issue quintessentially for the jury, which often can only be determined with certainty at the end of the case. Inevitably, the bounds of the offence are as uncertain as for conspiracy to defraud, and depend on an uncertain prediction of what a putative jury will think.

One of the technical areas surrounding the law of theft is the definition of 'property', which includes, in addition to money and real property, 'things in action and other intangible property' (Section 4 of the Theft Act 1968). In complex fraud cases, the property in question is rarely physical and, as such, the jury will probably be required to consider technical issues surrounding the status of intangible rights, such as debts, shares, letters of credit and intellectual property.

The difficulty is that there is rarely an intention permanently to deprive a victim of intellectual property. The victim retains the property, but the perpetrator unfairly makes use of the victim's work. Therefore theft is inapposite to much wrongdoing associated with intellectual property. It remains almost as true today as when it was said in 1968 by Sir Edward Boyle MP that: "It is not too much to say that we live in a country where … the theft of the boardroom table is punished far more severely than the theft of the boardroom secrets."

Section 2 of the Act uniquely prescribes specific circumstances that are 'not to be regarded as dishonest' for the purpose of the offence. Those circumstances are: belief in a legal right to deprive the other person of the property; belief that the other person would consent to the appropriation of the property; and belief that the owner of the property cannot be found by taking reasonable steps. The belief of the defendant does not have to be reasonable, but it must be genuinely held.

False accounting

Section 17 of the Theft Act 1968 created two offences of false accounting that are in essence committed where, dishonestly, a person either *makes* a false account or *uses* a false account. False accounting is a popular charge with prosecutors, as it is often an easy way of prosecuting someone where the intention of the perpetrator is uncertain or complex.

Under Section 17, false accounting occurs:

- "where a person dishonestly, with a view to gain for himself or another, or with intent to

cause loss to another – (a) destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purpose; or (b) in furnishing information for any purpose produces or makes use of any account, or any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material particular".

Whether something is an 'account' or a 'record or document made or required for an accounting purpose' is an issue where the terms should be given their ordinary meaning. Unless obvious, evidence should be called as to the nature of or the purpose of the document, but the accounting purpose identified does not have to be the sole or dominant purpose. Neither is the definition restricted to documents that may be required by an accountant or auditor. It is sufficient if the document would be used by anybody for an accounting purpose.

As to whether a document is 'false', Section 17(2) of the Act provides that:

- "a person who makes or concurs in making … an entry which is or may be misleading, false or deceptive in a material particular, or who omits or concurs in omitting a material particular … is to be treated as falsifying the account or document."

Nonetheless, the issue of whether an entry in an account is or may be misleading, false or deceptive in a material particular will often be difficult to resolve.

Take, for example, an invoice prepared by a company in relation to a public procurement contract. In order to obtain the contract, a bribe was paid to the official responsible for negotiating the contract price. The value of the bribe was then priced into the contract. The invoice therefore records a price that is higher than it would have been but for the payment of the bribe. Is the price recorded false? Arguably, the invoice records the true price of the contract, even though that price incorporates the cost of an illegal payment.

Difficulties may also arise where the making of an entry in an account necessarily involves a degree of interpretation or subjectivity. For example, the accounting rules regarding the preparation of company accounts provide for a margin of acceptable practices.

Even where an entry in an account is demonstrably outside the margin of acceptable practices, however, the question as to whether the entry is 'material' may be open to argument. That test is an objective one that may be resolved by determining whether the entry is likely to have had a bearing on anybody using the account, record or document. In *Lancaster* (2010), the court held that in a case of false accounting by omitting a material particular, the jury should judge whether the omission was thought 'significant'.

The Fraud Act 2006

Overview

The Fraud Act 2006 came into force on January 15, 2007 and applies only to conduct committed wholly after that date. Section 1 of the Act created a general fraud offence that can be committed in three ways: fraud by false representation; fraud by failing to disclose information; and fraud by abuse of position. Each of these requires dishonesty and an intention to gain or to cause loss to another (or expose another to a risk of loss) and each carries a maximum sentence of ten years' imprisonment.

The meaning of 'gain' or 'loss' is defined in the Act to extend only to gain or loss in money or other property, but to include any temporary or permanent gain or loss. 'Gain' includes keeping what one has, and 'loss' includes not getting what one might get. Thus, a defendant might 'gain' if the false statements he made to the market prevented a fall in the price of equities he held, or the victim tax authorities might suffer 'loss' if the defendant's false representations as to his tax liability resulted in an underpayment of tax.

Notably, the SFO is yet to bring many charges

under the Fraud Act. One reason for this is that the SFO's cases can take years to investigate and charge. As such, many recent cases have related to conduct that took place before the coming into force of the new Act. Another reason is that the complexity and size of many SFO cases are such that conspiracy to defraud is often still believed to provide the most suitable charge.

Fraud by false representation

Section 2(1) of the Act provides that a person is 'in breach' of that section (and thereby guilty of the general fraud offence under Section 1) if he dishonestly makes a false representation, and intends by making the representation either to make a gain for himself or another, or to cause loss to another or expose another to a risk of loss.

A representation is 'false' if it is untrue or misleading and the person making the representation knows that it is, or might be, untrue or misleading. 'Representation' means any representation of fact or law, including the state of mind of the person making the representation or any other person. A representation may be express or implied, and may be made if submitted to a machine without any human intervention.

The offence is complete as soon as the false representation is made. Unlike the deception offences that the fraud offence replaces, there is no need to show that the representation is operative on a person's mind. Under the old law, oddly, using fake coins to buy cigarettes over the counter was a deception offence, but using the same coins in a vending machine was not; no human mind was deceived. A side-effect of this change is that there is virtually no scope for attempted fraud by false representation; what were attempts under the old law now constitute the completed offence of fraud under the Fraud Act 2006.

Further, the offence imposes liability on the person making a representation not only in circumstances where he knows that the representation is untrue or misleading, but also where he knows it "might be untrue or misleading". Clearly, there are numerous examples of such representations in the business world: for instance, revenue forecasts might be untrue or misleading.

The debates in the House of Lords on this issue illustrated the point. They suggested that an auction house that sold a painting as a Renoir believing it to be a Renoir, but knowing this statement might be untrue, as with any attribution of the period, would be guilty of the offence if the attribution later turned out to be wrong. The Attorney General said that such issues would be resolved by a consideration of dishonesty.

Fraud by failing to disclose information

Section 3 of the Act provides that a person is 'in breach' of that section (and thereby guilty of the general fraud offence under Section 1) if he dishonestly fails to disclose information to another person, which he is under a legal duty to disclose, and intends by failing to disclose the information to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.

Although it is not defined in the Act, the reference to a 'legal duty' means, in practice, a requirement to disclose information imposed by the civil law, and not any moral duty or any expectation on the part of the recipient that is wider than a requirement imposed by the civil law. Examples of a legal duty include the provisions governing company prospectuses, transactions of the utmost good faith (such as insurance contracts), or where there exists a fiduciary relationship such as between an agent and his principal.

The existence of certain legal duties will be straightforward – for example, the requirement to disclose previous claims on an application for car insurance – and as such could well be prosecuted as a fraud by false representation. However, the existence and scope of other legal duties will be less straightforward and are likely to require, in the context of a criminal trial, consideration of complex areas of the civil law.

Fraud by abuse of position

Section 4 of the Act provides that a person is 'in breach' of that section (and thereby guilty of the

general fraud offence under Section 1) if he occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person, and he dishonestly abuses that position with the intent of making a gain for himself or another, or of causing loss to another or exposing another to a risk of loss.

Again, none of the key terms of this offence are defined in the Act. However, it is generally accepted that the offence will apply (but not be limited to) persons who owe a 'fiduciary duty'. It will be a matter for the judge to determine whether the particular facts of a case give rise to a relationship capable of being caught by the offence. Examples of positions that clearly fall within the terms of the offence include trustees, company directors and employees.

In the case of *Woods* (2011), the defendant had worked at a betting shop. She had changed a customer's horserace betting stake from £1 to £100. The horse won and the customer received his winnings of £10. The defendant retained the balance of £990. Although the defendant claimed that she had not intended to cause loss, as she would have paid her personal £90 bet had the horse lost, her conviction was upheld on the basis that she had dishonestly abused her position of trust as a manager of the betting shop.

Another example given by commentators of conduct that would be caught by Section 4 of the Fraud Act is the making of secret profits. It is arguable, for example, that an agent who profits from his position by receiving a payment from the counterparty to a transaction without informing his principal has abused his position.

Conclusion

The prosecutor in cases of serious economic crime benefits from a range of varied and overlapping offences from which to select an appropriate charge. One instance of wrongdoing can be charged under various offences within some or all of the following categories:

- narrowly described regulatory offences targeted at a particular wrong – such as insider dealing – described elsewhere in this work
- the versatile three-pronged fraud offence expressed in unambiguous language, which has been lauded for expressing the essence of fraud in a practical and comprehensible way
- the narrowly described but widely applicable false accounting offence that can target the lying document or documents at the heart of a case and leave the jury with a simple question: does this piece of paper tell a lie?

Notwithstanding this wealth of choice, what the Law Commission described as the 'indefensible anomaly' common law offence of conspiracy to defraud remains intact and in use. Indeed, conspiracy to defraud charges have been brought by prosecutors every year since the coming into force of the Fraud Act 2006. The rationale for its use is sometimes founded upon the premise that multiple counts expressed in clear statutory language, under, for example, the Fraud Act 2006, are harder for a jury to grasp than a single nebulous conspiracy to defraud count with multiple particulars. However, the authors' view is that the statutory offence is more than adequate to capture conduct which should be criminalised.

It may be that the continued use of the conspiracy to defraud offence can be put down to two causes. First, a perception among prosecutors that it is easier to prove – that its imprecise nature presents a low hurdle for a conviction and leaves scope for a change of emphasis in the prosecution case during the course of a trial. This may be true, but it needs to be weighed against reluctance by a jury to convict where a tangible wrong is not well-articulated. Second, it is possible that some prosecutors may prefer the common law offence as it avoids the need to identify the particular statutory offence that targets the true gravamen of the matter.

It is the authors' view that defendants are reluctant to plead guilty to poorly defined conspiracy to defraud offences, but may be willing (or have no choice but to) where the chosen

offence is restricted to wrongdoing that can actually be proved against them.

In the circumstances, it will be interesting to see the conclusions of the Ministry of Justice's review of how the current law works in practice, and whether it takes the view that the continued use of conspiracy to defraud is appropriate, or whether it is in fact now 'safe' to put into effect the Law Commission's recommendation to "dispose of an anomalous and excessively broad offence".

• *The authors would like to thank Kitty St Aubyn for her contribution to this chapter.*

15

The Proceeds of Crime Act 2002 and the prosecution of economic crime

John P Rupp, Partner, Robert Amaee, Counsel, and Ian Redfearn, Associate
Covington & Burling LLP

When enacted almost a decade ago, the UK Proceeds of Crime Act 2002 (POCA) was hailed as a powerful new tool that would help prosecutors target criminal assets and thereby "cut the profits that are made from crime and increase the risk to those who indulge in criminal activities".[1]

By any measure, POCA is a wide-ranging piece of legislation, running to 462 sections and 12 schedules. The money laundering offences created by the Act are broadly drafted and have significant extra-territorial effect. Further, the confiscation and civil recovery mechanisms in Parts 2 and 5 of POCA, together with the investigatory provisions in Part 8, are significant weapons for enforcement authorities. There is no doubt that POCA has been used effectively on many occasions since coming into force but the full strength of the legislation in the battle against bribery and other related forms of corruption has been recognised only in the last few years.

This chapter provides an overview of the ways in which POCA has been used in the past, and may be used in the future, by the Serious Fraud Office (SFO) against commercial organisations and individuals accused or convicted of serious economic crimes.

Jurisdiction and penalties

POCA gives UK enforcement authorities, including the SFO, broad extra-territorial jurisdiction over commercial organisations and individuals suspected of having engaged in money laundering, even when those authorities would not have jurisdiction to prosecute the underlying conduct giving rise to criminal proceeds. This is significant in the context of serious economic crimes, which often have an international dimension.

Take the case of a US-based company that bribed a foreign government official in a country in sub-Saharan Africa in connection with a tender for a major infrastructure project. Let us assume that the US company has no subsidiaries or operations in the UK, that no part of the corrupt scheme took place within UK territory, and that no British citizens were implicated in the bribery. As a result of the bribes having been made, however, the US company was awarded the tender and generated significant revenues from the project. The revenues were paid into a bank account held by the company in the UK and from that account they were transferred to one held by the company in the US.

It is unlikely the company would have committed an offence under the UK Bribery Act 2010. The mere fact that the project revenues were transferred into and out of a UK bank account would be sufficient, however, to bring the US company within the jurisdiction of the UK enforcement authorities. The company could thus be prosecuted for one or more substantive money laundering offences, so long as it could be established that a 'directing mind' of the company was himself guilty of money laundering (see the 'identification principle' dealt with elsewhere in this book). An enforcement authority would not need to demonstrate that the money was the benefit of a particular or specific act of criminal conduct; it would simply need to produce circumstantial evidence sufficient to justify an inference that the money had a criminal origin.

The penalties under POCA for money laundering are severe – often more severe than the penalties for the underlying conduct giving rise to the criminal property. A person found guilty of a substantive money laundering offence would be liable, on conviction in the crown court, to imprisonment for a term not exceeding 14 years, or to a fine, or both.

In contrast, a person found guilty of a bribery offence contrary to the Bribery Act 2010 would be liable to a maximum ten-year prison sentence, or to a fine, or both.

The prosecution of economic crime by the Serious Fraud Office

The Director of the SFO has broad prosecutorial discretion and POCA has clearly been a useful addition to the SFO's arsenal in the fight against several types of economic crime, including bribery and other forms of corruption.

The SFO is eager to encourage businesses and professional advisers to self-report cases of corruption, and the prospect of dealing with corruption using civil recovery orders, rather than through criminal prosecution, has often been cited by the SFO Director as an incentive to self-reporting.[2] It is therefore important that commercial organisations understand how the SFO has used civil recovery orders in the past, as previous actions are likely to offer a helpful guide to future conduct.

The confiscation and recovery of criminal property

POCA includes provisions that enable enforcement authorities to confiscate or recover criminal property in both criminal and civil proceedings.

Confiscation orders

Part 2 of POCA empowers the court to make an order against defendants requiring them to pay an amount equal to the benefit from crime, unless there are insufficient assets, where they:

- have been convicted of an offence in proceedings before the crown court; or
- have been committed to the crown court for sentencing in respect of an offence tried in a lower court.

A prosecutor may ask a court to make a confiscation order, or a court may decide of its own volition that a confiscation order would be an appropriate sanction.

The approach that the UK courts are required to take with respect to confiscation orders is set out in Section 6 of POCA:

(1) A court first must decide whether a defendant has a criminal lifestyle, which will be deemed to be the case if the offence: (a) is one of the so-called 'lifestyle offences' specified in Schedule 2 of POCA, such as drug trafficking, money laundering or counterfeiting; (b) constitutes conduct forming part of a course of criminal activity; or (c) is an offence committed over a period of at least six months that has benefited the defendant.

(2) If a court concludes that a defendant has a criminal lifestyle, it then must decide whether the defendant has benefited from his or her

general criminal conduct. If so, the court needs to determine the recoverable amount and make a confiscation order requiring the defendant to pay that amount.

(3) If a court concludes that a defendant does not have a criminal lifestyle, it must decide whether the defendant has nonetheless benefited from his or her criminal conduct. If it concludes that there has been a benefit, it must determine the recoverable amount and make a confiscation order requiring the defendant to pay that amount.

Civil recovery orders

In addition to the confiscation procedure that applies in the context of criminal proceedings, Part 5 of POCA allows enforcement authorities to recover, in civil proceedings before the High Court, property that is, or represents, property obtained through 'unlawful conduct'. This is defined as conduct:

- that is unlawful under UK criminal law; or
- that occurs in a country outside the UK and is unlawful under that country's criminal law and would be unlawful in the UK if it were to occur there.

The use of civil recovery orders by the Serious Fraud Office

Since 2008, the SFO has obtained several civil recovery orders in cases involving bribery and corruption.

Balfour Beatty

A subsidiary of Balfour Beatty, the international engineering company, was involved in a joint venture with an Egyptian company for the construction of a major cultural centre in Alexandria. Balfour Beatty discovered several payment irregularities that were inaccurately recorded in the subsidiary's accounts. Balfour Beatty self-reported to the SFO. The SFO found that the Balfour Beatty subsidiary had breached the Companies Act requirement to maintain accurate business records.

An investigation also concluded, however, that there was no financial benefit to any individual employee and that Balfour Beatty's management was working to review and improve the company's anti-corruption procedures. The SFO obtained a civil recovery order worth £2.25 million and a contribution toward the costs of the proceedings.

AMEC

AMEC, an international engineering and project management company, found evidence of irregular payments in connection with a project in which it was a shareholder. The company self-reported to the SFO in March 2008. The SFO found that AMEC had breached the Companies Act requirement to maintain accurate business records but acknowledged its prompt referral of the case upon the conclusion of its internal investigation and its co-operation with the SFO's investigation. On October 26, 2009, the SFO obtained a civil recovery order against AMEC worth almost £5 million plus costs.

DePuy International

DePuy International, a UK-based manufacturer of orthopaedic products, is a subsidiary of Johnson & Johnson, the US-based pharmaceuticals and healthcare products company. Between 1998 and 2006, DePuy International made payments to intermediaries for the purpose of making corrupt payments to healthcare professionals in Greece.

Following an internal investigation by Johnson & Johnson, the unlawful conduct was reported to the US authorities. The US Department of Justice referred the matter to the SFO in October 2007 and subsequently entered into a deferred prosecution agreement with Johnson & Johnson. The SFO obtained a civil recovery order against DePuy International on April 8, 2011 requiring the company to pay more than £4.8 million plus costs.

MW Kellogg

MW Kellogg is a UK-based subsidiary of a US company, Kellogg Brown and Root, an engineering and construction firm with experience in the energy

and petrochemicals sectors. The parent company was one of four corporate entities that formed a joint venture to bid for contracts on a liquefied natural gas project in Nigeria. The joint venture won four contracts, three of which had been obtained following the payment of bribes or promises to pay bribes. The parent company admitted to structuring the joint venture through MW Kellogg to avoid compliance with the US Foreign Corrupt Practices Act. It reached a civil settlement with the US authorities in February 2009.

MW Kellogg self-reported to the SFO and fully co-operated with an investigation into its conduct. The SFO obtained a civil recovery order against MW Kellogg on February 16, 2011, requiring payments of more than £7 million. MW Kellogg also undertook to review and strengthen its audit and anti-corruption procedures.

Macmillan Publishers

An agent for Macmillan Publishers, a UK-based company, attempted to make a corrupt payment with a view to influencing the award of a World Bank tender to supply educational materials in Southern Sudan. The company did not win the contract and the World Bank reported the agent's conduct. The City of London Police executed search warrants in December 2009 and Macmillan Publishers reported the matter to the SFO in March 2010. The SFO and the World Bank conducted parallel investigations, which concluded that the company may have won tenders in Rwanda, Uganda and Zambia as a result of corrupt relationships. The company co-operated with those investigations and reacted appropriately in reviewing and improving its internal anti-corruption policies and procedures.

The SFO obtained a civil recovery order requiring that Macmillan Publishers pay more than £11 million, which the SFO determined to be the amount of revenue earned by the company because of potentially unlawful conduct.

In each of these cases, the SFO concluded that a civil recovery order was an appropriate and proportionate alternative to a criminal prosecution. When deciding whether to opt for a criminal sanction or a civil penalty, the SFO will typically consider:

- the availability of evidence to support a criminal prosecution, bearing in mind the enhanced burden of proof in criminal cases ('beyond a reasonable doubt') compared with the burden of proof in civil cases ('a balance of probabilities');
- the extent of any co-operation with the SFO's investigations, including the provision of evidence that could lead to the investigation and prosecution of other entities or individuals;
- a commitment to remedial action to improve internal compliance procedures, including board-level support for strengthening audit and control processes; and
- whenever the conduct is also punishable under the criminal law of another jurisdiction, the need to ensure that the offender is not prosecuted twice for the same conduct.

This approach has attracted judicial criticism. For example, in his sentencing remarks in *R v Innospec Ltd* (2010), which concerned corrupt conduct in Iraq and Indonesia, Lord Justice Thomas said:

"Those who commit such serious crimes as corruption of senior foreign government officials must not be viewed or treated in any different way to other criminals. It will therefore rarely be appropriate for criminal conduct by a company to be dealt with by means of a civil recovery order … It would be inconsistent with basic principles of justice for the criminality of corporations to be glossed over by a civil as opposed to a criminal sanction."

Lord Justice Thomas did recognise, however, that "there may … be a place for a civil order, for example, as a means of compensation in addition to a fine".

The Director of the SFO has since reiterated

his view that "there may be cases when we [the SFO] are unable to prosecute and we consider that a civil recovery order is appropriate".[3] Indeed, as the Director has pointed out, the UK Attorney General has issued guidance that expressly permits the use of civil recovery orders whenever: (a) it is not feasible to secure a conviction; (b) a conviction is obtained but a confiscation order is not made; or (c) a relevant authority is of the view that the public interest will be better served by using those powers rather than by seeking a criminal disposal.[4]

It is therefore unlikely that the SFO will make significant adjustments to its policy regarding the use of civil recovery orders in the immediate future.

Money laundering offences

In addition to the confiscation and recovery mechanisms described above, POCA recast the English money laundering offences. The explanatory notes to POCA define money laundering as "the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently or recycled into further criminal enterprises".

Money laundering was first criminalised in the UK under the Drug Trafficking Offences Act 1986, which dealt specifically with the proceeds of these offences. Further money laundering offences were subsequently enacted but each set applied to a different category of predicate offences. In practice, this meant that law enforcement authorities needed to identify a specific underlying offence before they could prosecute for money laundering. This anomaly was addressed in POCA, which created a single set of money laundering offences applicable in all circumstances, without regard to the nature of any predicate offences.

POCA created three substantive money laundering offences.[5] It is a defence to each of these if a person makes an authorised disclosure and gains the appropriate consent.[6] A disclosure is an 'authorised disclosure' if:

- a constable, customs officer or a nominated officer is informed that property is criminal property;
- it is made in the form of a suspicious activity report (SAR); and
- either it is made before the alleged offender commits the prohibited act, or, if it is made after, there is a good reason for the failure to make the disclosure before the act and the disclosure is made as soon as it is practicable.

Suspicious activity reports

SARs are submitted to the Serious Organised Crime Agency (SOCA), typically electronically via a secure website. When a person is seeking consent to proceed with a transaction involving potentially criminal property, the SAR must identify as clearly as possible:

- the suspected criminal property, including its value (if known);
- the reason for the person's suspicion that the property is criminal property;
- the prohibited act that the person intends to undertake involving the suspected criminal property; and
- the other parties involved in dealing with the suspected criminal property, including their dates of birth and addresses.

Persons in the regulated sector should collect the fourth category of information to ensure compliance with their customer due diligence requirements under the Money Laundering Regulations 2007. The procedures that have been adopted by many banks and investment firms recently have been found to have serious weaknesses in that regard.

Upon receipt, SARs are logged in a database that is maintained by the United Kingdom Financial Intelligence Unit. The UKFIU evaluates all SARs for strategic and tactical intelligence and the SARs database can be accessed by approximately 80 law enforcement agencies, including police forces, the SFO, HM Revenue &

Customs, and the Department for Work and Pensions.

SARs containing requests for consent are prioritised by SOCA. A constable, customs officer or nominated person may give consent to the proposed or historic transaction. Alternatively, a person will be deemed to have consent to proceed if:

- he or she does not receive notice from a constable or customs officer that consent is refused within seven working days from the date of the request; or
- he or she receives notice from a constable or customs officer that consent is refused within the period of seven working days, but a moratorium period of 31 days has elapsed since he or she received that notice.

The strategy for filing suspicious activity reports

In practice, corporates and individuals often have difficulty in deciding whether they have the requisite knowledge or suspicion to justify making a disclosure. The Joint Money Laundering Steering Group has published helpful guidance on that issue.[7] The guidance emphasises that 'knowledge' does not necessarily mean actual knowledge; it also may be inferred from the circumstances surrounding a transaction or proposed transaction. 'Suspicion' is a lower standard than 'knowledge' but a suspicion still needs to be "more than merely fanciful" to justify disclosure.

Corporates should consider the timing of any SAR filing that they wish to make. For example, if a UK-based corporate concludes, following an internal investigation, that it benefited from bribes paid by its employees overseas, it is highly likely that a SAR would need to be filed. The corporate may also wish to self-report the overseas corruption to the SFO. When deciding on the timing of each of these filings, it should be borne in mind that concurrent filing is preferred by the enforcement authorities, and if the SFO finds out about an incident of overseas corruption from a SAR, the corporate could lose its opportunity to earn credit for self-reporting.

Corporates must take care to ensure that information on SARs is closely controlled, since POCA contains a separate 'tipping off' offence (Section 333). A person may commit that offence if:

- he or she knows or suspects that a SAR has been filed or that a disclosure has been made to a nominated officer; and
- he or she makes a disclosure that is likely to prejudice any investigation that might be conducted as a result of the filing of that SAR or the making of that disclosure.

The maximum penalty for the tipping-off offence is significant: imprisonment for a term not exceeding five years, or a fine, or both (Section 334). Corporates and individuals should therefore be mindful of the risk that prejudicial information may be disclosed inadvertently.

Future developments

In recent years the SFO has demonstrated a renewed determination to tackle overseas corruption and prosecute corporate wrongdoers. Those efforts may be expected to become more robust now that the UK's antiquated bribery laws have been replaced by the Bribery Act 2010.

As the risk of investigations and prosecutions of overseas corruption increases, POCA is likely to become more important to the SFO's work. It is therefore crucial that individuals and corporates working in industries and markets that present significant corruption risks familiarise themselves with the Act's key provisions and its far-reaching implications.

16

The money laundering reporting regime: the offences and the defences

Kevin Roberts, Partner Morrison & Foerster (UK) LLP
PwC implementation focus Andrew Clark and Marie-Alice Hofmaier

The Proceeds of Crime Act 2002 (POCA) sets out three principal money laundering offences as well as providing affirmative defences to them if a report is filed of suspicious activity. POCA requires that organisations in the regulated sector have a reporting regime including a nominated money laundering officer. It is an offence not to report suspicions of money laundering both internally within an organisation and externally to the Serious Organised Crime Agency (SOCA).

The regime is enforced with substantial custodial and financial penalties. It is wide in scope with expansive definitions of potential criminal activity and criminal property and a low standard of criminal intent. In the regulated sector, this low standard of intent is further bolstered by an objective assessment of the required test. The reporting regime is ringfenced by the offences of tipping off others after a report is made and of prejudicing an investigation.

Money laundering offences

The principal money laundering offences set out below apply to the laundering of criminal property after February 24, 2003. There are similar provisions under the Criminal Justice Act 1988 (as amended) and the Drug Trafficking Act 1994 (as amended) for offences prior to that date and under the Terrorism Act 2000.

The offences under Sections 327, 328 and 329 of POCA are 'either way' offences, carrying a maximum of 14 years' imprisonment or a fine or both in the crown court.

Section 327

It is an offence to conceal, disguise, convert or transfer criminal property, and to remove it from England and Wales.

Concealing or disguising criminal property is defined as concealing or disguising its nature, source, location, disposition, movement or ownership, or any rights with respect to it.

Section 328

It is an offence to enter into or become concerned in an arrangement that a person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

There is no statutory definition of 'arrangements' and the courts have

interpreted it widely. However, it is clear from the UK Law Society guidance following the decision in *Bowman v Fels* (2005) that those conducting litigation – including preparatory stages such as pre-action, or diversions from the court system such as negotiations, out-of-court settlements, alternative dispute resolution and tribunal representation – are not involved in Section 328 'arrangements' and therefore do not need to make authorised disclosures. The Law Society's view is that logically solicitors will also not be committing Section 327 or Section 329 offences in these circumstances (see paragraph 95 of the judgment).

Section 329

Under this section of POCA it is an offence to acquire or use criminal property, or to have possession of it with knowledge or suspicion that the property represents – in whole or in part, directly or indirectly – a benefit from criminal conduct.

Criminal property

Under Section 340, a property is criminal property if it constitutes a person's benefit from criminal conduct or it represents such a benefit – in whole or in part, whether directly or indirectly – and the offender knows or suspects it constitutes or represents such a benefit.

Under Section 340, the property is "all property wherever situated and includes money; all forms of property, real or personable, heritable or moveable; things in action and other intangible or incorporeal property".

A property is obtained if an interest is obtained in it.

The definition of a 'property' is deliberately wide and the criminal courts have shown no difficulty in the application of this section. Unlike the courts in civil fraud claims, the criminal courts have not troubled themselves with issues of equitable tracing or beneficial ownership and have applied a broad interpretation to the issue of obtaining an interest in property.

'Criminal conduct' is any conduct that is either

PwC's implementation

Andrew Clark, Partner, and
Marie-Alice Hofmaier, Manager, PwC

As this chapter demonstrates, there is a legal duty for businesses in the regulated sector to report suspicions of money laundering. A failure to report carries severe financial and custodial penalties.

Furthermore, the Financial Services Authority (FSA) Handbook requires senior management to ensure that adequate systems and controls are in place to prevent their firm from being used for money laundering or terrorist financing. Extensive industry guidance has been produced in this area by the Joint Money Laundering Steering Group (www.jmlsg.org.uk).

In order to ensure that they meet their obligations, firms should focus on knowing their customers and on their methods for transaction monitoring, record keeping, training and reporting. In addition, the tone from the top is vital in ensuring that a company's anti-money laundering (AML) programme functions properly.

Know your customers

To be able to identify any money laundering or terrorist financing, it is vital that a company knows its customers. Being aware of their background, the source of their wealth and any funds received, as well as their normal transaction patterns, is the basis for detecting any suspicious activities.

Transaction monitoring involves spotting unusual patterns and this cannot be done without first establishing what is normal for a given customer.

Transaction monitoring

The nature and extent of the monitoring itself will vary between institutions according to their size (smaller companies often use more manual, less sophisticated solutions) and the profile of their customers, as well as the product range on offer. The higher the customer and product risk profile, the more rigorous the transaction monitoring should be.

Equally important, the institution must devote sufficient resources to reviewing the results of the

focus: anti-money laundering

monitoring. Alerts must be investigated and followed up in a timely manner.

Record keeping

Record keeping is a legal obligation under the AML regime. Firms should keep records of the due diligence performed on their customers (both identification and verification). They should also keep historical transaction data.

Both of the above help companies when they are required to investigate an alert. For example, a firm may be able to establish links between various affiliated money launderers by working through the historical transaction data relating to an account where an alert has been raised.

From time to time, firms may also be required to co-operate with the authorities (both in the UK and overseas) by supplying customer due diligence or transaction data.

Training

In order to equip staff with the necessary skills to spot any money laundering or terrorist financing, it is vital to give them adequate training. This should be tailored to the institution and to the various people and divisions within it.

For example, foreign exchange traders, who operate in a market that is considered higher risk than most, should receive enhanced training to enable them to detect any illegal activity.

Staff should also be trained to act upon their suspicions, once they are formed. It is important to warn them about keeping the matter confidential, to ensure they do not inadvertently tip off a suspect.

Training is particularly important as awkward situations very often develop during the period between the report of a suspicion to SOCA and the receipt of permission to proceed with a transaction. Staff need to be able to maintain engagement with the customer without making them aware that such a report has been made.

Employees should be trained to take the advice of the compliance team, who will be able to guide them through the most appropriate methods of communication.

Reporting

The instinct to report suspicions as a matter of course, and with the right degree of urgency, should be developed through training but will also depend on the tone from the top. Occasionally there is a perceived conflict between commercial interests and AML regulatory obligations. Additionally, some individuals are incentivised in a way that could encourage them to turn a blind eye to suspicions in order to maximise profits and thus their own bonus.

It is in the best interest of a firm and its employees to follow applicable law and regulations. Quite apart from fines and potential custodial sentences, the intensified supervision (including the imposition of extensive remediation exercises) by the regulator has the potential to be extremely costly. The senior management team needs to make it clear that there is a zero tolerance policy on money laundering and terrorist financing and that adherence will be rewarded (and non-compliance punished).

There should be a clear and well-publicised method for airing concerns with the money laundering reporting officer (MLRO). The method should also be relatively straightforward, so as not to discourage reporting. It is important to keep good records of all reports made and how they have been treated, including any onward reports to SOCA. MLROs will want to include information about this in their annual report, which is required by the Financial Services Authority.

Regulators will often review this information with interest as it can be a good indicator of the strength of the AML systems and controls at an institution. Regulators are aware of reporting trends across all regulated entities and are therefore able to spot over- or under-reporting.

Under-reporting is obviously undesirable. Over-reporting is not useful either as providing a deluge of information of little value does not demonstrate that an institution has implemented a robust risk-based approach.

By bearing these various points in mind, regulated firms should be in a good position to protect themselves from the consequences of failing to adhere to the reporting regime.

an offence in the UK or would be if it occurred there. This is subject to an amendment introduced by the Serious Organised Crime and Police Act (SOCPA) 2005, which decriminalises conduct that is lawful abroad.

A person benefits from conduct if he obtains property as a result of, or in connection with, the conduct.

Knowledge or suspicion

The knowledge or suspicion must coincide with the act of the offence itself. The UK courts have confirmed that the words 'knowledge' and 'suspicion' are to be given their ordinary meaning and usage in this context.

Affirmative defences to money laundering offences

Authorised disclosures

If the person makes an authorised disclosure to SOCA before acting and receives the appropriate consent, then, under Section 338 of POCA, an affirmative defence is provided and a money laundering offence is not committed. An offence is also not committed if the person intended to make a disclosure but failed to do so with a reasonable excuse. There is no statutory definition of 'reasonable excuse' and this defence is rarely likely to be available.

Under Section 105 of SOCPA 2005, it is now an offence to make a disclosure other than in the prescribed form; the penalty is a fine not exceeding Level 5 (£5,000). Disclosures are made to the Financial Intelligence Division of SOCA, whose website (www.soca.gov.uk) gives guidance on the procedure and displays the disclosure forms, which should be filed electronically. It is now possible to submit limited intelligence reports.

Generally, disclosures to SOCA should contain a reason for the report, sufficient information to enable the authorities to identify relevant individuals, and any information that discloses suspected criminal activity. SOCA will not provide advice as to whether a report should be made.

If the disclosure is made to SOCA as a result of issues arising in an ongoing transaction, then the report should specifically request consent to continue that transaction.

Following the submission of a report, no action should be taken until one of the following occurs:

- within seven days, SOCA gives notice and consent to proceed
- within seven working days, SOCA gives refusal of consent to proceed
- there is no further communication from SOCA within 31 calendar days, in which case consent is deemed to have been given.

In theory, if SOCA refuses consent within seven days, it will then take action in relation to the subject matter of the report – for example by obtaining a freezing order against the relevant property. However, if no action is taken during the 31-day moratorium period, it is open to the party to proceed. In most circumstances, SOCA promptly replies to any report and action is likely to be taken by the relevant enforcement authority. In the event that this does not take place, caution should be exercised in relation to any transaction and further communication with SOCA is strongly recommended before any further action is taken.

Extra-territorial legality

Section 102 of SOCPA introduced a further defence to the money laundering offences under Sections 327-329 of POCA, and the failure-to-disclose offences under Sections 330-332, where the person knew, or believed on reasonable grounds, that the relevant criminal conduct occurred in a country or territory outside the UK where the conduct was not unlawful at the time it occurred. This defence does not apply where the relevant conduct is of a type described by an order made by the government.

Threshold amounts

Section 103 introduced an exemption to the obligation to make an authorised disclosure, in

respect of Sections 327-329 of POCA, and inserted a new Section, 339A, on threshold amounts. Under Section 327 of POCA, a bank or other deposit-taking body would need to make a disclosure to obtain consent before proceeding with any transaction suspected of involving criminal property. The amendment allows deposit-taking bodies to continue to operate accounts without the need to seek consent in each case.

A bank or other deposit-taking body does not commit an offence in operating an account of a person suspected of money laundering when the amount of money concerned in the transaction is below £250 (or such higher threshold amount as may be specified by a constable or an officer of Revenue and Customs, or by the director-general of SOCA). Where a deposit-taking body requests a threshold amount higher than the £250 default, one may be specified. The threshold can be varied by order of the government.

Inability to identify

Section 104 of SOCPA amends the failure-to-disclose provisions in Sections 330-332 of POCA. The obligation to disclose suspicions of money laundering will apply only if the person required to make a disclosure knows the identity of the person engaged in the money laundering offence or the whereabouts of any of the laundered property – or if the information that would have to be reported discloses, or may assist in uncovering, the identity of the person engaged in that offence or the whereabouts of any of the laundered property.

Adequate consideration

In addition to the affirmative defences made under Sections 327 and 328, the person does not commit an offence if he acquired, used or had possession of the property for adequate consideration. If a person acquires property for inadequate consideration then the value of the consideration is significantly less than the value of the property. The provision by a person of goods or services that he knows or suspects may help another to carry out criminal conduct is not consideration.

Failure to report offences

Under Section 330 of POCA, a person in the regulated sector commits an offence if he knows or suspects – or has reasonable grounds for knowing or suspecting – that another identified person is engaged in money laundering and he fails to make the required disclosure to a nominated officer or to SOCA as soon as is practical after the information is given to him.

The offence is punishable with up to five years' imprisonment and/or a fine.

A person is required to disclose the identity of the person engaged in money laundering, the location of the laundered property or any other information that may assist in identifying the relevant person and property. Under Section 339, the government has the power to specify the manner and form of disclosures. Additionally, under Section 105 of SOCPA, it is an offence not to make a disclosure in the prescribed form.

There is a specific exception to the commission of this offence, where a person in the regulated sector has not been provided with sufficient training in relation to money laundering.

An offence is also not committed if the person had a reasonable excuse for not making the required disclosure or he is a professional legal or other relevant adviser and the information came to him under privileged circumstances (an exemption that is distinct from legal professional privilege). These circumstances arise where the information is communicated or given by a client or his representative or in connection with the giving of legal advice to a client, or by a person or his representative seeking legal advice, or by a person in connection with actual or contemplated legal proceedings. The privilege exemption does not apply to information communicated with the intention of furthering a criminal purpose.

Whether a business is in the regulated sector is set out in Schedule 9 of POCA.

Case study

In *R v Da Silva* (2006), it was held:

- (i) that where the *mens rea* of an offence required suspicion on the part of the defendant as to the existence of a particular fact, a judge could not be criticised if he declined to define 'suspicion', other than by saying that it was an ordinary English word and that the jury should apply their own understanding of it
- but (ii) that the mere fact a word is an 'ordinary English word' within *Brutus v Cozens* (1973) does not prevent a judge from providing assistance to the jury as to its meaning
- (iii) that where such assistance is provided, in the absence of judicial authority, the dictionary definition would be likely to be an appropriate starting place
- (iv) that in the context of the money laundering offences created by the Criminal Justice Act 1988, what was required was that the defendant had to have thought there was a possibility, which was more than fanciful, that the relevant fact existed – and while a vague feeling of unease would not suffice, there was no requirement for the suspicion to be 'clear' or 'firmly grounded and targeted on specific facts', or based upon 'reasonable grounds' (other than where there was a specific requirement of 'reasonable grounds')
- (v) that if a judge felt it appropriate to assist the jury with the word 'suspecting', a direction along these lines would ordinarily be adequate
- (vi) that a more careful direction might be required where there was reason to suppose that the defendant's suspicion was not of a settled nature, such as where he had entertained a suspicion (as defined) but, on further thought, had dismissed it from his mind as being outweighed by other considerations
- and (vii) that use of words such as 'inkling' or 'fleeting thought' to explain the meaning of suspicion was liable to mislead; if they were to be used, they should ordinarily be combined with the more careful direction referred to in (vi).

Reasonable grounds to suspect

The test for knowledge and suspicion under Sections 327-329 is a subjective one. The offence in Section 330 introduces the objective test of having reasonable grounds to suspect. Under Section 330, it is not necessary to show that the defendant actually suspected money laundering was taking place but that an objective observer would conclude money laundering was taking place. It envisages a reasonable person engaged in a business similar to the regulated entity. The offence is essentially one of criminal negligence.

Section 331: failure by a nominated officer in the regulated sector

Under Section 338, a person may be nominated to receive disclosures by his employer. This nominated officer is also known as the money laundering reporting officer.

It is an offence for the nominated officer not to make a disclosure to SOCA where he has received a disclosure and knows or suspects – or has reasonable grounds to know or suspect – that a person is engaged in money laundering and that relevant property and/or an individual can be identified.

The offence carries a sentence of up to five years' imprisonment and/or a fine.

A person does not commit an offence under Section 331 if he has a reasonable excuse for not making the required disclosure, or he believes on reasonable grounds that the money laundering occurred outside the UK and was not criminal in that territory and not of a description set out under order of the government.

A disclosure made to a nominated officer in these circumstances will not be privileged and so the defence does not apply in these circumstances.

Section 322: offence by other nominated officers

Where a nominated officer who is not in the regulated sector receives a disclosure that causes him to know or suspect that money laundering has taken place, then it is an offence not to make the required disclosure to SOCA.

The offence is punishable with up to five years' imprisonment and/or a fine.

As under Section 331, it is not an offence if the person has a reasonable excuse or any extra-territorial exceptions to apply. Again, reports made to nominated officers are not privileged.

Section 333A: tipping-off offence

Where there has been a disclosure to a constable, officer of Revenue and Customs, a nominated officer or SOCA, a person commits an offence if he discloses any matter in relation to it and that disclosure is likely to prejudice an investigation. The person must have subjective knowledge or a suspicion that the disclosure is likely to prejudice any potential investigation.

This offence can only be committed by those in the regulated sector. It is punishable with up to five years' imprisonment and/or a fine.

The offence is not committed if the disclosure is between those within an undertaking or group, or between institutions or professionals or anti-money laundering authorities, or is made by a professional legal or other relevant adviser to the client for purposes of dissuading the client from committing a crime.

Section 342: prejudicing an investigation

Under Section 342, it is an offence for a person to make a disclosure that is likely to prejudice an investigation, or to falsify, conceal, destroy or otherwise dispose of documents relevant to an investigation. The person must suspect the disclosure was likely to prejudice the investigation, or intend to destroy the documents relevant to the investigation, or intend to conceal the facts disclosed by the documents. The offence is punishable with up to five years' imprisonment and/or a fine.

17

Serious financial crime in the financial services sector

Stephen Gilchrist, Solicitor and Director Saunders Law Ltd

We live in a world of uncertainty. The longer-term future of a standalone Serious Fraud Office (SFO) is in doubt although for the time being it will continue to work with the economic crime command within the National Crime Agency – as it will with the City of London Police and other relevant criminal justice agencies at home and abroad.[1]

Meanwhile, the Financial Services Authority (FSA) is being abolished in 2012 in favour of two new agencies – the Prudential Regulation Authority and the Financial Conduct Authority – and its enforcement powers transferred.

The Financial Services and Markets Act

Under the Financial Services and Markets Act 2000 (FSMA), one of the statutory objectives of the FSA is "the reduction of financial crime – reducing the extent to which it is possible for a regulated business to be used for a purpose connected with financial crime".

This broad objective rather understates the enforcement powers of the regulator, since, apart from Part V of the Criminal Justice Act 1993 (which sets out the criminal offence of insider dealing, for which the FSA is a prosecuting authority), it has the power to prosecute several specific offences relating to regulated activities. Some of these are 'summary' and can only be dealt with by the magistrates' courts. Others are 'indictable' and can only be heard in the crown court, where a jury decides on guilt. Yet others are 'either way', and so can be tried either in a magistrates' or crown court. Punishments include fines at various levels and imprisonment for up to seven years.

Jurisdiction to prosecute and the relationship between the FSA and SFO

The SFO, as its name implies, concentrates on investigating and prosecuting fraud – that is, acts of deception intended for personal gain or to cause loss to another. Of course, fraud comes in many flavours and is usually a civil wrong as well as a crime. Both the SFO and FSA are empowered to take civil proceedings to secure the proceeds of crime, including funds believed to have been salted away abroad.

After a conviction for fraud, the court will invariably be asked to consider making a confiscation order under the Proceeds of Crime Act 2002 (POCA)

for the lesser of any benefit from the crime, or all the defendant's net assets. A default prison sentence of up to ten years consecutive will be imposed, and so in FSMA cases this penalty may exceed the sentence for the crime itself. A restraint order may also be granted to the prosecutor even at the investigative stage to prevent dissipation of assets.

The SFO may also prosecute on behalf of the FSA and works closely with external agencies such as the FSA.

Significantly, however, in the 2010 Supreme Court case of *R v Rollins (Neil)* and *R v McInerney (Michael)*, it was decided that the FSA's powers to prosecute criminal offences were not limited to the offences set out in FSMA Sections 401 and 402. So in *Rollins* the FSA had the power to prosecute offences of money laundering contrary to POCA Sections 327 and 328.

Essentially, the FSA can act as a private prosecutor, since generally any person can bring a private prosecution. Clearly, money laundering can be a consequence of the commission of an offence under the FSMA, such as carrying on a regulated activity without authorisation.

Impact on victims

Arguably the most serious offences under the FSMA are those of carrying on a regulated activity without authorisation and making misleading statements to induce investments.

Doing so can have very serious consequences for the victim or consumer, who will typically have 'invested' large amounts of money in unauthorised schemes, which often take the form of collective investment schemes (CIS), and will be unable to recover their money from the unauthorised operators of the scheme.

Neither will they have access to the Financial Ombudsman Service if they wish to make a complaint, and they will not be covered by the Financial Services Compensation Scheme.

Increasingly the FSA will obtain civil freezing orders against these operators, but in practice it is often too little too late, despite the fact that under Section 26 of the FSMA "an agreement made by a person in the course of carrying on a regulated activity in contravention of the general prohibition is unenforceable against the other party".

Such activities may have generic characteristics – they may be pyramid or 'easy money' schemes – that make any recovery all but impossible. 'Boiler rooms', which sell often worthless investments and target UK-based consumers though they are operated from abroad, may also fall into this category since communicating an inducement or invitation to engage in investment activity (in the absence of authorisation) is also prohibited under Section 21 of the FSMA – if it is "capable of having an effect in the United Kingdom".

Offences under the FSMA

The most serious criminal offences and incidents of misconduct in the financial services sector that fraud practitioners are likely to encounter are:

- carrying on a regulated activity without authorisation. This is described in Sections 19 and 23 of the FSMA as a breach of the general prohibition
- communicating an invitation or inducement to engage in investment activity
- making misleading statements to induce investments.

Carrying on a regulated activity without authorisation

Section 19 of the FSMA provides that no person may carry on a regulated activity in the United Kingdom, or purport to do so, unless he is an authorised person or an exempt person. The prohibition is referred to in this Act as the 'general prohibition'.

Under Section 23 of the FSMA, it is a criminal offence to contravene the general prohibition and punishable in the magistrates' court with six months' imprisonment and/or a fine of £5,000; in the crown court it is punishable with two years' imprisonment and/or an unlimited fine.[2]

The offence is committed through breach of

the prohibition and no specific intent is required, although it is a defence under Section 23 for "the accused to show that he took all reasonable precautions and exercised all due diligence to avoid committing the offence". The issues are:

- **Is the accused carrying out a regulated activity?** An activity, for the purposes of this Act, is one of a specified kind that is carried on by way of business and (a) relates to an investment of a specified kind; or (b) is carried on in relation to property of any kind (Section 22). Schedule 2 of the FSMA (which has been subject to a series of amending orders) sets out the parameters of such activities and includes offering investment advice, deposit taking, managing investments and establishing a collective investment scheme.[3]
- **Is the regulated activity being carried out in the UK?** Section 418 elaborates on when regulated activities will be considered to be carried out in the UK and also relevant is Section 21 of the FSMA, as described above.
- **If so, is the accused an authorised or exempt person?** Those who are authorised persons are set out in Section 31 of the Act and in most cases will have FSMA Part IV permission to carry on one or more regulated activities. The Treasury may, by an exemption order, provide for specified persons, or persons falling within a specified class, to be exempt from the general prohibition.
- **Even if the accused is not actually carrying out a regulated activity, is he purporting to do so?** It is likely that the reasoning in *Securities and Investments Board v Scandex Capital Management A/S* (1998), in relation to the equivalent provisions in the Financial Services Act 1986, will be held to apply to the FSMA – and a mistake of law as to the need for authorisation will therefore not give rise to a defence.[4]
- **Has the accused taken all reasonable precautions and exercised all due diligence to avoid committing the offence?** The evidential burden is on the accused to prove this on a balance of probabilities.

Collective investment schemes

Establishing, operating or winding up a collective investment scheme constitutes a regulated activity. Such schemes are described in Section 235 of the FSMA as:

> *(1) … any arrangements with respect to property of any description, including money, the purpose or effect of which is to enable persons taking part in the arrangements (whether by becoming owners of the property or any part of it or otherwise) to participate in or receive profits or income arising from the acquisition, holding, management or disposal of the property or sums paid out of such profits or income.*
> *(2)The arrangements must be such that the persons who are to participate ('participants') do not have day-to-day control over the management of the property, whether or not they have the right to be consulted or to give directions.*
> *(3)The arrangements must also have either or both of the following characteristics –*
> *(a) the contributions of the participants and the profits or income out of which payments are to be made to them are pooled;*
> *(b) the property is managed as a whole by or on behalf of the operator of the scheme.*

Under FSMA Section 238 (Restrictions on promotion), only certain kinds of collective investment scheme may be promoted to the public by an authorised person.

Under Section 284, the FSA or the Secretary of State can appoint a person to carry out an investigation into a collective investment scheme.

Very often an investigation into a breach of the prohibition will reveal, or arise from, the operation of a CIS. Of course not all these schemes are illegal; a classic CIS is a unit trust, which is generally operated under appropriate FSA authorisation by a reputable body. However, other types of unauthorised scheme that have been investigated, and sometimes prosecuted, include the provision of a betting service that involved collecting money from the public and placing bets on their behalf on horse races.[5]

Another example was an 'easy money' scheme in which a substantial investment business primarily involved investing in a pyramid scheme (see the case study below).

Recently, there have also been a number of so-called 'land banking' schemes, which involve persuading people to invest in plots in the green belt, on the improbable basis that the land will rocket in value when planning permission is secured for building houses; the profits to the unauthorised land bankers from buying land at agricultural prices and selling for development have been phenomenal.

The CIS issue here is an alleged promise by the operators to apply for planning permission on behalf of the plot buyers, or otherwise manage the plots for them after purchase. The FSA takes the position that this amounts to the pooling of assets and depriving the plot holders of day-to-day management. Although trading in land is not in itself a regulated activity under the FSMA, the property concerned in a CIS can be any property, including land.

In some of these cases, the offences of fraud by misrepresentation and money laundering[6] are also engaged.

Communicating an invitation or inducement to engage in investment activity

Section 23 of the FSMA provides that a person must not, "in the course of business, communicate an invitation or inducement to engage in investment activity" save where the person is an authorised person or where "the content of the communication is approved for the purposes of this section by an authorised person".

An offender is liable on summary conviction to imprisonment for up to six months and/or a fine not exceeding £5,000, and on indictment up to two years' imprisonment and/or an unlimited fine.

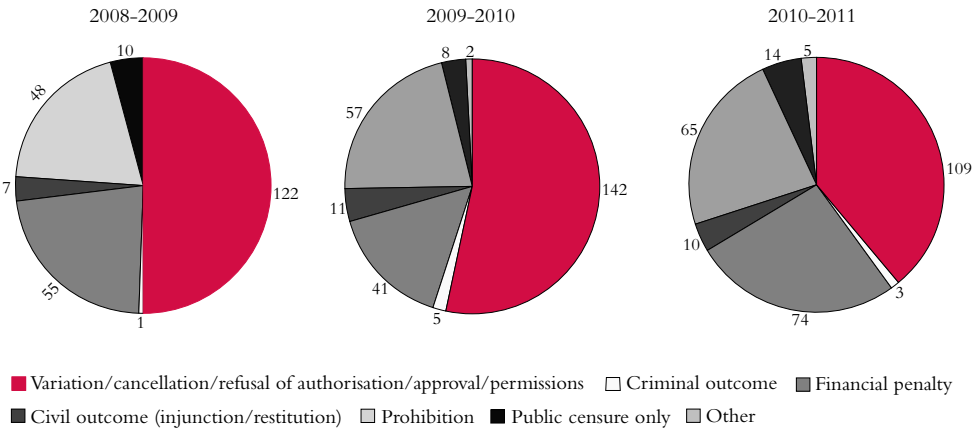
Detailed issues that may arise are:

- **Is the communication in the course of business?** Normally this will be a straightforward issue, but the Treasury may specify circumstances in which a person is deemed to be acting in the course of business, or not.
- **Is there a communication?** 'Communicate' includes causing a communication to be made and Order 2005 (Financial promotion) in the FSMA deems what may be a 'communication'. It may be, for example, to an individual, or a class or group of persons, by written, electronic or other means.[7]
- **Is there an invitation or inducement?**
- **Is there engagement in an investment activity?** 'Engaging in investment activity' means (a) entering or offering to enter into an agreement – the making or performance of which by either party constitutes a controlled activity; or (b) exercising any rights conferred by a controlled investment to acquire, dispose of, underwrite or convert a controlled investment (Section 21). Clarification of 'controlled activity', 'controlled investment', 'specified class of activity' and 'specified class of investment' is provided in separate FSMA Orders.
- **Is there a defence?** Under Section 25 of the FSMA, it is a defence for the accused to show that he believed on reasonable grounds that the content of the communication was prepared or approved by an authorised person, or that he took all reasonable precautions and exercised all due diligence to avoid committing the offence. Under Section 21, in the case of a communication originating outside the UK, the restriction applies only if the communication is capable of having an effect in the UK.

Misleading statements and practices

Section 397 of the FSMA creates criminal offences concerning misleading statements and practices, punishable by up to seven years' imprisonment and/or an unlimited fine. An offence is committed where a person deliberately makes a misleading statement, promise or forecast, or dishonestly conceals facts from someone with

The use of powers by the FSA: outcomes of cases



the intention of inducing another to do, or refrain from doing, something in relation to an investment. A possible example of this offence would be someone lying about a company's financial position at a time when he was seeking to dispose of shares in that company,[8] but it can also include misleading information communicated to prospective investors in an unauthorised CIS.

A person is guilty of an offence if he:

- makes a statement, promise or forecast that he knows to be misleading, false or deceptive in a material particular
- dishonestly conceals any material facts whether in connection with a statement, promise or forecast made by him or otherwise
- recklessly makes (dishonestly or otherwise) a statement, promise or forecast which is misleading, false or deceptive in a material particular ...
- for the purpose of inducing, or is reckless as to whether it may induce, another person to enter, or refrain from entering, a relevant agreement, or to exercise, or refrain from exercising, any rights conferred by a relevant investment.

A 'relevant agreement' is one that constitutes an activity of a kind specified in Section 397 of the FSMA, or falls within a specified class of activity; and relates to a relevant investment.

A further offence is committed, under Section 397, by a person who engages in any course of conduct that creates a false or misleading impression as to the market in, or the price or value of, any relevant investments – if he does so for the purpose of creating that impression and of thereby inducing another person to acquire, dispose of, subscribe for or underwrite those investments, or to refrain from doing so, or to exercise, or refrain from exercising, any rights conferred by those investments.

There is a statutory defence under Section 397 if the accused can show:

- that he reasonably believed his actions or conduct would not create an impression that was false or misleading
- that he acted, or engaged in the conduct, for the purpose of stabilising the price of investments, and in conformity with price-stabilising rules
- that he acted in conformity with control-of-information rules

- that he acted in conformity with the relevant provisions of Commission Regulation (EC) 2273/2003.

Section 397 does not apply unless the act is carried out, or the course of conduct engaged in, in the UK, or the false or misleading impression is created there. It is important to note that these offences may be committed by unauthorised persons, such as those who are in breach of the general prohibition, by, for example, running an unauthorised CIS.

Other offences that may arise in fraud investigations are:

- it is an offence under Section 24 to falsely claim to be authorised by the FSA or to be an exempt person, or to behave as such although the due-diligence defence is available. This is a summary offence for which the sanction is six months' imprisonment and/or a £5,000 fine. The fine may be increased if there is a public display of any misleading material
- it is an offence under Section 398 to knowingly or recklessly give the FSA information that is false or misleading in a material particular in purported compliance with any requirement under the FSMA. In either a magistrates' court or a crown court, this is punishable by a fine.

Case study: Kevin Foster

In 2010, Kevin Foster was convicted of defrauding investors through his various schemes, collectively known as the KF Concept. Foster attracted £34 million from investors by promising very high returns on a variety of gambling and network marketing activities. It was alleged that little of the money was in fact used for such activities, but that millions were poured into an offshore pyramid scheme. Meanwhile, Foster paid himself and his close associates handsomely from KF Concept money and they lived extravagant lifestyles. The case was prosecuted by the SFO on behalf of, and in conjunction with, the FSA, which had previously investigated and intervened in the KF Concept with civil freezing orders.

Foster was charged with eight offences under the FSMA and eight offences under the Theft Act 1968. The FSMA offences included:

- communicating an investment or inducement to engage in investment activity, contrary to Sections 21and 25
- not being an authorised person carrying on a regulated activity, contrary to Sections 19 and 23.
- concealing a material fact, contrary to Section 397.

Foster was said to have promised unrealistic returns on a series of gambling schemes initially based on football league betting, and increasingly on a pyramid scheme format. His personal charisma and his 'magic touch' were central to the marketing. His schemes were said by the SFO to have had the characteristics of a collective investment scheme in that investors' money was pooled, the pool was managed by Foster, and the investors had no day-to-day control over their funds.

Communication

Communication was by word of mouth – via family and friends and friends of friends and so on – and was important as a means of raising money. But a major fundraising strategy for the scheme was the holding of roadshows nationwide. These became increasingly well attended and successful in raising money. They would usually include what was described by the SFO as a barnstorming and rabble-rousing talk by Foster, full of confidence, optimism and bluster, but short on detail.

Carrying on a regulated activity

It was the SFO's case that Foster had established and was operating a CIS by virtue of the characteristic structures of his schemes. It did not matter how he described them, or that his schemes

concerned products that were not regulated, if the reality was that he was operating a CIS.

Concealing a material fact

A multitude of claims of financial security and stability were made, which were said to have been false and/or highly misleading. Examples of this were:

- "The scheme makes its money from gambling wins and network marketing"
- "The scheme is worth £200m in the bank" "I'm making about £28.50 from every £1"
- "One of my networks is making me about £1.5 million a month"
- "We've got offices in X number of countries"
- "This scheme has got 50,000 people in it".

It was said that these and other statements were untrue, misleading or grossly extravagant.

The defendant was ultimately sentenced at the crown court to a total of eight years for the FSMA offences, reduced by the Court of Appeal to seven years. In combination with additional counts under the Theft Act 1968, he received a total of ten years, reduced on appeal to nine.

Many early investors had in fact been paid out by the time the FSA stepped in and halted the scheme in 2004, but this was from funds paid in by later investors, who were not so fortunate. The schemes ran for three years and the £34 million came from more than 8,500 investors, some of whom lost enormous sums of money. One investor who put in £180,000 said: "I never thought that I was stupid, but I was convinced by him, and thousands of others were too."

It could be said that the successful operation of such schemes is dependent on the greed of the participants and their absurd belief in the promises of easy and fabulous riches. But, as can be seen, the courts are not in consequence inhibited from passing heavy sentences on offenders.

18

Economic sanctions laws: the European Union and the United States

Greta Lichtenbaum, Partner (Washington DC), James Barratt, Counsel (London), and Hayley Ichilcik, Associate (London) O'Melveny & Myers LLP

The European Union and the United States have both enacted – albeit with varying scope and frequency – economic sanctions to support foreign policy goals. The response of anti-democratic regimes to the wave of popular uprisings in North Africa and the Middle East since late 2010 has resulted in a host of stringent new sanctions targeting governments, individuals and entities, casting a spotlight on this dynamic area of law. Non-compliance with these restrictive measures could result in potentially significant liability and reputational damage.

As this chapter was being finalised, the latest events in both Syria and, in particular, in Libya served to emphasise the evolutionary nature of the economic sanctions regimes imposed by the EU and US in response to political developments.

Overview

Under the United Nations Charter, the Security Council is charged with the responsibility of maintaining international peace and security. The Security Council is empowered to introduce certain sanctions, by way of resolutions, in the event that it determines the existence of any threats to the peace, breaches of the peace or acts of aggression in or against any state. The sanctions can include comprehensive economic and trade penalties and/or more targeted measures such as arms embargoes, or financial, travel or diplomatic restrictions.

As members of the UN, the 27 EU member states and the US are legally obliged to implement the measures adopted by a resolution of the Security Council. Individual states may also adopt unilateral measures.

This chapter explores the EU and US sanctions regimes imposed on Iran, Libya, Syria, Sudan, North Korea, Burma and Cuba, as well as sanctions targeting particular individuals and entities. It concludes with a discussion of the increasing enforcement in both the EU and US. Compliance with these laws is a critical component of any company's ethics and compliance programmes, particularly for those that operate in multiple jurisdictions.

European Union mechanisms for the adoption of economic sanctions

The EU adopts sanctions regimes in accordance with the objectives of its Common Foreign and Security Policy (CFSP). Following the European Council's adoption of a 'common position' that resolves to limit trade or

economic relations with a target country, sanctions may be implemented either directly at national level (if they relate to arms embargoes or travel prohibitions), or through a specific regulation approved by the European Council (if they relate to prohibitions on providing financial or technical assistance).

Once approved, EU regulations have direct effect on all member states and are required to be implemented in a proper and timely manner, taking precedence over any conflicting domestic legislation. Any failure in this respect may result in infringement proceedings being brought against the offending state.

EU sanctions also have direct effect on nationals of EU states (regardless of their location), companies incorporated within the EU wherever they do business, and companies that do business within the EU wherever incorporated. Given the broad application of the sanctions regimes, even non-EU companies with no visible connection to the EU could fall within their scope.

United States mechanisms for the adoption of economic sanctions

In recent years, the US has resorted comparatively often to economic sanctions to further its foreign policy and national security goals. In some cases, these measures have served to implement UN resolutions. Just as frequently they have been unilateral. These sanctions rules prohibit US persons from doing business with specific countries, companies and individuals, and sometimes extend (not without international controversy) to foreign entities. Violations may result in severe criminal and civil penalties.

The US President has the authority to impose economic sanctions under various statutes, among which the one most frequently invoked by the President is the International Economic Emergency Powers Act (IEEPA). The US Treasury's Office of Foreign Assets Control (OFAC) is responsible for implementing most economic sanctions laws and regulations, and while it is the President who typically initiates these measures, in some situations – Syria, for example – they are imposed through an Act of Congress.

Additionally, the US Commerce Department's Bureau of Industry and Security (BIS) administers parallel export control laws, which work in conjunction with the sanctions laws. These restrict the export and re-export of sensitive goods, software or technology of US origin.

Sanctions are either applicable to particular countries or governments, or are more targeted against certain individuals and entities engaging in activities inconsistent with US interests. Such parties are on the OFAC list of Specially Designated Nationals and Blocked Persons (the OFAC Prohibited Parties List).

Sanctions against Iran

European Union

Council Regulation (EU) No 961/2010 of October 2010, as amended (the Iran Regulation), forms the bedrock of the EU sanctions regime against Iran, setting out a broad spectrum of restrictions in relation to the energy, financial, insurance and transport industries, and enterprises associated with the Iranian government and the country's nuclear industry. It confirms the restrictive measures taken since 2007 and imposes additional restrictions in order to comply with the 2010 UN resolution as well as to enforce accompanying measures requested by the European Council.

The Iran Regulation imposes:

- an asset freeze
- restrictions on transfers of funds to and from Iran
- an arms embargo
- restrictions on trade in key equipment and technology used in the Iranian oil and gas industry.

Asset freeze

This extends to all funds and economic resources of sanctioned entities that are listed in annexes to the Iran Regulation. The freeze implements a

broad prohibition on any dealings with funds that would result in any change whatsoever to their character, and prevents the use in any way of every kind of asset that may be used to obtain funds, goods or services. As well as placing a freeze on the funds and resources belonging to, or owned, held or controlled by designated entities, the Iran Regulation forbids transactions that might directly or indirectly benefit such entities.

Restrictions on transfers of funds to and from Iran

The Iran Regulation also enforces notification and authorisation controls on the transfer of funds above certain thresholds to and from non-sanctioned Iranian persons and entities – widely defined to potentially include persons and entities *outside* Iran. Notification is required for transfers valued over €10,000, while authorisation is required for transfers of more than €40,000 (with certain exceptions, such as for humanitarian aid).

Arms embargo

Another key feature of the Iran Regulation is the prohibition on any sale, supply, transfer or export (directly or indirectly) of specified goods that could potentially contribute to the development of Iran's nuclear weapons delivery systems, including items with dual military and civilian application. Similar controls apply with regards to the importing or transporting of such goods from Iran, and with regard to equipment that might be used for internal repression.

The provision of financing, financial assistance, technical assistance or brokering services ('related services') in relation to the above, and additionally in relation to the goods and technology listed in the EU's Common Military List, is also prohibited.

Restrictions in respect of the Iranian oil and gas industry

One controversial aspect of the Iran Regulation is that it bans the sale, supply, transfer or export (directly or indirectly) of key equipment and technology related to the Iranian oil and gas industry. The provision of related services is prohibited. There is also a prohibition on any investment in these industries. These stringent restrictions have resulted in several oil companies ceasing to operate in Iran and a sharp decline in foreign investment.

Notably, the Iran Regulation explicitly states that restrictive measures should not affect the import or export of oil or gas to and from Iran, including the fulfilment of payment obligations.

Other restrictions

The Iran Regulation also includes restrictions on: the country's banking sector (including enhanced due diligence requirements for EU financial institutions); Iranian access to the EU's insurance and bonds market; Iranian investment in the uranium-mining and nuclear industry; and providing certain shipping services to Iran.

United States

The US has maintained comprehensive economic sanctions against Iran since 1995, both for its alleged nuclear weapons programme and because it is viewed as a state sponsor of terrorism. These unilateral sanctions are implemented through the Iranian Transactions Regulations (ITRs). Separately, the US has implemented various UN Security Council resolutions that target Iran's nuclear and ballistic missile programmes, while in 2010 Congress passed the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA), which principally targets non-US companies conducting certain business in Iran or with the Iranian government – specifically, activities that support aspects of Iran's energy sector, its nuclear and ballistic missile programmes, and its alleged terrorism activities.

The ITRs

These regulations are very broad, restricting virtually all commercial trade with Iran. They generally apply only to 'US persons', defined as including any entity established under US law (including foreign branches, but not foreign subsidiaries), US citizens and permanent residents,

and anyone in the US (including, for example, a foreign citizen acting on behalf of a non-US company, while that person is in US territory).

The ITRs prohibit US persons from:

- investing in Iran or performing contracts relating to the development of petroleum resources located in Iran
- the "exportation, re-exportation, sale or supply, directly or indirectly, from the United States, or by a US person, wherever located, of any goods, technology, or services to Iran or the Government of Iran". These prohibitions are mirrored on the import side
- engaging "in any transaction or dealing in or related to: (a) goods or services of Iranian origin or owned or controlled by the Government of Iran; or (b) goods, technology, or services for exportation, re-exportation, sale or supply, directly or indirectly, to Iran or the Government of Iran".

In addition to these direct prohibitions, a key provision in the ITRs is the facilitation prohibition. This provides that "no United States person, wherever located, may approve, finance, facilitate, or guarantee any transaction by a foreign person where the transaction by that foreign person would be prohibited … if performed by a United States person or within the United States". Although there is no formal definition of 'approval' or 'facilitation' – and they have been construed broadly by OFAC – the ITRs contain examples of conduct that fall within the scope of the prohibition, such as the referral of specific business opportunities with Iran to a non-US person.

Sanctions targeting specific activities in Iran

Separately from the ITRs, US economic sanctions target Iranian parties suspected of being involved in the proliferation of weapons of mass destruction. These sanctions were expanded in 2010 following action in the United Nations. Such entities (including many Iranian banks) are listed on the OFAC Prohibited Parties List.

In addition, in 2010 the US enacted CISADA, which amended and significantly expanded the Iran Sanctions Act 1996 (ISA) to create additional categories of activities that could subject non-US firms to sanctions, along with new types of sanctions that could be imposed on such firms. The new activities include those that support the production of refined petroleum products in Iran and the import of these products into the country. Also, CISADA targets foreign financial institutions that facilitate Iran's alleged nuclear programme and support for terrorism, and the activities of the country's Islamic Revolutionary Guard Corps.

The ISA applies to any person but primarily targets non-US persons because they are already prohibited from investing or trading with Iran under other US economic sanctions programmes. Under the ISA, sanctions are imposed if an investigation concludes that a prohibited activity has occurred. The President can waive the sanctions, and has done so in the past, but since the enactment of CISADA, the White House has had more limited discretion with respect to both launching investigations and granting waivers. As a result, the President has imposed sanctions on several entities since 2010.

Activities subject to sanctions under CISADA

Prior to the 2010 amendment, the ISA targeted investments of US$20 million or more "that directly and significantly contributed to the enhancement of Iran's ability to develop petroleum".

Now, the ISA can impose sanctions on persons who 'knowingly' engage in activities that could 'directly and significantly' facilitate or contribute to Iran's domestic production of refined petroleum products, or its ability to import such products – if such activities exceed a fair market value of US$1 million or more, or an aggregate fair market value of US$5 million or more in a 12-month period. Specifically, the amendments target the sale, lease or provision to Iran of:

- "goods, services, technology, information, or

support that could directly and significantly facilitate the maintenance or expansion of Iran's domestic production of refined petroleum products, including any direct and significant assistance with respect to the construction, modernization, or repair of petroleum refineries"
- refined petroleum products or "goods, services, technology, information, or support that could directly and significantly contribute to the enhancement of Iran's ability to import refined petroleum products", including activities such as underwriting, insuring, reinsuring, financing, brokering, or providing ships or shipping services.

There is an exception for underwriters and insurance providers who exercise due diligence to ensure they will not be involved with prohibited activities.

Menu of sanctions

If the President determines that a person engaged in specified activities is subject to sanctions, he must select from a menu of penalties. The ISA previously required the President to impose at least two of the following six sanctions:

- denial of export-import bank loans, credits or guarantees
- denial of licences to export military or militarily useful technology
- a prohibition on US financial institutions making loans or providing credit of more than US$10 million in any 12-month period (with minor exceptions)
- a prohibition on obtaining US government procurement contracts
- restrictions on imports into the US
- if the violator is a financial institution, a prohibition on being designated as a primary dealer in US government debt, and/or on acting as an agent for government funds.

The amendments added three new sanctions to this menu and the President is now required to select at least three of the nine now available. The new options would prohibit:

- foreign exchange transactions in the US
- the transfer of credits or payments by financial institutions in the US
- dealings in property in the US.

Sanctions against Libya

Libya is, at the time of writing, the subject of intense diplomatic attention. Following the effective ousting of Gaddafi and his supporters after 42 years of dictatorship, the restrictive measures against Libya have eased dramatically.

Most recently, following Gaddafi's downfall, the Security Council unanimously adopted UNSC 2009 (2011) on September 19, 2011.

The new resolution began the process of easing the UN sanctions against Libya imposed under UNSC 1970 (2011) and 1973 (2011). Notably, the Libyan National Oil Corporation and Zueitina Oil Company are no longer subject to the asset freeze. In addition, the new resolution has modified the measures imposed on the Central Bank of Libya, the Libyan Arab Foreign Bank, the Libyan Investment Authority and the Libyan Africa Investment Portfolio. In short, assets of these entities that have been frozen prior to the enactment of the new UN resolution shall, for now, remain frozen (subject to certain exemptions), but these entities shall not be subject to the freeze going forward.

The continued easing of sanctions against Libya by the UN (and, consequently, the EU and the US) is strongly anticipated.

European Union

Council Regulation (EU) No 204/2011 of March 2011, as amended (the Libya Regulation), imposes economic sanctions directed at the Gaddafi regime that basically replicate, although are in places broader than, the Security Council resolutions 1970 (2011) and 1973 (2011) that created the UN Libya sanctions regime. The Libya

Regulation enforces, primarily, an asset freeze and an arms embargo, including restrictions on equipment that might be used for internal repression.

Even before the new 2009 (2011) UN resolution, the EU had already begun to ease sanctions in light of the ongoing developments in Libya, as discussed below. It now appears inevitable that the EU will continue to further modify and substantially ease its sanctions regimes as it seeks to implement the new UN resolution.

Asset freeze

The asset freeze currently in force is largely akin to the freeze applied on Iran described above. However, the latest political developments in Libya have already seen those subject to the freeze significantly dwindle in number. This process is expected to continue.

Following the Libya Conference in Paris on September 1, 2011, which involved representatives from 60 nations meeting with the objective of restoring stability to Libya's economy, the EU amended the Libya Regulation, removing 28 entities from the sanctions list.

This will enable more commercial and financial interaction with the National Transitional Council (NTC), which has been recognised by many countries as Libya's new and legitimate governing authority.

Entities no longer subject to the asset freeze include a number of oil companies, financial institutions and Libyan ports. The British-registered company Tekxel is among the entities removed from the EU's blacklist. Afriqiyah Airways was also removed from the EU sanctions list on September 15, 2011.

Prominent entities that remain on the EU sanctions list include the Central Bank of Libya, the Libyan Investment Authority, the Libyan Foreign Bank, the Libyan African Investment Portfolio and the Libyan National Oil Corporation. Following the passage of UNSC 2009 (2011), the EU is expected to remove or modify sanctions on these entities significantly.

Arms embargo

Although narrower than the embargo imposed under the Iran Regulation, the Libya embargo also places a prohibition on the provision of related services (with certain exemptions for non-lethal military equipment intended solely for humanitarian purposes). A similar derogation is provided with regard to restrictions on equipment that might be used for internal repression.

United States

Pursuant to his IEEPA authority, President Obama imposed US economic sanctions in February 2011 after finding that continued violence in Libya posed an "unusual and extraordinary threat" to America's national security and foreign policy.

The US provisions include a blocking order freezing all the US property interests of Gaddafi and members of his family, the government of Libya and its agencies and controlled entities, and the Central Bank of Libya. The order in effect prohibits all transactions with these blocked entities, including any transfers of funds, goods and services. It applies to US persons, which includes US citizens and permanent residents, entities organised under the laws of the US (including foreign branches), or any person in the US.

In addition to the blocking order, the State Department suspended all existing licences and other approvals for the export of defence articles and services to Libya.

The abrupt imposition of sanctions by the EU, the US and other jurisdictions early in 2011, in response to Gaddafi's repressive activities, had a dramatic effect. In a very short time, Libya's energy and financial sectors ground to a virtual halt. With the August 2011 successes of the rebel movement, most of the sanctions have been lifted.

Sanctions against the Gaddafi family and individual members of the former regime remain, however, and Libyan accounts at US financial institutions continue to be blocked. Moreover, companies that violated the restrictions while in place may still be the subject of an enforcement action.

Sanctions against Syria

European Union

Council Regulation (EU) No 442/2011 of May 2011, as amended (the Syria Regulation), provides primarily for an asset freeze in relation to persons and entities deemed responsible for the violent repression of the civilian population in Syria, and an arms embargo, including restrictions on equipment that might be used for internal repression.

At the time of writing, however, and testament to the tumultuous nature of the sanctions regimes, the EU has substantially extended existing restrictive measures and imposed additional restrictive measures against Syria. These changes are explored in more detail below.

Asset freeze

Those subject to the asset freeze consisted of just 13 individuals up until July 23, 2011 when four entities were added. The President of Syria, Bashar al-Assad, was himself added to the list of sanctioned persons on May 23, 2011.

Most recently, on September 2, 2011, the EU adopted Council Regulation (EU) No 878/2011 (the New Syria Regulation).

This not only added four individuals and three entities to the ever-expanding list of designated persons and entities, but also extended the criteria for imposing asset freezes to stretch beyond natural or legal persons, entities and bodies identified by the European Council as being responsible for violent repression in Syria (and their associated persons), to further incorporate persons and entities benefiting from or supporting the Syrian regime.

Notably, the New Syria Regulation also expanded the circumstances pursuant to which competent authorities may authorise the release of frozen funds or economic resources, to include where such funds or resources are intended to be used for official purposes of the diplomatic or consular mission or international organisation, or where necessary for humanitarian purposes.

Arms embargo

This largely replicates the embargo set out under the Libya Regulation, including the available derogations.

United States

The US has maintained limited sanctions targeting Syria for a number of years. Most notably, in 2004, it imposed a virtual ban on the export and re-export of US-origin goods and technology to Syria. In 2011, the President has imposed additional measures, responding to the repressive violent actions of President Bashar al-Assad's regime. These include blocking orders freezing all US property interests of key Syrian government officials, including President al-Assad, as well as the Commercial Bank of Syria and the state-owned telecommunications firm, Syriatel.

The most significant new measure in 2011 has been an August Executive Order imposing a broad blocking order freezing the property interests of the government of Syria, its agencies, instrumentalities and controlled entities. The Order has also specifically designated several entities in the Syrian petroleum sector as coming within the scope of the Order, including the Syrian Petroleum Company, the Syrian Company for Oil Transport, and the Syrian Gas Company.

The Order has in effect prohibited all transactions with these blocked entities, including any transfers of funds, goods and services. The Order applies to US persons, which includes US citizens and permanent residents, entities organised under the laws of the US (including foreign branches), or any person in the US. As most commercial activity in Syria involves state-owned entities, the US blocking order has very broad effect.

In addition to the blocking order, the Executive Order prohibits all US investment in Syria, the export of services to Syria, and any dealing in Syrian-origin petroleum products. In this sense, it is broader than the sanctions imposed on Libya in February. No US person may engage in any transaction involving Syrian-origin petroleum products, even if such products remain outside the US.

Sanctions against Sudan

European Union

Amid the conflict in the Darfur region in Sudan, which began in 2003, Council Regulation (EC) No 131/2004 was passed in January 2004, imposing an arms embargo. Notably, there are no restrictions in relation to equipment that might be used for internal repression.

Nearly a year and a half later, an asset freeze was added by Council Regulation (EC) No 1184/2005 in relation to persons and entities impeding the peace process and breaking international law. The sanctions list is made up of four individuals only: Major Gaffar Mohamed Elhassan, a commander in the Sudanese air force; Sheikh Musa Hilal, a pro-government militia leader; Adam Yacub Shant, a rebel commander; and Gabril Abdul Kareem Badri, a rebel field commander.

United States

The Sudan sanctions regulations are unilateral measures that have been in place since 1998. They do not apply to the recently seceded Southern Sudan. The regulations prohibit virtually all trade and investment activities in Sudan by a US person, wherever located, with a 'US person' defined as including US citizens, permanent resident aliens, US companies (wherever they operate) and any person in the US. The principal provisions of the Sudan sanctions regulations are the following:

Blocked property

No property, or interests in property, held by the government of Sudan in the US may be transferred, paid, exported, withdrawn or otherwise dealt with. This blocking prohibition also extends to transactions with entities and individuals owned by or acting on behalf of the government of Sudan. These entities are included on OFAC's Prohibited Parties List.

Exports, re-exports, imports

No goods, technology (including technical data, software or other information) or services (including financial services, such as loans) may be exported or re-exported, directly or indirectly, to Sudan from the US or by a US person, wherever located, except for information materials or humanitarian donations of food, clothing and medicine. No goods or services of Sudanese origin may be imported into the US.

Facilitation

No US person may facilitate any act by a non-US person that would violate the Sudan Sanctions.

Sanctions against North Korea

European Union

Council Regulation (EC) No 329/2007 of March 2007, as amended (the North Korea Regulation), provides for:

- an asset freeze in relation to persons and entities supporting programmes related to nuclear and ballistic missiles, or other weapons of mass destruction
- an arms embargo, including restrictions on trade in dual-use goods and technology that could contribute to the above programmes
- an export ban on listed luxury goods. There is an element of uncertainty as to the applicability of this restriction as some of the terms used in the North Korea Regulation involve elements of subjectivity, such as 'high quality', 'high end' or 'pure bred'.

United States

While there is a long history of US economic sanctions against North Korea, currently the sanctions regime is basically limited to export restrictions. In 2007, consistent with UN Security Council Resolution 1718, the Export Administration Regulations (EAR) were amended to require a licence for the export or re-export of any item of US origin to North Korea, except certain food and medicines. In addition, there are various North Korean entities on the OFAC Prohibited Parties List.

Sanctions against Burma/Myanmar

European Union

Council Regulation No 194/2008 (as amended), originally introduced in 2008 and extended for a further one year in April 2011, imposes economic sanctions against Burma/Myanmar in response to the continued anti-democratic regime and violation of human rights. The sanctions primarily include:

- an asset freeze against certain individuals involved in or with the regime
- an arms embargo, including restrictions on trade in equipment that might be used for internal repression
- a ban on trade and investment in timber, coal, gems and precious metals.

However, the EU is supportive of the need to promote dialogue with the regime in Burma. In April 2011, it suspended certain travel and financial sanctions against members of the Burmese government and lifted the ban on high-level EU ministerial visits to Burma for one year in the hope of facilitating pro-democracy discussions.

United States

The US imposed sanctions against Burma in May 1997 and these have been expanded periodically. The Burmese Sanctions Regulations are more limited in scope than those involving Iran and Sudan. They apply to 'US persons', which includes US citizens and permanent resident aliens, US business entities and their US subsidiaries and foreign branches, and any person actually within the United States. The key features of the prohibitions include:

No new investment in Burma

The Burmese Sanctions Regulations do not prohibit a US company's foreign subsidiaries from making new investments in Burma; US persons may not be involved, however.

US persons are prohibited from facilitating, approving, aiding or supporting a foreign subsidiary's new investment in Burma.

Financial services

The sanctions prohibit export or re-export of most financial services to Burma by US persons. Financial services transactions include: the transfer of funds, directly or indirectly, to Burma; and the provision of banking, insurance, investment, or money-remittance services, as well as loans or guarantees.

Imports, exports

Imports of Burmese-origin goods into the US are banned. However, there is no general prohibition on the export of goods or services (except financial services) to Burma, unless such activities involve new investment. There are, however, significant restrictions on the export of dual-use goods.

Sanctioned persons

All property and interests in property of the Burmese government and certain of its officials are blocked. US persons may not transact business with these parties, who are on the OFAC list.

Sanctions against Cuba

United States

The US has maintained a comprehensive economic embargo of Cuba since 1963, pursuant to the Cuban Asset Control Regulations (CACRs), which prohibit almost all commercial transactions between the two countries or involving a US person and Cuba. The regulations prohibit all unlicensed transactions by persons subject to the jurisdiction of the US that involve property in which Cuba or Cuban nationals have at any time since the effective date of the prohibition had any interest whatsoever. Prohibited Cuban property interests are broadly defined to include goods, chattels, financial instruments, intellectual property rights, leaseholds "and any other property, real, personal or mixed, tangible or intangible, or interest or interests therein, present, future or contingent".

One notable aspect of these regulations is their potential application to certain non-US citizens or entities. Without specific authorisation, any

person subject to the jurisdiction of the US may not do business in Cuba or with Cuban state-owned enterprises, and such a person may not export products, technology or services to Cuba, even items from foreign locations that are not of US origin. 'Persons subject to the jurisdiction of the US' includes US residents, US corporations and their US or foreign subsidiaries, and any person actually within the United States.

European Union

In response to the CACRs' broad application to transactions by any persons subject to US jurisdiction, the EU imposed 'blocking legislation' in the form of a Council Regulation in 1996, forbidding compliance with the US sanctions against Cuba unless an EU entity received a waiver on the basis that failure to comply would seriously injure either the company or the EU's interests. This leaves EU subsidiaries of US-controlled companies in a potentially difficult situation, faced with the conflicting requirements of US and EU law. However, OFAC is generally willing to consider granting a licence to allow EU entities to carry out activities that would otherwise breach the provisions of the CACRs.

Targeted sanctions

European Union

In addition to the adoption of sanctions against specific states, the EU has the power to impose financial sanctions on specific persons, groups or entities identified as being responsible for offending policies or activities, an example being persons on the 'EU Terrorism List'. In recent years, there has been a trend towards more targeted measures, which are generally considered to be more effective than comprehensive sanctions and are intended to minimise adverse consequences for innocent third parties.

Targeted sanctions typically comprise an obligation to freeze all the funds and economic resources of specific persons or entities, and a prohibition on making funds available, directly or indirectly, for their benefit. However, exemptions are available, such as for funds necessary for basic living expenses. Targeted third-country nationals may also face a ban on travel to any country within the EU, with member states being required to take all necessary steps to enforce such prohibition, though once again exemptions may be available on humanitarian or other grounds.

As with comprehensive sanctions, the decision to place targeted restrictions on an individual or entity requires a 'common position' to be approved by the European Council. Clear criteria must be met and should be set out in the relevant CFSP legal instrument. If, following regular review, the European Council determines that the specific objectives of a sanction have been achieved, the individual or entity's name should be removed from the relevant list.

United States

In addition to the country programmes, US economic sanctions laws restrict or prohibit business by US persons with specific individuals and entities, wherever they may be located. These targeted or 'smart sanctions' have been the primary sanctions tool in recent years, as the US has sought to avoid measures that are unnecessarily broad and can have an adverse impact on innocent civilians.

Many of the targeted sanctions focus on government officials of regimes engaging in repressive activities. They currently include: (a) Cuban nationals; (b) 'specially designated nationals' of the Balkans, Belarus, Burma, Cuba, Cote D'Ivoire, Democratic Republic of the Congo, Iraq, Liberia, Somalia, Sudan, Syria and Zimbabwe (these can include certain state-owned entities, individual governmental representatives or agents of those countries); (c) 'specially designated narcotics traffickers' or significant foreign narcotics traffickers; (d) 'specially designated terrorists', 'specially designated global terrorists' or 'foreign terrorist organizations'; and (e) designated persons or entities involved in the proliferation of weapons of mass destruction.

These entities and individuals are included on OFAC's Prohibited Parties List. US persons may not engage in most transactions with blocked persons, and this order extends to any entity in which a listed person has a majority interest, even though such majority-owned entities may not themselves appear on OFAC's Prohibited Parties List.

Enforcement

European Union

EU member states retain autonomy in terms of penalties to be imposed for any breach of sanctions. Compared with the US, relatively few cases of enforcement have been brought by national authorities.

In recent years, however, there have been several investigations in the UK by the Serious Fraud Office (SFO) into alleged breaches of the UN sanctions against Iraq. In September 2009, engineering firm Mabey & Johnson was prosecuted in relation to admitted breaches of the sanctions following illegal payments to the Iraqi government in order to secure a contract under the UN oil-for-food programme. This was the first successful UK prosecution of a company for either overseas corruption or violation of the Iraq sanctions and resulted in a fine of £2 million. In February 2011, two former executives of the same firm were sentenced for providing kickbacks to the Iraqi government of Saddam Hussein in violation of the UN sanctions. One of the executives was sentenced to 21 months' imprisonment, disqualified from acting as a company director for two years and ordered to pay prosecution costs of £75,000.

Another high-profile case was the conviction and sentencing of Aftab Noor Al-Hassan, a British citizen, to 16 months' imprisonment in February 2011, once again for the illegal payment of funds to the government of Saddam Hussein in order to secure oil contracts.

It remains to be seen whether additional enforcement proceedings will follow in the near future, in particular in the event of breaches of the more recent EU sanctions against Syria.

United States

OFAC has maintained a consistent enforcement focus on all of the IEEPA programmes and the CACRs, although those efforts used to be predominantly civil. In recent years there has been more criminal enforcement by the Department of Justice (DOJ), and in addition, civil penalties have increased dramatically. The current maximum civil fine is US$250,000 per violation (up from US$50,000) and the maximum criminal fine for both organisations and persons is up to US$1 million.

Until recently the US government concentrated primarily on US companies, with limited enforcement actions targeting foreign companies, because the sanctions apply principally to US persons. But the focus has shifted in recent years as OFAC, the DOJ and bank regulators have pursued non-US financial institutions that allegedly used the US banking system to facilitate activities in sanctioned countries.

These 'transaction stripping' cases have resulted in very large criminal and civil fines against European banks, including the following large settlements:

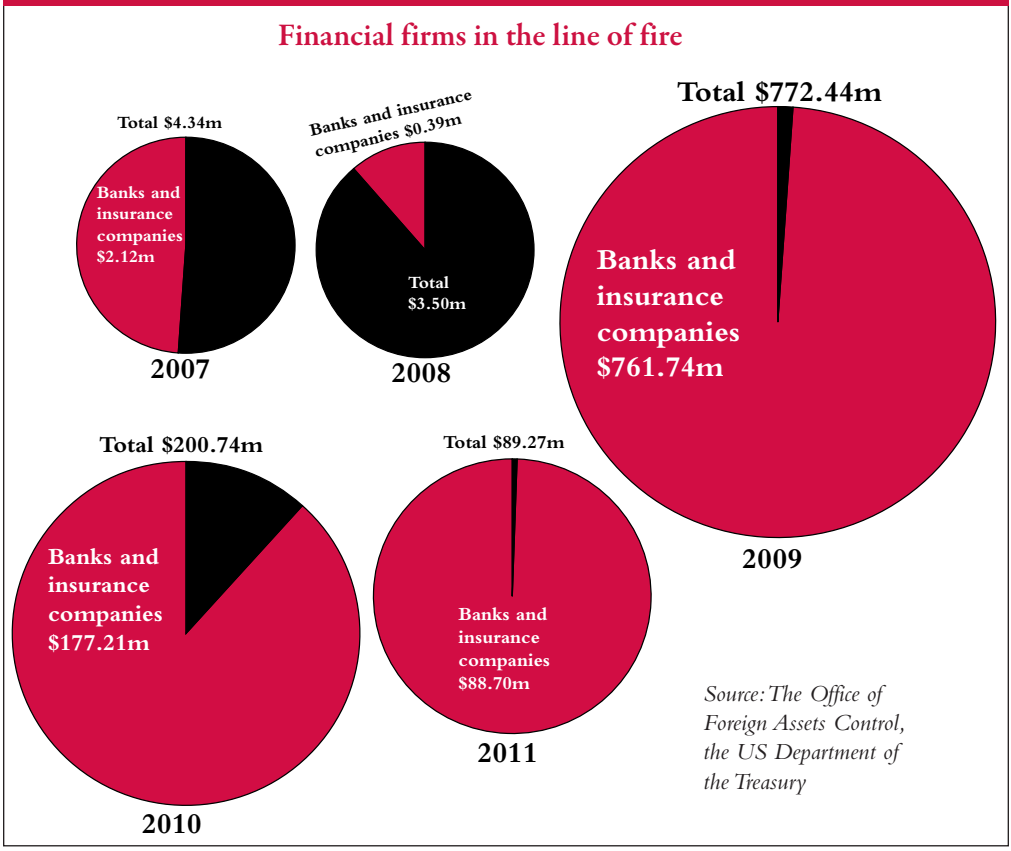
Barclays – August 2010

Deferred Prosecution Agreement (DPA) – agreed to forfeit a total of US$298 million. The UK bank allegedly stripped identifying information from sanctioned country customers by routing the payments to a US bank through an internal account and reformatting messages. It also apparently used cover payments, a less transparent method of payment messages, to hide information.

ABN Amro – May 2010

DPA – agreed to forfeit US$500 million. The Dutch bank allegedly stripped customer names, bank names and addresses, and other identifying information from wire transfers to US financial institutions over a period of ten years.

Civil penalties: 2007-2011



Credit Suisse – December 2009

DPA – agreed to forfeit US$536 million. The Swiss and UK branches allegedly stripped customer names, bank names and addresses, and other identifying information from wire transfers to US financial institutions. They also trained Iranian clients how to do the same. The scheme lasted over ten years and involved evidence of wilfulness (such as a pamphlet to Iranian clients, 'How to transfer USD payments').

Lloyds TSB – January 2009

DPA – agreed to forfeit US$350 million. The UK branches allegedly stripped customer names, bank names and addresses, and other identifying information from wire transfers to US financial institutions over a period of ten years.

The 'transaction stripping' cases and other cases (including an US$88 million fine paid by JP Morgan Chase in August 2011) show that financial institutions are at the highest risk of substantial fines. In looking at civil enforcement history since 2007 – with the notable exception of 2008 – fines targeting financial institutions were very large and comprised well over 90 per cent of the fines imposed. Multinational companies should be mindful, however, that the fine in a civil or criminal case is usually only part of the cost of an enforcement action. The costs of investigation typically are higher than the fine imposed.

Conclusion

Given the political developments in many parts of the world, the use of economic sanctions by the EU and US as an instrument of foreign policy looks unlikely to wane.

Compliance may involve more than merely avoiding transactions with sanctioned entities or regimes. Companies also need to be cautious that their dealings with counterparties in non-sanctioned countries do not inadvertently brush up against the prohibitions in the sanctions laws. Keeping up to date with the sanctions regimes – and carrying out due diligence into the corporate structure of otherwise legitimate entities to ensure that no funds are made available to sanctioned entities – has become a necessity.

Given the increasing enforcement in the US and EU, it is imperative that businesses are aware of the contours of the sanctions regimes and implement effective policies to minimise the risk of breaching applicable laws. Failure to do so can result in significant liability and reputational damage.

• *The authors would like to thank Claire Bentley, associate in O'Melveny's Singapore office, and Lauren Sweet, trainee in O'Melveny's London office, for their research and other assistance in writing this chapter.*

19

Corporate manslaughter and criminal liability arising from a fatal accident

Guy Bastable, Partner BCL Burton Copeland

Organisations operate in a highly regulated environment with an emphasis on corporate and director criminal liability which extends beyond that for economic crime such as fraud and corruption. With the very real risk of high fines and imprisonment, organisations and their directors are increasingly concerned about criminal liability arising from fatal accidents in the workplace, whether in relation to the death of an employee, a contractor or a member of the public.

Introduction

Over the past five years, there have, on average, been more than 500 workplace deaths each year. Against this background and well-documented public outrage, there has been a marked emphasis on criminal enforcement, particularly legislation and prosecutions focused on organisations and their directors.

In 2008, the Corporate Manslaughter and Corporate Homicide Act 2007 (CMCHA) was added to the range of offences available to the police and the Crown Prosecution Service (CPS) when investigating or prosecuting an organisation and its directors and employees following a fatal accident. Indeed, the law positively anticipates simultaneous or sequential prosecutions for corporate manslaughter and a breach of health and safety legislation arising out of the same set of facts.

An investigation following a fatal accident is now undertaken with a view to prosecuting:

- an organisation for corporate manslaughter
- an organisation for breaching the Health and Safety at Work etc Act 1974 (HSWA)
- an individual for common law gross-negligence manslaughter
- a senior officer for secondary liability in relation to a breach of the HSWA by the organisation
- an employee for breach of the HSWA for failing to take reasonable care of others.

Although the maximum sentence for gross-negligence manslaughter has always been life imprisonment, the situation has been compounded by the coming into force of the Health and Safety (Offences) Act 2008, which has meant most health and safety offences now carry the possible punishment of

a prison sentence rather than merely a fine, adding to the risks associated with the criminal liability of senior officers and employees.

Given that an investigation of a fatal accident often takes a number of years, the effect of these changes has only now begun to be realised. Indeed 2011 saw the first conviction, as well the launch of a second prosecution under the CMCHA. In those two prosecutions, the CPS proved itself willing to deploy the full arsenal of applicable criminal offences, including targeting senior management.

In *Cotswold Geotechnical*, the company was convicted of corporate manslaughter. In addition, it was charged with health and safety breaches. Further, the police charged a director with gross-negligence manslaughter and a secondary liability offence under the HSWA in relation to health and safety breaches by the company.

In *Lion Steel*, the company was charged with corporate manslaughter and health and safety offences. In addition, three of its directors were charged with gross-negligence manslaughter, as well as secondary-liability health and safety offences relating to the company's conduct.

If found criminally liable for a fatal accident, organisations face enormous fines, and directors and employees may be at risk of imprisonment.

The Corporate Manslaughter and Corporate Homicide Act

The CMCHA came into force in April 2008. It was enacted against the backdrop of a number of high-profile failed prosecutions of companies, particularly those relating to public disasters, and in order to remedy the perceived failings of the common law offence of gross-negligence manslaughter when applied to companies.

Previously it had been notoriously difficult to convict large companies of gross-negligence manslaughter (which, until the Act, was commonly referred to as 'corporate manslaughter'), although there had been a number of convictions of small companies. This had been attributed to the old law's reliance on the 'identification doctrine'.

The CMCHA removed the necessity under the old law to identify and establish the guilt of a 'directing mind' – a senior individual who could be said to embody the company in his actions and decisions. In a large or medium-sized organisation, such an individual is often far removed from the events surrounding the death, making establishing his guilt for gross-negligence manslaughter unlikely. Instead, the CMCHA concentrates on the way in which the organisation's activities were managed or organised, commonly referred to as a 'management failure', and whether that was a significant cause of the death (although it need not be the sole or principal cause of death). Importantly, the CMCHA has not created any new duties; rather, it criminalises gross breaches of duty by organisations that cause death.

The CMCHA specifically does not apply to individuals and also expressly states that an individual cannot be guilty of aiding, abetting, counselling or procuring corporate manslaughter. In addition, an individual cannot be guilty of the relatively new offence of encouraging or assisting crime in relation to an offence of corporate manslaughter.

However, although the CMCHA has abolished the common law offence of gross-negligence manslaughter so far as it applies to organisations, an individual can still be prosecuted and imprisoned on conviction for gross-negligence manslaughter, as well as a number of health and safety offences.

The offence

An organisation will commit the offence of corporate manslaughter where:

- it owed a relevant duty of care to the deceased
- the way in which its activities were managed or organised caused the deceased's death
- the way in which its activities were managed or organised amounted to a gross breach of that relevant duty of care; and
- the way in which its activities were managed

or organised by its senior management was a substantial element of that breach.

The relevant duty of care

The identified relevant duties of care are those owed as an employer; as an occupier of premises; or in connection with the supply of goods or services, the carrying on of construction or maintenance, the carrying on of any other activity on a commercial basis, or the use or keeping of any plant, vehicle or other thing. There is also a further category, known as the 'custody duty', relating to duties owed to a person in detention, which came into force in September 2011.

Gross breach

A breach of a relevant duty of care by an organisation is 'gross' where the conduct fell "far below what can reasonably be expected of the organisation in the circumstances". In particular, when assessing whether a breach by an organisation was gross, the jury *must* consider whether the "evidence shows that the organisation failed to comply with any health and safety legislation that relates to the alleged breach", and, if so, how serious the failure was and how much of a risk of death it posed.

The jury *may* consider the extent to which the evidence shows that there were attitudes, policies, systems or accepted practices within the organisation that were likely to have encouraged the breach or produced tolerance of it. The jury *may* also have regard to any health and safety guidance that relates to the alleged breach, as well as any other matters that they consider relevant.

Senior management

As mentioned above, an organisation will only be guilty if the way in which its activities were managed or organised by its senior management was a substantial element of the breach. 'Senior management' is defined as the persons who play significant roles in the making of decisions about how all or a substantial part of the organisation's activities are to be managed or organised, or in the actual managing or organising of those activities.

A number of critics have asserted that the CMCHA will be ineffective against large organisations, in particular due to the requirement for the involvement of senior management. However, it is important to note that, unlike the old law, the CMCHA allows for the aggregation of failings by a number of individuals. In reality, it is this principle of aggregation that sets the new law apart from the old.

The scope of the Act

The CMCHA applies to 'organisations', which includes: corporations (except for corporations sole) whether incorporated in the UK or abroad; identified government departments and bodies; police forces; and partnerships, trade unions and employers' associations that are employers.

The crucial element is that the harm that resulted in the death must have been sustained within the UK. Unusually, this is defined as including UK territorial waters and British-controlled ships, planes, hovercrafts, oil rigs and other offshore installations. It is inconsequential whether the death, the breach or the management failure occurred outside this defined territory, so long as the harm that resulted in the death occurred within it.

This highlights the far reach of the CMCHA. If, for example, an air crash occurred in the UK, the CMCHA would apply to the relevant airline operator (wherever incorporated), which is not surprising. However, if the air crash happened elsewhere, for example in the US, the CMCHA would still apply so long as the harm occurred on a British-controlled aircraft.

The sanctions

The main sanction on conviction for corporate manslaughter is an unlimited fine, which guidance and case law make clear could be millions of pounds. As mentioned above, individuals cannot be convicted of corporate manslaughter and no individual can be sentenced to imprisonment

under the Act, although directors and senior individuals can be sentenced to imprisonment if convicted of gross-negligence manslaughter or a number of health and safety offences, including those of secondary liability for breaches by the organisation (see below).

In addition, the sentence of an organisation can include a remedial order where the court specifies matters that must be remedied at the organisation's own expense. However, in practice, most if not all organisations will have already addressed the failures either voluntarily or pursuant to compliance with a Health and Safety Executive (HSE) improvement/prohibition notice.

Further, a court can also impose a publicity order – an entirely novel sentencing concept for England and Wales that requires an organisation to publicise its conviction along with the details of the offence, the fine imposed and any remedial order made.

Failure to comply with a remedial or publicity order is a separate indictable-only criminal offence carrying a further penalty of an unlimited fine.

The Health and Safety at Work etc Act

Irrespective of the applicability of corporate manslaughter, fatal accidents ordinarily involve a potential breach of the HSWA. Indeed, this Act places a number of general duties on employers and others, the breach of which constitutes a criminal offence.

So far as organisations are concerned, the most significant duties are those contained in Sections 2 and 3 of the HSWA.

In addition, Section 7 places a similar duty on employees and Section 37 creates secondary criminal liability for senior officers in relation to breaches by the organisation by virtue of their consent, connivance or neglect.

The offences

Broadly speaking, Section 2 of the HSWA sets out the duty on employer organisations to ensure, so far as reasonably practicable, the health, safety and welfare at work of employees. Similarly, Section 3 sets out the duty to ensure, so far as is reasonably practicable, that non-employees are not exposed to risks to their health or safety arising from the organisation's undertaking.

By virtue of Section 33, failing to discharge either of these duties constitutes a criminal offence of 'strict liability' (requiring no mental element such as intention, knowledge or negligence). In addition, following the decision of the House of Lords in *Chargot* (2008), a person's death is strong evidence that there was exposure to risk such that the burden of proof in effect shifts to the defence; the defendant organisation has to prove that it took all reasonably practicable steps to ensure the health and safety of the deceased.

Together, these three sections cover the criminal liability under the HSWA of an organisation in relation to the death of employees and others – although, strictly speaking, a death or injury need not occur, as the offences under the HSWA are directed at exposure to health and safety risk irrespective of whether any injury actually occurred.

In addition, Section 37 creates secondary liability for senior officers. If either of the above health and safety offences is committed by an organisation with the consent or connivance of a senior officer (or a person purporting to act as such), or is attributable to any neglect on his part, that person can also be prosecuted for the offence.

Consent and connivance only require knowledge of the relevant circumstances and, respectively, positive or tacit agreement to the organisation's conduct; there does not need to be any causal connection between the consent or connivance and the commission of the primary offence by the organisation.

Neglect is more complicated and requires the senior officer to have, as part of the scope of his office, a duty to inform himself of, and act in relation to, the relevant circumstances – and to have failed to do so. In addition, unlike consent or

connivance, there must be a causal connection between the neglect and the organisation's primary offence.

Finally, Section 7 places a duty on employees to take reasonable care for the health and safety of others who may be affected by their acts or omissions. Again, by virtue of Section 33, failure to do so is a criminal offence.

The sanctions

Previously, these health and safety offences could only be punished with a fine. However, following the Health and Safety (Offences) Act, most of these offences now carry the possibility of imprisonment, while the maximum fines in the lower courts have also increased significantly.

Where death occurs, organisations face an unlimited fine, usually in the hundreds of thousands of pounds and even in the millions for more serious incidents involving large companies. A court can also impose a remedial order on the organisation, but again these are rarely imposed (for the reasons set out above).

Senior officers convicted of Section 37 secondary liability and employees convicted of breaching Section 7 face a maximum prison sentence of two years and/or an unlimited fine. In addition, convicted directors can also be disqualified from acting as directors.

The investigation of a fatal accident

Corporate manslaughter, gross-negligence manslaughter and health and safety offences are all criminal offences that are prosecuted in the criminal courts.

Where an offence of corporate manslaughter or gross-negligence manslaughter is suspected, the police will lead the investigation into a fatal accident in line with the Work-Related Deaths protocol, working in partnership with the HSE or another similar relevant regulatory authority.

In addition, the CPS has issued guidance requiring police forces investigating fatalities to consider the possibility of a prosecution for corporate manslaughter, as well as looking at the actions of individuals for possible prosecution for gross-negligence manslaughter. The CPS has also made it clear that investigations will have a far greater focus than before on the senior management and whether their acts or omissions contributed to the fatality.

Police powers

The CMCHA does not create any new powers for the police when investigating corporate manslaughter, but the nature of the offence does present some problems for the police.

Ordinarily, the police can arrest and interview under caution a person whom they have reasonable grounds for suspecting of being guilty of a criminal offence. However, where an organisation is suspected of corporate manslaughter, it cannot be arrested or compelled to attend an interview under caution, nor can anyone on its behalf. The police can only invite the organisation to nominate a duly authorised representative to attend such an interview voluntarily and answer questions on its behalf.

Similarly, as there is no individual liability under the Act, a director cannot be arrested and interviewed under caution in relation to corporate manslaughter. Also, although the police could arrest and interview a director suspected of gross-negligence manslaughter, it is unlikely that any such interview would be admissible against the organisation in a prosecution for corporate manslaughter.

In addition, the police have the power to search premises following arrest, but again no one can be arrested on suspicion of corporate manslaughter. However, the police can apply to a magistrate for a search-and-seizure warrant, although an organisation's co-operation would make such an application unnecessary.

As such, the police generally rely on statements and documentation obtained from witnesses, via compulsory requests made by the HSE or another relevant regulatory authority (see below), or from the organisation voluntarily.

HSE powers

The HSE does not have any powers in relation to search and seizure or obtaining a warrant. Neither can it investigate corporate manslaughter. Its powers are limited to the investigations of health and safety breaches.

Nonetheless, under Section 20 of the HSWA, HSE inspectors have extensive powers to obtain evidence. Arguably the most potent are:

- Section 20(2)(j): the power to require a person to answer such questions as the inspector thinks fit to ask, and to sign a declaration of the truth of his answers
- Section 20(2)(k): the power to require the production of books or documents.

In addition, like the police, the HSE can obtain statements and documentation from witnesses and seek to interview under caution an organisation by inviting it to nominate a duly authorised representative.

Sentencing guidance

In 2010, the Sentencing Guidelines Council issued its definitive guidance for sentencing organisations for corporate manslaughter or health and safety offences that cause death. The guidance provides that inevitably there will be a broad range of fines reflecting the seriousness involved and the differences in circumstances of defendant organisations, but it goes on to specify that fines for organisations found guilty of corporate manslaughter may be millions of pounds and should seldom be below £500,000; for health and safety offences that cause death, fines from £100,000 up to hundreds of thousands of pounds should be imposed.

Significantly, the guidance further provides that while a court should have regard to a number of factors when assessing the financial consequences of a fine (including the effect of the fine on innocent employees and the provision of public services), in 'some bad cases' it may be acceptable that the fine will have the effect of putting the organisation out of business. Accordingly, in appropriate circumstances, a court has the power to fine an organisation out of existence.

Cotswold Geotechnical (Holdings) Ltd was the first organisation to be convicted under the CMCHA. The company was very small (with only four employees at the time of sentence) and it was in a dire financial position with limited assets. However, the sentencing judge fined it £385,000, which amounted to 115 per cent of its turnover for the year of the accident, to be payable over ten years. This was despite the fact that the judge considered that the fine and payment plan might well cause the company's liquidation; it was an "unfortunate but unavoidable" consequence of the serious breach.

This approach was approved by the Court of Appeal when refusing the company permission to appeal. The Lord Chief Justice stated that a fine that the company could pay would have resulted in a "ludicrous" penalty and confirmed that, in some cases, putting a company out of business may be inevitable.

Organisations convicted of corporate manslaughter can expect high fines. In cases of serious breach, large organisations can expect much higher fines and very large organisations can expect fines in the millions of pounds – even if they can't afford to pay.

Health and safety offences also attract significant fines. Indeed, even before the new guidance, the courts handed down enormous fines for such offences, particularly those that resulted in death. In 2005, Transco was fined £15 million following an explosion in which four people died. In 2006, following the Hatfield rail crash when four people died and 102 were injured, Balfour Beatty and Network Rail were fined £7.5 million and £3.5 million respectively. More recently, in May 2011, Network Rail was fined £3 million after pleading guilty following the Potters Bar rail crash in which seven people died.

In addition, accidents do not have to result in death or serious injury before huge fines are imposed. In June 2010, after the successful

prosecution of five organisations for the Buncefield explosion (the largest peacetime explosion in Europe), the companies were each ordered to pay fines and costs of up to £6.2 million, in the absence of any serious injury or death. *Buncefield* followed *New Look*, a case involving a fire where there were no deaths or injuries, in which the Court of Appeal upheld fines totalling £400,000, with Lord Justice Pitchford stating that the Court "does not have to wait until death or serious injury has occurred to express its displeasure at wholesale breaches".

Last, but by no means least, senior officers and employees face imprisonment of up to two years for health and safety offences. In addition, gross-negligence manslaughter has a maximum sentence of life imprisonment and a convicted defendant can expect the sentence to be measured in years rather than months.

Conclusion

Organisations that cause death, whether by corporate manslaughter or by breaching health and safety legislation, face enormous fines and possible collapse. In addition, fatal accidents present directors and employees with the very real risk of imprisonment. Finally, organisations, directors and employees risk criminal conviction, disqualification from acting as a director, severe reputation damage, and significant costs associated with remedial action and legal representation.

Where things go wrong, there is rightly great cause for concern for those organisations and individuals that may be caught up in an investigation following a fatal accident.

PART III

Investigation

20

Voluntary disclosure and the problems of plea bargaining

John P Rupp, Partner, Robert Amaee, Counsel, and Alexandra Melia, Associate
Covington & Burling LLP

Voluntary disclosure can provide enforcement authorities with an appealing alternative to prolonged and costly criminal investigations and prosecutions. The voluntary disclosure regimes that have developed in the US and, more recently, the UK involve the active encouragement of companies by enforcement authorities to report instances of actual or suspected corruption in return – at least purportedly – for the possibility of receiving a more lenient penalty than they otherwise would have received.

The US enforcement authorities responsible for dealing with instances of corruption have long been able to avail themselves of a variety of tools in seeking to resolve cases, including plea agreements and deferred prosecution agreements. In recent years, the UK Serious Fraud Office (SFO) has sought to emulate the US model through the use of civil settlements and plea negotiations, with varying degrees of success. The SFO's adoption of this model has led to some notable successes, including the prosecution of Mabey & Johnson in 2009, which represented the first prosecution of a UK company for foreign bribery since the UK ratified the OECD Anti-Bribery Convention in 1998.

More recently, however, the SFO's power to resolve corruption cases through the use of plea agreements came under judicial scrutiny in the Innospec case (discussed later in this chapter), which highlighted the difficulties the SFO faces in seeking to encourage self-reporting of actual or suspected corruption.

The challenge currently facing the SFO is how to use most effectively the limited tools – and decreasing resources – at its disposal to fight corruption.

Voluntary disclosure

The US model

The US Foreign Corrupt Practices Act (FCPA) does not require a company to report to enforcement authorities the bribes that it has paid to foreign government officials unless the company is listed on a US exchange and the matter at issue would be material to investors.

While once a comparatively rare phenomenon, the number of voluntary disclosures of actual or suspected FCPA violations to US enforcement authorities has increased sharply in recent years. That development has been fuelled by a number of factors, including a substantial increase in FCPA

enforcement actions coupled with higher penalties; an increased risk that FCPA violations will be discovered if they are not reported; and increased US Securities and Exchange Commission (SEC) reporting and certification requirements following enactment of the Sarbanes-Oxley Act in 2002.

The US enforcement authorities have actively encouraged voluntary disclosure by assuring companies that such action, accompanied by co-operation, can result in more lenient treatment – whether through a reduction in penalties or the pursuit of civil rather than criminal penalties – than if the authorities were to learn of the violations from other sources (such as enforcement authorities in other countries or a whistleblower).

The benefits of voluntary disclosure, however, are not statutorily guaranteed or quantified in advance by the authorities.

The approach adopted by the SFO

For the past few years, the SFO has worked to cultivate a home-grown version of the voluntary disclosure regime that has become an established part of anti-corruption enforcement in the US. It has sought to promote self-reporting by offering companies that detect bribery and fully engage with UK enforcement authorities the possibility of receiving a civil rather than a criminal penalty as well as the possibility of the SFO investigating the suspected wrongdoing in a discreet way that lessens the impact that otherwise might be felt by the company.

The appeal to a company of self-reporting and reaching a negotiated settlement with the SFO has been heightened as a result of the implementation in the UK of Article 45 of the EU Public Sector Procurement Directive 2004. This requires contracting authorities in all member states of the European Union to exclude from public contracts any companies that have been convicted of corruption offences. Significantly, these mandatory debarment provisions do not apply to the negotiated civil settlements that may be available to companies that voluntarily disclose.

In July 2009, the SFO issued guidance on voluntary disclosure in a document entitled 'Approach of the Serious Fraud Office to dealing with overseas corruption'.

The SFO guidance reiterated the benefits of voluntary disclosure. It also clarified the SFO's expectations with regard to co-operation by companies that self-report. According to the SFO guidance, once a self-report is made, the SFO seeks to establish how genuine the reporting company is in its commitment to an anti-bribery culture by assessing its readiness to:

- co-operate in carrying out any further investigation deemed necessary by the SFO and keep the SFO appraised of pertinent findings
- undertake remedial measures at the conclusion of any such investigation, such as restitution through civil recovery, retraining of employees, disciplinary action against individuals when deemed to be appropriate and/or external monitoring of the company's compliance efforts
- behave transparently and in a manner that is consistent with the public interest (for example, by issuing a joint public statement with the SFO discussing the outcome of the investigation)
- work with the SFO to reach a global settlement with other enforcement authorities that have jurisdiction over the company's behaviour.

Companies that are considering making a self-report should not underestimate the burdens that compliance with those expectations can impose. The costs of both additional investigative steps and any remediation measures that are deemed necessary will be borne by the company.

The financial burden of voluntary disclosure must, however, be weighed against the consequences of a failure to make a timely disclosure.

The uncertain benefits of voluntary disclosure

In deciding which of the range of options available to it should be used, the SFO is required to consider each case on its merits and dispassionately assess whether the criteria for prosecution have been met. It must give careful consideration to whether a particular case is suitable for criminal or civil treatment. While the SFO cannot guarantee a civil outcome when companies voluntarily disclose actual or suspected bribery, its declared aim is to pursue a civil outcome when companies satisfy the criteria discussed above.[1]

Any company considering whether to self-report actual or suspected bribery should consider the case of Mabey & Johnson, which is often held out by the SFO as a model of self-reporting. On August 7, 2009, the engineering group pleaded guilty at Southwark Crown Court to conspiring to corrupt officials in Ghana and Jamaica between 1993 and 2001 and breaching the United Nations sanctions against Iraq. The agents used by Mabey & Johnson were paid a commission to act as the company's representatives in foreign countries. Despite Mabey & Johnson having implemented policies on business ethics and the provision of hospitality, the evidence in the case demonstrated that bribes had been authorised at director level.

Mabey & Johnson elected to self-report to the SFO after allegations were made in civil proceedings against former employees and agents. The company also decided to waive privilege over the results of an internal investigation that it had conducted and to share that information with the SFO.

That approach was expressly commended by the SFO as demonstrating proper co-operation and Mabey & Johnson was given credit in court for adopting that approach. The waiver of privilege is now, in most cases, expected by the SFO as an indication that a company is fully co-operating.

On September 25, 2009, Mabey & Johnson was fined £750,000 for each of the two corruption offences and £2 million for breaching the Iraq sanctions. A confiscation order was also entered totalling £1.1 million in relation to the corruption offences and £618,484 with regard to the UN Iraq Development Fund. Mabey & Johnson was also required to pay reparations of £797,000 to Ghana and Jamaica.

The most notable aspect of the case was that the company's self-report did not result in a civil outcome. Any company considering making a voluntary disclosure will no doubt take note of that when deciding whether to self-report, particularly as the confiscation regime and mandatory debarment from competing for public contracts in the EU are triggered by conviction for a corruption offence.

There have been several examples of self-reports to the SFO that resulted in a civil outcome. For example, construction company Balfour Beatty self-reported following the discovery of irregular payments to a subsidiary in Egypt. Balfour Beatty ultimately paid a settlement of £2.25 million and contributed toward the SFO's costs.

Similarly, following a self-report by AMEC, the SFO decided to pursue civil recovery, having determined that the consultancy group had failed to keep accurate records – as it was required to do by Section 221 of the Companies Act 1985. Following AMEC's disclosure that it had received irregular payments in respect of a project in which it was a shareholder, a civil recovery order was made for almost £5 million.

Based on these cases, the SFO's decision to pursue a civil – as opposed to a criminal – resolution appears typically to be based on:

- the speed and openness with which a company makes a voluntary disclosure
- a company's willingness to co-operate fully
- a company's willingness to take steps to minimise the risk that irregularities will recur.

When the SFO decides on a civil resolution, it typically looks to settle the case by using a variety of measures, including:

- restitution by way of civil recovery, including the amount of the unlawful property, interest and the SFO's costs

- the imposition of an independent monitor proposed by the company and accepted by the SFO
- a programme of training and other steps designed to achieve a change of culture within the company
- discussion, when appropriate, about the role of key individuals
- a public statement agreed by the company and the SFO.[2]

Plea bargaining

An important element in the growth of the voluntary disclosure regime in the US has been the widespread use of plea negotiation and deferred prosecution agreements to settle corruption cases when companies have voluntarily disclosed instances of wrongdoing to the relevant authorities.

The workability of those agreements is, in turn, due in significant part to the willingness of the courts in the US to "give considerable deference" to the sentencing proposals put forward by the regulatory bodies responsible for policing corruption.[3]

In recent years, the SFO has enthusiastically supported the development and use of plea agreements as a tool for resolving corruption cases. The SFO guidance emphasises its willingness to engage in these negotiations in accordance with the Attorney General's 'Guidelines on plea discussions in cases of serious or complex fraud' and, in cases of voluntary disclosure, its willingness to avoid criminal proceedings altogether by agreeing a civil settlement.[4]

The SFO's foray into negotiated plea agreements has enjoyed some success:

Balfour Beatty

In October 2008, Balfour Beatty agreed to a civil settlement of £2.25 million for 'books and records' offences following the SFO's decision to use its civil recovery powers under Part 5 of the Proceeds of Crime Act 2002 in lieu of prosecution. Commenting on the settlement in a press release, the SFO stated: "The use of these new powers should be seen as an important example of how the SFO will use the new tools at its disposal to enhance the criminal justice process."

Mabey & Johnson

In July 2009 Mabey & Johnson pleaded guilty to ten counts of violating UN sanctions applicable to Iraq and was fined £6.6 million. Although the case largely preceded the Attorney General's guidelines, it was the first case in which the substance of the new procedures was followed.

AMEC

In October 2009, following an investigation into the receipt of irregular payments associated with a project in which AMEC, a consultancy group, was a shareholder, AMEC self-reported to the SFO its failure to keep accurate records, as required by the Companies Act 1985, and agreed to pay a civil recovery order of almost £5 million.

Julian Messent

In October 2010, Mr Messent, the former chief executive of insurance broker PWS Holdings, entered into a plea agreement with the SFO that was approved by Southwark Crown Court. Pursuant to that agreement, Mr Messent pleaded guilty to paying bribes totalling £1.2 million to Costa Rican officials between 1999 and 2002 and was jailed for 21 months.

The Innospec case

The legality of plea negotiations was questioned, however, in the Innospec case, which concerned the SFO's efforts to reach a global settlement of concurrent criminal proceedings in the US and the UK.

Innospec Ltd – a manufacturer of a lead-based fuel additive called tetraethyl lead – is a subsidiary of Innospec Inc, a US listed company. Both entities were implicated in a systemic scheme to breach United Nations sanctions in Iraq between 2000 and 2003 and to influence decision makers in Indonesia responsible for awarding public

contracts for the purchase of tetraethyl lead between 1999 and 2006.

Although Innospec reportedly wanted to settle the case, the fines and other penalties that may have been imposed in the US and UK could have exceeded by a significant amount what Innospec was able to pay. Taking into consideration the company's co-operation, the SFO and the US Department of Justice (DOJ) concluded that they should not seek to impose a penalty that would drive Innospec out of business.

In March 2010, Innospec entered into a global settlement with the SFO and various regulatory agencies in the US pursuant to which it was agreed the SFO would seek a penalty of no more than the sterling equivalent of US$12.7 million. In effect, the US$40 million that Innospec was able to pay in fines was divided among the SFO, DOJ and SEC. It was also decided that US$6.7 million of the SFO's share would be allocated to a fine or confiscation order to be imposed in the crown court, with the remainder being the subject of a civil settlement.

It was on that basis that Innospec pleaded guilty to conspiring with its directors and others to make corrupt payments to Indonesian government officials.

In his sentencing remarks, Lord Justice Thomas said he considered the fine of US$12.7 million to be "wholly inadequate" in relation to the degree of criminality displayed by Innospec.[5]

He went on to criticise the scope and content of the agreement reached by the SFO on the grounds that the suggested financial penalties had not been subject to judicial determination in either the UK or the US – save the determination inherent in the US Federal District Court's approval of the pertinent plea agreement – and that the proposed division of those penalties between the SFO, DOJ and SEC did not accord with the facts of the case.

Although he ultimately approved the proposed penalties, Lord Justice Thomas warned that the circumstances of the case were unique and were not to be interpreted as restricting the court's sentencing powers in future cases. He emphasised:

- the SFO did not have the power to enter into plea arrangements such as the one it had made with Innospec. Lord Justice Thomas stated that "no such arrangements should be made again"
- parties could put forward a joint submission on sentencing but should not include a specific sentence or sentence range, save for those set out in the pertinent sentencing guidelines
- only the court could make the final decision as to the appropriate sentence in a particular case.

Self-reporting: the pitfalls and the advantages

The Innospec case highlighted the difficulties faced by the SFO in seeking to encourage self-reporting of actual or suspected corruption, while at the same time retaining the confidence of the judiciary and the public that those found guilty of corrupt behaviour will receive appropriate penalties. While taking note of Lord Justice Thomas's comments, the SFO has continued to use plea negotiations as the basis for dealing with what it considers to be suitable corruption cases.

Companies that choose to self-report should be aware of the potential risk that any understanding reached with the SFO on penalties may ultimately be disregarded by the courts. There remain, however, good reasons – at least in some instances – for companies to continue self-reporting actual or suspected instances of corruption to the SFO.

Chief among those is the likelihood of crippling penalties being imposed on companies that fail to report wrongdoing voluntarily. Support for that approach was clearly apparent in Lord Justice Thomas's observation that corruption is "at the top end of serious corporate offending" and that fines for a recalcitrant corporate defendant are likely to be measured in the tens of millions.

That sentiment has been echoed by the SFO, which has stated that when information is received from a whistleblower or a suspicious activity report, rather than directly from a company itself, this will be regarded as a "negative factor".[6]

The development of other enforcement tools

The SFO has made it clear that it would like to be given the power to enter into deferred prosecution agreements – a tool already utilised by the DOJ in its resolution of corruption cases. Deferred prosecution agreements, as they currently operate in the US, differ from plea agreements because companies that comply with their terms can avoid formal charges in relation to the underlying corrupt conduct.

In that respect, companies entering into deferred prosecution agreements are in effect placed on probation for a period, during which time they are expected to co-operate with the DOJ and engage in remediation activities that, typically, are outlined in the terms of the agreement itself. Provision is also often made in deferred prosecution agreements for the payment of a significant fine by the offending company. The difficulty for the SFO is that it does not currently have the statutory power to impose fines or to enter into such an arrangement.

21

Do the principles of corporate prosecution in the US provide a roadmap for the UK?

Matthew Reinhard, Member (Washington DC) Miller & Chevalier, Chartered

Compared to the United States, the criminal prosecution of corporate entities in the United Kingdom is a new phenomenon, but one that is likely to increase in scope and frequency with the implementation of the Bribery Act 2010. While both the Serious Fraud Office (SFO) and Ministry of Justice (MoJ) issued initial compliance guidance for the Bribery Act, publicly available criteria guiding charging decisions for UK corporates remain lacking.

Recognising the similarities between US and UK anti-corruption laws and common-law systems, it is reasonable to consider established US policies and procedures guiding the prosecution of corporate entities – and how these procedures have been applied in cases under the Foreign Corrupt Practices Act (FCPA) – as providing a potential roadmap for the way in which such prosecutions may develop in the UK.

This chapter will examine the 'Principles of the Federal Prosecution of Business Organizations' (the Principles) included in the United States Attorneys' Manual (USAM), and discuss the evolution of the Principles relating to corporate co-operation and charging decisions. It will also highlight the tensions that remain in the Principles and between prosecuting authorities and the defence bar, explore recent charging decisions illustrative of these Principles, and consider the extent to which the US experience offers practical guidance in the UK.

The US Principles for prosecution of corporates

The jurisprudence allowing the criminal prosecution of corporate actors has existed for over a century. In 1909 the US Supreme Court permitted an employee's criminal intent to be imputed to his employer, laying the groundwork for the concept that a corporation could possess the necessary intent to engage in criminal acts separate from individual employees. However, the modern era of criminal corporate prosecutions in the US began in earnest at the beginning of the 21st century, notably with the prosecution of Arthur Andersen in 2002, and a dramatic increase in FCPA cases starting around the same time.

Modern guidance for all federal criminal charging decisions is set out in the USAM, issued by the Department of Justice (DOJ) to its prosecutors. The USAM makes it clear that prosecuting corporate crime is a high priority and that corporations are not to be "treated leniently because of their

artificial nature". The Principles in the USAM have evolved over the past decade, but in their current form they set out nine specific factors that federal prosecutors must consider when deciding whether and how to charge corporate actors with criminal acts:

- the seriousness of the offence
- the pervasiveness of the wrongdoing within the corporate
- whether there is a history of similar misconduct
- the corporate's disclosure of wrongdoing and its willingness to co-operate
- the 'existence and effectiveness' of a compliance programme
- remedial actions taken by the corporate in response to the activity
- the collateral consequences of a prosecution on shareholders, pension holders, employees, the public, and other individuals not personally culpable
- the adequacy of the prosecution of the individuals responsible for the actions
- the adequacy of civil or regulatory remedies.

Of these nine factors, perhaps none has generated more commentary or consternation among the defence bar than the one providing that a corporate's "disclosure of wrongdoing and its co-operation with the government's investigation may be relevant factors" in deciding whether to charge and "how to resolve" a criminal case.

In gauging the extent of co-operation, a prosecutor may take into account whether a disclosure was "voluntary and timely", as well as the corporate's "willingness to provide relevant information and identify relevant actors within and outside the corporation, including senior executives". The DOJ takes care to point out that failure to co-operate "in and of itself, does not support or require the filing of charges with respect to a corporation". By the same token, co-operation "does not automatically entitle [a corporate] to immunity or a favorable resolution of its case".

Self-disclosure and co-operation – evolution

The first question a corporate must face when encountering potential criminal activity is whether and when to disclose. That is not a straightforward consideration. While both the US and UK authorities maintain that self-disclosure and co-operation may influence the decision on whether to charge in the first instance, the costs of making the disclosure, responding to subsequent inquiries and 'co-operating' (as that term is understood by the government) may be significant.

Generally, an internal investigation to gather enough information to make an educated assessment as to whether a potential issue should be self-disclosed is appropriate. Ultimately, however, the decision to disclose is one that must be carefully weighed with the advice of a solicitor – and, presumably, if that decision is taken, the final analysis will be that the costs of disclosing (including money, reputation and opportunity) are less than those faced were the issue not to be disclosed but subsequently discovered and prosecuted.

Assuming the decision to self-disclose is made, how does a corporate go about demonstrating 'co-operation'? In this regard, there has been an evolution of policy in the US over the past decade, and what constitutes full co-operation remains an issue of some dispute between prosecutors and the defence bar.

Early guidance: the Holder, Thompson and McNulty Memos

Early guidance was offered to DOJ prosecutors by then Deputy Attorney General (and current Attorney General) Eric Holder in a 1999 memorandum: 'Bringing Criminal Charges Against Corporations'. The Holder Memo explicitly stated that one factor that may be weighed in evaluating the adequacy of corporate co-operation is the "completeness of its disclosure,

including, if necessary a waiver of the attorney-client and work product protections, both with respect to its internal investigation and with respect to communications between specific officers, directors, and employees and counsel". Beyond complaints from the corporate defence bar, this policy eventually caught the attention of Congress, which held a variety of hearings and offered draft Bills (never passed) intended to maintain the integrity of the attorney-client privilege.

The Holder Memo further stated that "another factor" to be weighed was whether a corporate "appears to be protecting its culpable employees and agents". This protection could include the advancing of attorneys' fees, maintaining the employment of 'culpable employees' without sanction for misconduct, and entering into a joint defence agreement (JDA) with employees deemed 'culpable'.

Under US jurisprudence, JDAs (whether oral or written) formalise the recognised joint defence privilege and permit defendants with a 'joint defence' or 'common interest' to communicate with one another and their attorney (if the same attorney is representing multiple defendants), or allow the defendants' own attorneys to communicate with one another – sharing information and documents – without being deemed to waive the attorney-client privilege.

The DOJ policy discouraging such agreements and indemnification of employees' legal fees, and encouraging employment sanctions, served only to create further tension between prosecutors and the defence bar, many of whom represented corporations that were bound by local corporate and employment laws, or by contract, to advance legal fees to employees or withhold terminations or discipline until certain procedural steps were complete.

Thus, corporations found themselves on the horns of a dilemma – either violate local laws and contracts or be deemed 'unco-operative' by federal prosecution authorities.

The next major policy statement by the DOJ on corporate cooperation – a 2003 memorandum from then Deputy Attorney General Larry Thompson – reiterated these positions in the Holder Memo verbatim.

In 2006 a federal court in New York, presiding over a criminal action against former partners of the KPMG accounting firm, ruled that the Thompson Memo guidelines regarding indemnification of employees were unconstitutional and that KMPG had elected not to pay the attorneys' fees of the individuals being prosecuted (in an effort to avoid a prosecution of KMPG itself) because "the government held the proverbial gun to its head" (*United States v Stein*, 2006).

In December 2006 – in response to *Stein* as well as an outcry from corporations and their solicitors, and the renewed possibility of Congressional interference in DOJ policy making – then Deputy Attorney General Paul McNulty issued his own memorandum regarding the charging of corporate entities, supplanting the Thompson Memo.

On the subject of waiver, the McNulty Memo attempted to split the difference, stating that waiver of the attorney-client privilege was "not a prerequisite to a finding that a company has co-operated", but reiterating that prosecutors could request a waiver of the privilege when there was "a legitimate need for the privileged information to fulfill their law enforcement obligations".

Reading *Stein* as narrowly as possible, the McNulty Memo clarified that prosecutors should "generally not take into account whether a corporation is advancing attorneys' fees to employees or agents", and acknowledged that local corporate laws and individual contractual obligations may require the payment of such fees. Nonetheless, the McNulty Memo reiterated the Holder and Thompson views that entering into JDAs with employees and failing to take employment or disciplinary actions could have an impact on the assessment of co-operation.

The Filip revisions to the USAM and current tensions

The defence and corporate bar generally panned the McNulty Memo as offering little substantive

change from the principles laid out by its predecessors. In August 2008, with the DOJ again facing scrutiny from Congress regarding these policies, then Deputy Attorney General Mark Filip announced a new set of principles. These changes were made directly to the USAM and remain in effect today.

With respect to the attorney-client privilege, the USAM changes addressed the criticism that greeted the Holder, Thompson, and McNulty Memos. Now, the USAM emphasises disclosure of 'facts' to the government as evidence of co-operation. The revised Principles state that waiver of the attorney-client or work product protections has "never been a prerequisite" for a corporate to be viewed as co-operative, but acknowledges that "members of the American legal community and criminal justice system" asserted that prior policies on corporate co-operation were used to coerce corporations into waiving privileges and protections.

While the current Principles make it clear that a corporation may still choose to waive privileges, the DOJ may no longer request a waiver. Moreover, the USAM provides that where defence attorneys believe prosecutors are violating the principles regarding waiver, they should raise their concerns with the prosecutor's supervisor.

The current USAM also makes it clear that prosecutors "should not take into account whether a corporation is advancing or reimbursing attorneys' fees or providing [solicitors] to employees, officers or directors under investigation or indictment" when evaluating co-operation. Similarly, participation in a JDA "does not render the corporation ineligible to receive co-operation credit", although the DOJ still warns that a company "may wish to avoid putting itself in the position of being disabled, by virtue of a particular joint defence or similar agreement, from providing some relevant facts to the government and thereby limiting its ability to seek such co-operation credit".

While, to many, the revised USAM represents an improvement over earlier policies, the emphasis on disclosure only of 'facts' (not privileged communications) ignores an inherent tension in how corporates become aware of such facts. In many cases, 'facts' relevant to a criminal prosecution known by a corporate are discovered as the result of some form of internal investigation led by solicitors. The application of a lawyer's mental impressions and judgement to the investigative process that reveals those facts – deciding what documents to review, which employees to interview (and the actual interviews), what questions to ask etc – necessarily involves communications between attorney and client and creation of work product such that the 'facts' uncovered could themselves properly be considered privileged and protected.

Under US jurisprudence, the courts – not the DOJ or private litigants – are the ultimate arbiters of whether privileges have been waived. Thus, facts disclosed to the DOJ in the course of co-operating (without the intention of waiving any privileges) could subsequently cause such co-operation to be deemed an unintentional waiver of the attorney-client privilege and result in a broad set of materials being subject to civil discovery requests (for example, in shareholder derivative litigation) or to subpoena (for example, in criminal prosecutions of individuals). As yet, this tension has not been resolved or squarely faced by the courts. Meanwhile, the prospect of an unintentional waiver of privileges by corporates as they co-operate with the DOJ continues to concern the defence bar, who often encourage caution by corporates.

The current state of co-operation – the *Panalpina* dispositions

In the summer of 2007, in response to several disclosures by various companies, the DOJ instituted a large-scale anti-corruption investigation of the global freight forwarder and customs broker Panalpina. This investigation expanded to include many of Panalpina's largest customers in the oil and gas industry. Though a number of inquiries remain ongoing, in late 2010

the first tranche of *Panalpina*-related resolutions was released. These cases, revolving around the same actor, industry and, in many cases, behaviour, provide an insight into the effects of co-operation on prosecutorial decisions.

Most notably, while each case involved a variety of charges under the FCPA, all the resolved cases involved corporate actors that were deemed by the DOJ to have co-operated with the investigation (though Panalpina itself did not co-operate initially, only to reverse course), and nearly all of the corporate parties obtained deferred prosecution agreements (DPAs) or non-prosecution agreements (NPAs). Simultaneously with the DOJ resolutions, the US Securities and Exchange Commission (SEC) also entered into civil settlements with the same corporate actors, which included substantial civil penalties, disgorgement of profits and injunctive relief.

Declinations, DPAs and NPAs

The ultimate goal of any corporation in disclosing wrongdoing and co-operating with prosecutors is to obtain a total declination of prosecution. However, such declinations are rarely publicised and it is difficult to create a comprehensive catalogue of factors that increase a corporate's chances of receiving a declination after self-disclosure and co-operation.

While they do not represent a complete declination of prosecution, and often involve significant financial penalties, DPAs and NPAs have become an increasingly common vehicle to resolve criminal actions – ones that allow corporates to avoid the stain of criminal convictions while still providing the DOJ with an opportunity to collect penalties, extract admissions of wrongdoing and, in the case of DPAs, file formal criminal charges.

The more formal of the two, a DPA is a written agreement between the DOJ and the corporate, generally filed in court concurrently with criminal charging papers. While the terms of DPAs vary from case to case, they almost always include the corporate/defendant acknowledging that criminal information will be filed in federal court, formally admitting to a set of written facts (often negotiated, but sufficient to support the burden of proof for all charges contained in the information), agreeing to financial penalties, agreeing to undertake compliance-programme enhancements, and waiving certain legal protections (such as the statute of limitations).

In exchange, the DOJ agrees that it will defer prosecution of the criminal information for a set period and, if the corporate complies with the agreement for the term of the DPA (typically two to three years), dismiss the criminal indictment without prosecution and with prejudice.

DPAs are sufficiently established within the criminal justice system that, while they involve formal filings in court, the substance or terms of individual agreements are rarely questioned or challenged by the presiding judge.

By contrast, an NPA is not filed with any court, nor are formal criminal charges filed. Rather, NPAs generally take the form of a written letter of agreement between the DOJ and the corporate where the DOJ agrees not to bring criminal charges in exchange for a set of promises by the corporate. While the contours of individual NPAs may differ, many of the corporate obligations are similar to a DPA, including admitting to a certain set of facts, agreeing to make compliance-programme enhancements and paying a monetary penalty directly to the US Treasury. Although resolving a criminal investigation, NPAs lack any form of judicial oversight or approval and in many regards are more akin to a civil settlement.

The initial *Panalpina* resolutions

The tables on pages 173 and 174 summarise the resolutions of criminal actions by the DOJ against Panalpina and several of its customers, released in late 2010.

While all the results were undoubtedly the product of intensive negotiation between attorneys for the corporation and the DOJ, a few themes can be teased from them.

Criminal actions and the Department of Justice: the Panalpina resolutions

Company	Entity	Resolution	Monetary penalties	Other penalties	Noteworthy aspects
Panalpina World Transport Ltd (Switzerland)	Panalpina World Transport Ltd	DPA	$70.56m criminal penalty	• Enhanced corporate compliance programme and remedial measures • Undertake follow-up reviews and draft detailed initial report and three annual reports to the DOJ • Mandatory disclosure of additional issues during DPA	• DPA details co-operation • Monetary fine was at the bottom end of the sentencing guidelines evaluation • Voluntarily self-appointed compliance consultant for 3 yrs to assist with DPA
	Panalpina Inc (US subsidiary)	Guilty plea		• 3-yr term of organisational probation	
Royal Dutch Shell plc (Netherlands)	SNEPCO (Nigerian subsidiary)	DPA	$30m criminal penalty	• Enhanced corporate compliance programme and remedial measures • Mandatory disclosure of additional issues during DPA • Detailed initial report and 2 follow-up reports to DOJ	• DOJ notes co-operation of SNEPCO and Royal Dutch Shell with investigation and remedial measures, including implementation of enhanced compliance programme
Transocean Ltd (Switzerland)	Transocean Inc (Cayman subsidiary)	DPA	$13.44m criminal penalty	• Enhanced corporate compliance programme and remedial measures • Mandatory disclosure of additional issues during DPA • Detailed initial report and 2 follow-up reports to DOJ	• Monetary fine is $3.4m below the sentencing guidelines fine range
Tidewater Inc (New Orleans)	Tidewater Marine Int'l Inc (Panama subsidiary at time of conduct)	DPA	$7.35m criminal penalty	• Enhanced corporate compliance programme and remedial measures • Mandatory disclosure of additional issues during DPA • Detailed initial report and 2 follow-up reports to DOJ	• Monetary fine is $3.15m below the sentencing guidelines fine range

Declination is possible

While the tables illustrate the terms of settling corporates, public filings confirm that at least two companies that made voluntary disclosures to the DOJ and SEC regarding Panalpina received declinations from either or both agencies.

Because of the non-public nature of such negotiations, it is difficult to pinpoint the precise reasons for the declinations; but it is clear that, in some instances, co-operating corporates may avoid prosecution entirely, particularly when self-disclosing.

Co-operation alone may not be as beneficial as voluntary disclosure and co-operation

While self-disclosure is not a guarantee of declination, the tables show that it does appear to offer tangible benefits to companies that have not received declinations. While the DPAs for Transocean and Tidewater both commented on

Criminal actions and the Department of Justice: the Panalpina resolutions

Company	Entity	Resolution	Monetary penalties	Other penalties	Noteworthy aspects
Pride Int'l Inc (Houston)	Pride Int'l Inc	DPA (3 yrs, 7 days; may be extended by up to 1 yr for knowing violations; may also be ended early)	$32.62m criminal penalty (paid by Pride Forasol or Pride Int'l on Pride Forasol's behalf	• Enhanced corporate compliance programme and remedial measures • Mandatory disclosure of additional issues during DPA • Detailed initial report and 2 follow-up reports to DOJ	• DPA explicitly notes Pride's co-operation and assistance in providing information regarding Panalpina • Fine is approximately $40m below the sentencing guidelines fine range minimum based on early voluntary disclosure; extensive co-operation; substantial assistance with other DOJ investigations; and extensive remedial efforts
	Pride Forasol SAS (French subsidiary)	Guilty plea	$32.62m criminal penalty, plus mandatory assessment of $400 per count to district court	• 3-yr term of organisational probation • Conditions of probation include: (a) Pride Int'l's maintenance of corporate compliance programme; (b) annual report to DOJ by Pride Int'l on behalf of itself and Pride Forasol	• Fine is approximately $40m below the sentencing guidelines fine range
Noble Corp (formerly Caymans, now Switzerland)	Noble Corp	DPA	$2.59m criminal penalty	• Enhanced corporate compliance programme and remedial measures • Undertake follow-up reviews and draft initial report and 2 annual reports to DOJ • Mandatory disclosure of additional issues	• DOJ release says NPA recognises Noble's "early voluntary disclosure, thorough self-investigation ... full co-operation ... and extensive remedial measures"

each company's co-operation with the DOJ, the Tidewater DPA explicitly noted that Tidewater voluntarily disclosed issues to the DOJ. Transocean's DPA, by contrast, noted that the company investigated potential issues "after becoming aware of information indicating potential issues with its Freight Forwarding Agent" (possibly as a result of a DOJ inquiry), co-operated with the DOJ's inquiries and shared the findings of its internal investigation; it did not indicate that the company voluntarily disclosed information to the DOJ in the first instance.

In the US, criminal laws provide a statutory range of punishment but sentencing is also guided by the United States Sentencing Guidelines. From their inception until 2005, the guidelines provided a complex, and mandatory, sentencing formula that resulted in a 'guidelines range' of penalties, within which the presiding judge was (except in rare circumstances) required to sentence.

In 2005, the Supreme Court ruled that the mandatory nature of the guidelines was unconstitutional and that they should only be 'advisory' in sentencing decisions. The DOJ still uses the 'advisory' guidelines to calculate an initial range of penalties for the criminal charges being resolved by the DPA, but may assess penalties below the guidelines range as a reward for co-operation and self-disclosure.

Notably, in *Panalpina*, both the Tidewater and Transocean DPAs included penalties approximately US$3 million below the guidelines range for the offences. However, the criminal information accompanying the DPAs charged Transocean with a substantive violation of the FCPA's anti-bribery provisions, a charge not included against Tidewater. This extra count greatly inflated the range of potential penalties against Transocean, such that it ultimately paid a penalty of over US$13 million (to Tidewater's US$7 million), even though the DPA calculated that the benefit Transocean received from its corrupt activities was over US$4 million less than the commercial benefit received through Tidewater's actions.

Indeed, over all the *Panalpina* settlements to date, and including the SEC penalties and the declinations of prosecution, the average amount paid by corporates that made voluntary disclosures and co-operated was just under US$16 million, whereas corporates that did not voluntarily disclose (but still co-operated) paid an average settlement of over US$50 million.

Voluntary disclosure matters, but severity of conduct matters too

The resolution of the charges against Pride and Noble illustrates that voluntary disclosure and co-operation in themselves are no guarantee against prosecution or hefty penalties. Both Pride and Noble voluntarily disclosed FCPA violations to the DOJ and co-operated in subsequent investigations. Pride International received a DPA but its French subsidiary (Pride Forasol) was charged and pleaded guilty to three FCPA-related counts. Meanwhile, Noble received an NPA.

While both companies voluntary disclosed, the scale of the issues at Pride (at least US$800,000 in improper payments to secure US$13 million in benefits), as compared to Noble (at least US$75,000 in improper payments to secure US$2.9 million in benefits), clearly influenced the DOJ's decision to subject Pride to a harsher financial penalty (though one that was still a 55 per cent departure from the normally recommend range of penalties) and a criminal charge.

Where does the UK go from here?

While UK principles of self-disclosure and co-operation will undoubtedly evolve with their own unique elements grounded in UK criminal law, one can be optimistic that the UK authorities can learn from the evolution of corporate prosecution in the US over the past decade and avoid the controversies over corporate co-operation, the attorney-client privilege and indemnification of employees which have caused such consternation.

While some tensions still exist in the US regarding the contours and benefits of self-disclosure and co-operation, the current USAM offers a clearer path to navigate. In the UK, a set of clear, published principles of corporate prosecution, including what will be expected of corporates that self-disclose and co-operate with investigations (as well as the potential rewards for such co-operation), would greatly assist in assuring corporates of a level playing field and clarifying the potential benefits and risks of any disclosure decision.

Perhaps more important is whether the UK legal system can overcome current judicial resistance and develop mechanisms for the resolution of corporate criminal activity similar to DPAs and NPAs, as these will allow prosecutors to collect their 'pound of flesh' while providing corporate actors with palatable alternatives to gambling on the binary options of non-prosecution or a criminal charge.

Unlike the broad acceptance of DPAs in US courts, the few attempts made by the SFO to file

and enforce negotiated resolutions of criminal charges against corporates for corruption-related issues have been met with strong resistance by the UK judiciary.

At the beginning of this book, SFO Director Richard Alderman calls for the creation of similar DPA powers for the SFO. Surely the development of such an option, along with clear, published guidance on corporate charging considerations, will permit corporate actors in the UK to make more fully informed decisions on whether to disclose issues to the SFO and co-operate in any investigation.

22

Preparing for a 'dawn raid' – and dealing with the aftermath

Peter Crowther, Partner Dewey & LeBoeuf LLP

They happen without warning and are timed for maximum surprise. Launched by national and international authorities from the Serious Fraud Office (SFO) to the European Commission (EC), 'dawn raids' of corporate premises form the first front of investigations into suspected unlawful activities by companies and individuals. Searches for information are carried out and the aim is that, caught off guard, the target will not have the chance to hide or destroy evidence.

But while, by their nature, the raids cannot be foreseen, companies can still prepare for them by putting procedures in place, knowing their rights and understanding how to deal with the impact, both in the short and longer term, of a dawn raid.

Responding to a dawn raid

Prior to a raid

Apart from the SFO (for suspected fraud offences) and the EC (cartels and other anti-competitive behaviour), bodies empowered to carry out a dawn raid in the UK include the Office of Fair Trading, HM Revenue & Customs (tax offences), and the Financial Services Authority (insider dealing). The investigative powers of these bodies vary and, in some cases, will depend on the nature of the authorisation (or mandate) under which the raid is conducted.

However, investigators generally have the power to enter and search the premises of the target company (although not necessarily to do so forcibly) and request copies of documents discovered during the search.

Despite the term, dawn raids more usually take place during office hours, typically at the start of the working day. But in certain cases – notably investigations of criminal cartel activity – searches may take place earlier and be dawn raids in the literal sense. In the event of suspected criminal activity, the homes of employees may also be subject to the raids.

Clearly, the best preparation for a dawn raid is to ensure that compliance procedures are sufficiently robust to avoid regulatory breaches in the first instance. However, even if a company has no reason to suspect it might be guilty of any wrongdoing, it is still essential to prepare a dawn raid protocol on the assumption that a raid could take place at any time and without warning. These steps will include:

- circulating guidelines to employees that outline the powers available to the various authorities, provide information on the way in which raids are carried out, and set out a checklist of procedures that should be followed in the event of a raid
- briefing staff directly involved in dealing with a dawn raid – for example, receptionists, security staff and senior executives – on their individual responsibilities. Depending on the size and nature of the company, it may be worth extending this training programme to other employees, such as the IT department and in-house lawyers.

When the investigators arrive

Checking their mandate

On arrival, the investigators should produce their credentials and the authorisation for the raid. In the event of an SFO or Financial Services Authority (FSA) raid, this will be a warrant. The mandate should be checked to ensure that the investigators have the authority to carry out the raid. In particular, it is important to check that:

- the mandate applies to the company that is subject to the raid
- it is of a type to which the company is bound to submit
- the investigators are individually named in the mandate (or in an accompanying document)
- each investigator has valid identification
- the mandate was issued for a period that is still valid.

In competition investigations, the subject matter and period of the alleged infringement should be confirmed with the investigators and a note made of this. In inquiries by the FSA or SFO, the precise scope of the information required will be specified in the warrant.

Seeking a delay, but avoiding obstruction

It is advisable to request that the investigators delay their searches until in-house or external lawyers are present. In the event of a criminal raid, such a request is less likely to be granted; the Office of Fair Trading (OFT) and EC tend to be more willing to wait for a reasonable period, but this is unlikely to be more than an hour. As outlined above, it is important in this regard that front-line staff are adequately briefed to deal with the investigators if necessary.

It is, however, also important to note that an attempt to delay a search significantly may be construed by regulatory authorities as obstruction. That in itself may give rise to a fine, and it is a criminal offence to fail to comply with a lawful request made by the SFO during an investigation. In addition, there may be negative consequences in terms of any subsequent application for leniency in relation to a competition inquiry.

All staff, therefore, should be instructed to co-operate with investigators to the extent that the latter do not exceed the limits of their legal powers.

Monitoring the dawn raid

Shadowing

In general, investigators have the right to take copies of documents during their search. Certain regulatory authorities also have the right to take possession of original documents. It is crucial that each investigator is shadowed at all times by a company employee.

These 'shadowers' should make an additional copy of each document either retained or copied by the investigators, and also request a complete list of those documents from the investigators. Any questions asked by the investigator, as well as answers given, should be noted. A shadower should also ensure that no attempt is made to read or copy either 'privileged' documents or information that is not relevant to the scope of the inquiry.

Replying to questions

The rights of regulatory authorities vary in asking questions of employees during a raid. The OFT and EC are permitted to ask questions on the

location of relevant documents and request explanations of particular contents – for example, the meaning of internal codes. More general questions are not allowed and should not be answered; employees should take care to avoid self-incrimination or incriminating the company.

Although investigators generally have the right to ask to speak to any employee, a company should try to maintain a single point of contact for any questions – preferably an in-house lawyer or senior executive.

Other points to note

It is important not to inform anybody outside the company (other than external legal counsel) of the inspection, or to send internal emails commenting on the investigation, other than necessary instructions to staff.

In no circumstances should documents, whether electronic or hard copy, be destroyed once investigators have arrived. In the event an inquiry lasts for more than one day, the regulatory authorities may seal boxes or rooms; such seals should be well protected and staff should be instructed not to tamper with them.

In December 2010, the EU General Court upheld a fine of €38 million against a company for breaching an official seal following a dawn raid. Fines of up to 1 per cent of a company's annual turnover are permitted under EU law for such acts, and it is not necessary to prove by whom the seal was broken. Likewise, any destruction of a document that a person under investigation knows or suspects would be relevant to an SFO inquiry is a criminal offence.

Legal privilege and relevance

It is important that a company utilises its right of legal privilege during a dawn raid. The basic position under EU law (which will apply in the event of an EC raid) is that privilege covers confidential written communications between a company and external lawyers qualified in the European Economic Area (but not in-house lawyers), made for the purposes of the company's rights of defence. Under UK law, the position is more nuanced: privilege will generally apply to written communications with in-house lawyers and, broadly speaking, any legal communication created for the purpose of being used in actual or potential litigation.

The consequences of failing adequately to protect communications under legal privilege may be significant: in 2004 the EC fined Akzo Chemicals €21 million, having relied on incriminating communications between the company's in-house lawyers and various senior employees. The European Court of Justice upheld the fine, on the basis that in-house lawyers are not generally protected by legal professional privilege.

Employees should look to ensure that the investigating authority does not review documents that fall outside the scope of the mandate and are thus not relevant to the investigation. However, this is a judgement exercise; it may not be advisable to contest the relevance of borderline documents too strongly as this may be regarded as an attempt to obstruct the investigation. The final decision on relevance will be taken by the investigators, although it may be possible to redact irrelevant parts of a particular document.

Immediately following the raid

In practice, the steps that the company takes in the days after a dawn raid often have a significant bearing on the outcome of the case. The best course of action immediately following a raid will depend on the type of investigation involved and the specific facts at issue, but certain steps are necessary in response to any type of raid.

Assemble the right team

In larger organisations, there may be employees whose role would involve organising an internal investigation following a dawn raid. It is nevertheless crucial, given the potential impact on a company, to obtain appropriate external assistance. In terms of legal advice, since the initial stages of an investigation are of key importance in its eventual outcome, it is vital to select

experienced external counsel at the outset. It may also be necessary to obtain advice on handling the public relations consequences.

Ensure the retention of documents

A company that has been raided should immediately issue a 'document hold' and employee guidance on the retention of documents. It is critical that the company takes steps to ensure the preservation of all documents, data and other potentially relevant information, including electronically stored data, in order to avoid possible criminal penalties and jeopardising potential leniency applications.

Complete an initial internal audit

The company must immediately commence an expedited review of the evidence copied or confiscated by the authorities during the dawn raid. It is crucial to identify the salient facts regarding the alleged offence in order to be able to take the appropriate decisions on the best course of action. In particular, the company must take an initial view on whether there is any foundation for the allegations. An initial document review, possibly combined with brief interviews of relevant employees, will often be sufficient to formulate a working defence strategy.

Formulate a first defence strategy

Considerations relevant to all investigations

In most instances, a party's freedom of action in the immediate aftermath of a raid will be constrained by the authority's powers to demand explanations, document freezes and the production of documents from the raided party. In these circumstances, the most appropriate response is to obtain external legal advice immediately, both in order to start formulating a defence strategy and to ensure that the company is clear about its continuing obligations to the investigators and any relevant limits on their powers. For example, the SFO has ongoing investigatory powers that can be exercised on the same basis as when the initial raid took place, and any obstruction of these will also constitute a criminal offence.

Issues relevant to competition investigations

In the context of a competition investigation, the actions of the company in the immediate aftermath of a raid take on an even greater significance, since the severity of the sanctions for anti-competitive behaviour may be substantially mitigated in nearly all jurisdictions should a company choose to admit its role in a cartel and provide full evidence against itself at as early a stage in the investigation as possible. The fact of the dawn raid normally suggests that a participant in a cartel has self-reported and therefore assumed the 'immunity position'. There is, however, significant value in being 'second in' (a 30-50 per cent reduction in fines) as opposed to third (20-30 per cent reduction) or fourth (up to 20 per cent).

Cartel participants that have coerced others into participation will not be able to benefit from immunity in certain jurisdictions. It will, as a result, be important to quickly identify the role played by the company in a cartel.

The raiding authority will usually announce the dawn raid in the relevant sector within a few days, so alerting rivals that may look to approach the competition authorities. Responding quickly could make a difference. To minimise risk, a number of competition authorities may be contacted on an anonymous basis for guidance.

Certain jurisdictions allow a company to request a 'marker' to preserve an early-reporting time while the company performs a fuller internal investigation. The company must submit relevant evidence within the set period to 'perfect' this marker. Note, however, that a marker may be revoked only if the company fails to find evidence of an infringement, and not if it subsequently decides on a strategy of non co-operation.

Approaching local counsel in other jurisdictions

Many investigations lead to criminal and civil liability in multiple jurisdictions where a single set of facts amounts to an offence in those countries.

Under the Bribery Act, for example, companies may be liable for the act of bribery, the failure to prevent bribery and for the actions of their business partners wherever these take place, including where these partners are foreign companies.

Once a company has established those countries that may be affected, counsel should immediately contact experienced local counsel in those jurisdictions. The 'priority' areas include the EU (and member states), the US, Canada and Brazil – although Australia, Japan, New Zealand, Mexico and South Korea are increasingly active, in particular in competition enforcement.

Once a shortlist of 'hot' jurisdictions has been drawn up, the company will need to determine, in conjunction with local counsel, whether there is any value in approaching the relevant authorities to self-report the infringing behaviour in order to obtain formal or informal leniency in any future proceedings. For competition investigations, this shortlist will usually comprise the countries in which the alleged participants achieved sales; for other types of investigation, the relevant jurisdictions may be identifiable from the facts of the offence in question.

Conducting an internal investigation

Setting the scope of the investigation

The next priority is to determine the scope of the full internal investigation, and the physical location and custodians of the documents under investigation should be the starting point.

Non-competition investigations

For a raid involving potential criminal offences, it will be important to determine the individuals responsible (if any), and whether or not their seniority in the company, combined with any negligence in the compliance procedures and/or corporate behaviour, may lead to criminal sanctions against the company itself.

An appropriately focused internal investigation will identify any compliance-related failings, especially in a larger organisation, which may need to be remedied at the earliest opportunity to prevent any recurrence of the offence in question. It will also identify any ongoing offending behaviour that could aggravate the severity of potential sanctions.

It may be apparent to a company or individual subject to an investigation that an offence has not, in fact, taken place; if this is the case, the internal investigation must be prompt, thorough and appropriately targeted in order to mount as vigorous a defence as possible against any future charges.

Cost considerations may also come into play in determining the scope of an internal investigation; there may be limited value to a company in conducting an extensive and expensive inquiry if the relevant facts can easily be identified. In such circumstances, it may be worth adopting a more passive approach and simply responding to requests made by the authorities. It will be necessary to seek the guidance of external legal advisers in this regard.

Competition investigations

The scope of an internal investigation will often be far greater when a competition is the issue. In general terms, the investigation will need to catch the following:

- *Affected products.* The inquiry should focus in the first instance on the sector in which the raiding authority appears to be interested. It will be essential to understand the chain of distribution, the extent of sales (both direct and indirect) and the customers that may be affected.
- *The geographic scope of the alleged conduct.* The jurisdictions in which a cartel may have operated should be quickly identified. Any investigation flowing from the dawn raid will potentially draw the interest of competition authorities in other jurisdictions and, as described above, it may be possible to gain substantial discounts by voluntarily approaching thse authorities.
- *The duration of the alleged conduct.* The

investigation should determine the starting point of the alleged anti-competitive behaviour and whether there may have been any identifiable 'breaks' in such conduct.

- *The nature of the alleged conduct*. The investigation should assess whether the conduct involved geographic market allocation, price fixing, bid rigging or information exchange, the frequency of any meetings with competitors and the purpose of such contacts, and the specific role played by the company in a cartel.
- *Key employees for interview*. The individual role played by the relevant employees must be established. Witnesses should be interviewed separately and accurate notes recorded. The interviews should be carried out by external local counsel for the purposes of protecting legal professional privilege.
- *Other possible infringing conduct*. The inquiry should explore all anti-competitive behaviour with company employees – not just their knowledge of the products affected by the anti-competitive behaviour under investigation.

Managing the internal investigation

Although the internal inquiry should be set in motion as quickly as possible, the company must take care to assemble an independent team able to supervise the investigation across the relevant business units and jurisdictions. The company should also confirm whether there are any existing or concurrent investigations being carried out by other competition authorities. Co-operation and co-ordination between these enforcement authorities, often on an informal basis, should be expected.

Considering 'amnesty plus'

As described above, in the context of a competition investigation, the company's internal inquiry should extend to possible cartel activity in other sectors. This is particularly relevant in jurisdictions that have adopted the 'amnesty plus' programme, under which companies co-operating with the competition authorities may also report anti-competitive activity in related product markets in return for an amnesty for those markets. In the US, there may be negative consequences for a failure to do so, referred to as 'penalty plus'. The US competition authorities will probably ask witnesses about any other anti-competitive conduct of which they have knowledge – the so-called 'omnibus question'.

Next steps

Continued co-operation with the regulatory authorities

In the context of competition investigations, in order to qualify for immunity or a reduction in penalties, the company must continue to meet the conditions of the relevant leniency programme. It will be required to co-operate fully with the authorities, in particular by providing accurate and complete information. It will be further obliged not to disclose the fact or content of the leniency application and not to destroy, falsify or conceal relevant information or evidence relating to the alleged infringement.

A failure to comply with the conditions of the leniency programme will disqualify the company from the programme.

It is also likely that ongoing requests for the production and/or explanation of documents and other information will be made by the authorities; responding to these will be crucial, as not to do so may hinder a leniency application and, in certain circumstances, constitute a criminal offence.

Employee management issues

A company will need to consider certain staff-related issues following a dawn raid, including applicable employment law and data protection rules. For example, the company may need to obtain an employee's consent for the transfer of his or her personal data outside the European Economic Area, where the third country may not ensure an adequate level of protection.

In addition, it will be essential to resolve any

conflicts of interest between individual staff members and the company. For example, some employees may require separate legal representation in certain jurisdictions, such as the UK and the US, depending on the alleged conduct.

A company may also need to consider whether disciplinary action may be appropriate. Often, investigating authorities will expect individuals involved in unlawful or criminal behaviour not to be promoted subsequently, and may even wish to see them demoted or even dismissed in the context of a formal or informal co-operation programme.

Accounting and disclosure issues

A company may also want to consider including provisions in its accounts to reflect its potential financial exposure to sanctions and/or civil litigation.

Bespoke compliance programmes

A company should also review and update (or put in place) compliance programmes in order to reduce the chance of recidivism. The nature and extent of the programme may depend on the size of the company, the relevant sector and the background of the employees, but it will often include the circulation of a detailed compliance manual, together with regular training sessions and interactive tools.

Preparing for civil damages actions

The potential for civil damages actions will depend on the alleged offence under investigation. But where it could have a significant negative effect on a listed company's share price, for example, the company's own shareholders may contemplate civil actions for damages against the management.

In the context of anti-competitive conduct, in particular, there is a significant risk of private litigation. Although, historically, that danger has been confined to the US, other jurisdictions are in the process of establishing effective legal frameworks for such actions. In addition, in the EU, a final EC infringement decision will be binding on national courts in member states and may give rise to 'follow-on' actions.

A company must therefore secure and review all documentary evidence in its originating jurisdiction to protect against the risk of discovery in any future foreign proceedings. A company should take care to check the location of servers used to host related documents.

Conclusion

The steps taken by a company in the days and weeks following a dawn raid will often have a major bearing on the strategic choices subsequently open to the company. The difference between getting the strategy right and getting it wrong can usually be measured at the end of any lengthy investigation.

23

How to manage a corporate fraud investigation – limiting the damage and protecting your business's reputation

Jonathan Hitchin, Partner, Arnondo Chakrabarti, Partner, and Davina Given, Senior Associate Allen & Overy LLP

A corporate fraud investigation can have serious consequences for a company, regardless of the final outcome. Potential customers may prefer not to enter into contracts, existing customers may drift away, recruitment of new employees may be hindered, morale among existing employees may fall, and management time that might have been better spent building a business is spent managing the investigation.

While some damage is inevitable, there are ways in which companies can limit that damage before the investigation starts and at all stages of the investigation right through to its conclusion.

Pre-investigation preparation

Before an investigation begins, corporates can do much to protect themselves.

Prevention

It is becoming increasingly important that corporates arm themselves with appropriate policies and procedures to prevent fraud. While, historically, companies have been focused on possible fraud within their business, the regulatory environment is forcing them to look externally as well, for fraud against customers. The Bribery Act 2010, and the accompanying guidance from the UK Ministry of Justice on preventing bribery, is only the most recent example of this.

The primary aim of any such procedures is prevention of corporate fraud and that is, of course, the best way to protect a corporate's reputation. However, rapid identification of warning signs is also valuable, and a company that can demonstrate early in an investigation that it has robust controls in place may be able to persuade a prosecutor to focus on investigating 'rogue' individuals rather than the corporate itself. At a later stage, if a company is prosecuted, its procedures may constitute a defence, or at least potentially important mitigating factors in the context of a sentencing decision.

Preparing for the worst

While the possibility of an investigation should not be the driving force in how a business is run, corporates can build that risk into their ordinary

processes in order to allow them to respond better to an investigation. Key to this is effective document management. Ideally, corporates should be able to:

- explain their IT infrastructure quickly and clearly
- store material relating to a particular project in one or more easily defined areas, so as to avoid the expense of having to trawl through large parts of the IT system to identify a relatively small number of relevant documents
- isolate legally privileged material
- rigorously enforce a document retention policy applicable to both hard-copy and electronic information, in order to ensure uniformity across the business and to limit the quantities of data that need to be processed for an investigation, while maintaining adequate records for business, legal and regulatory purposes.

Corporates should also consider implementing and testing a 'dawn raid' policy, to ensure that the right people (including communications/PR specialists) will be notified to help the company keep control in what is potentially a very difficult situation.

Early warning signs

Corporates should encourage internal 'whistleblowing'. This may be difficult in the face of increasing incentives for whistleblowers to make their first report externally. English law provides for immunity from prosecution in exchange for a whistleblower's assistance and reduced sentences for convicted whistleblowers, while the US Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 provides substantial financial incentives to whistleblowers for reporting financial fraud, as well as extending whistleblower protections to employees of foreign affiliates whose financial information is consolidated with a US reporting company.

Once an external report is made, the matter may be out of the corporate's control. By contrast, if an internal report is made first, that allows the company to take the initiative in investigating the matter and managing external reporting (whether to the authorities, the media or otherwise) so as to protect its reputation.

The initial stages

1. Act quickly in response to allegations

Sometimes a corporate will not know that there are potential issues until the police arrive to arrest individuals and seize documents. On other occasions, the corporate may have time to respond between public allegations of wrongdoing and an investigation. Such allegations may arise from:

- the media
- disgruntled customers or competitors (anti-trust law, in particular, seeks to take advantage of this by offering immunity to the first participant to report cartel activity)
- reviews of the business environment, such as the thematic reviews of products or business lines carried out by the Financial Services Authority (FSA)
- actions by foreign regulators.

In these cases, the corporate is likely to be on the back foot. It may be better to seize the initiative, where possible, to defuse any issue early, rather than allow a stream of damaging allegations to continue. This may involve launching an internal investigation or review, offering redress to consumers or approaching the relevant regulators or prosecutors.

2. Identify a core team

Once an external investigation has begun or action is being taken in response to public allegations, important strategic decisions will need to be made, and the right people must deal with them. Key elements of the team may be:

- *senior management*. In large corporates, and in

Self-reporting

As soon as an internal or external investigation begins, it is necessary to start considering whether, when and how to self-report issues to the applicable authorities. In some cases, there may be an obligation to do so; in others, favourable treatment may result. How this is managed may be a fundamental feature of the damage limitation process.

In England, there are three principal situations in which a report may be required:

- if any benefit from the suspected fraud remains in the business, those dealing with that benefit run the risk of committing a money laundering offence under the Proceeds of Crime Act 2002, unless they report to and obtain consent from the Serious Organised Crime Agency (SOCA). This legislation has the potential to extend liability in the business beyond those included in the original fraud
- persons in the 'regulated sector' (including bankers, auditors and, in limited cases, lawyers) must make a report to SOCA where they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering. The possibility that a third party may report the suspected fraud in turn puts pressure on a business to report even if it is not required to do so in order to manage that risk
- FSA-authorised firms are required to disclose to the FSA anything relating to the firm of which the FSA would 'reasonably expect notice', as well as any matter that could have a significant adverse impact on the firm's reputation, and (where it is significant) employee fraud on a customer, fraud or attempted fraud against the firm, or suspected serious employee misconduct connected with the firm's business that concerns their honesty or integrity. Failure to do so will constitute a regulatory breach that may lead to further investigation, publicity and sanctions.

In these situations, the choice of whether to self-report may not be a real one; a report must be made. In other circumstances, voluntary self-reporting may bring the company protection or limit damage. For example, many prosecutors, including the Serious Fraud Office and the US Department of Justice, offer informal credit to those who self-report, with the possibility (but not certainty) of:

- the subsequent investigation being limited
- no prosecution
- prosecution on better terms
- a reduced sentence (though in England, sentencing remains in the sole discretion of the courts).

Anti-trust prosecutors offer even more concrete benefits, with the first in a cartel to report being offered immunity from prosecution.

Where self-reporting remains voluntary, the decision whether to do so needs careful, early consideration and continuing review. Relevant factors will include the likely credit, the involvement of other authorities and third parties, the likelihood of prosecution, the information available about the suspected fraud, and the consequences of a conviction. Although they may not always be appropriate, carefully managed disclosures can avoid damaging enforcement action or, at least, assist the business in proactively managing the investigation and related publicity.

cases of severe and/or widespread wrongdoing, it may be necessary to involve the board of directors. It is essential to ensure that the team does not include any of those alleged to have been involved in the wrongdoing, as this will undermine the company's response to the investigation, internally and externally

- *public relations specialists* – to manage media interest
- *IT* – to manage any document recovery exercises
- *human resources* – to deal with the employees implicated
- *internal and external legal advisers*, although external advisers will not be required in all cases and a judgement will need to be made based on the circumstances
- *compliance personnel*
- *internal and external audit or accounting advisers* – to assist in tracing financial flows.

3. External communications

If a significant issue arises, a public announcement may be appropriate. In some cases, this is a necessity: price-sensitive information must be disclosed by listed companies in the UK and information that would have a material effect on a company's finances may need to be included in its accounts. In other cases, it will be optional. Given the potential impact of negative press coverage on customers, employees and investors, businesses should give careful thought to their media strategy from the beginning, using internal or external public relations specialists where appropriate.

Internal management of investigations

Once an investigation is under way, significant resources are likely to be needed to ensure that all the moving parts are co-ordinated to provide the best possible corporate response.

1. Internal communications

First, an internal communications strategy may well be necessary. It is likely to be important to control the content and flow of information to those who need to know. Employees should be warned to be careful as to what they commit to writing in relation to the suspected fraud or investigation; unprivileged communications after the event, speculating on what happened, can be very damaging.

2. Preserving documents

Companies should identify where relevant documents (hard copy and electronic) may be located and ensure they are preserved (specialist IT support may be required). This will allow the business to piece together what happened with a greater degree of accuracy. It is also likely to be an offence if documents relevant to a criminal investigation are falsified, concealed, destroyed or otherwise disposed of.

What is relevant will depend on the scope of the investigation, so an early discussion with the investigating authority will help to define this.

3. Dealing with implicated employees

If current staff are implicated in the suspected fraud, careful consideration should be given to:

- whether they need independent legal advice
- who should fund that advice (insurance cover may be available)
- their position in the business ('no fault' suspension or dismissal may be appropriate). Advice on employment law may also be needed.

Attention needs to be given to the evidence against the employees, and their continued access to any materials relevant to the allegations. Their disciplinary position should continue to be assessed during the investigation as more facts emerge. If you are dealing with a whistleblower, he or she will also have the benefit of certain statutory protections. Again, employment advice should be sought throughout to ensure that any disciplinary process is dealt with properly.

If an employee has been suspended or dismissed,

the company may well want to try to ensure that the individual continues to co-operate. However, although an agreement can be entered into with the aim of achieving this, it may be difficult in practice to secure that co-operation, particularly if an employee is dismissed. In addition, any severance payments need to be carefully considered from both a legal and reputational perspective.

4. Internal investigations

Finally, once a criminal investigation has begun, the value of an internal inquiry should be assessed as it may allow the business to understand the principal facts relatively quickly and cheaply and to determine its approach accordingly. However, the views of prosecutors differ as to whether companies should conduct such inquiries. It may be prudent to consult with the relevant investigators to ensure that evidence is obtained in a way that the prosecutors are content with.

External management of investigations

In parallel with the internal concerns noted above, management will need to maintain a balance with the investigator or prosecutor between:

- the co-operation expected of a good corporate citizen
- the potentially significant resources required
- protecting the company's position.

1. Documents

Corporate fraud investigations tend to involve a sizeable quantity of documents. Most investigators have powers (granted by the court on a case-by-case basis or in their own right) to search property and seize material, or to require persons to produce specified information. The former approach puts the onus on the investigators to identify and find relevant material, but it is likely to disrupt the business, increase the risk of accidental loss of privilege, damage staff morale and generate adverse publicity. A company may prefer the alternative, where possible, of producing documents itself.

2. Waiver of privilege

If a company is raided, investigators have a duty to take steps to preserve the company's legal professional privilege. If material is clearly privileged, it should not be taken. If it is not practicable to determine whether or not material is privileged at the time of the search, the data may be seized and the investigator and defence lawyers will subsequently agree, or apply to the court to determine, a procedure for dealing with it. Usually a review by independent counsel is appropriate. Equally, a company cannot be compelled to disclose any privileged information or produce any privileged documents.

Privilege is an important protection for a company, enabling it to be full and frank when seeking advice as to its legal position, but it is sometimes regarded with suspicion by investigators. In some circumstances, companies should consider whether waiving privilege would be more beneficial than preserving it. This may be viewed as a positive sign of co-operation by the authorities, and the privileged information may be supportive of (or at least not damaging to) the company's position.

However, partial waiver over only some documents may amount to a waiver over all related documents and it may not be possible to limit the waiver to the investigation.

A company will therefore need to be satisfied that any short-term advantages are not outweighed by the wider consequences (such as disclosure in broader civil litigation).

3. Employee arrests and interviews

Prosecutors may wish to arrest and interview the corporate's staff. Businesses face a number of practical challenges when managing these interviews, from the loss of the employee's time to obtaining separate legal counsel. Perhaps most difficult for both company and employee is that an arrest or interview may become public and attract media attention. The company will need to handle this carefully to minimise reputational damage, paying attention to small details (such as

arrangements for the employee's entrance into and exit from the interview) as well as the larger questions of media strategy.

4. Interplay with foreign authorities

Investigators have frequent contact with foreign authorities, sharing information both informally (such as through police-to-police channels) and within the formal framework of mutual legal assistance, which depends on the relevant arrangements between the UK and the states in question. Although theoretically the owner of any documents being sent abroad should usually be given notice of the disclosure, there is no guarantee that this will occur. Investigators may also co-operate to restrain assets and enforce confiscation orders internationally.

A corporate may therefore be in the position of dealing with multiple investigators in different jurisdictions, with different powers and agendas, conducting investigations on the same or similar facts, with information being shared to an extent unknown to the corporate. This can cause increased difficulties and costs. It can sometimes, but not always, be in the company's interests to encourage different investigators to co-ordinate with each other.

5. Dealing with affected customers

A corporate being investigated or prosecuted for a criminal offence may also face civil claims arising from the same issues. Although the English courts have discretion to stay civil proceedings pending the outcome of criminal proceedings if there is a real risk of injustice, generally the civil courts will allow the proceedings to continue concurrently. Such civil claims may raise the media profile of the issue, as the alleged victims try to exert maximum pressure on the company. They also carry a greater potential risk of liability, given the lower standard of proof. A finding of civil liability may also be taken by the media as evidence of criminal liability, even if the business is never prosecuted.

It may therefore be important to communicate with affected customers carefully from the beginning. This may also be appropriate, in any event, from a general business perspective.

Agreeing outcomes with the authorities

Theoretically, the conduct of investigations and prosecutions is largely in the hands of the authorities. Increasingly, however, corporates are taking the initiative with a view to finding a quicker solution.

At quite an early stage, a company may seek immunity from prosecution. This is well-established in the anti-trust field for the corporate that is first to report, but it also exists in a different form for other offences (where it is not always tied to the first person to report and is at the discretion of the authorities). However, while this may offer protection from criminal liability, there will be little protection from the media if the matter becomes public, or from civil claims.

Alternatively, a corporate may seek to negotiate with the investigators to reach an agreed end to the inquiry. 'Settlement' of a criminal investigation may take different forms:

- *no further action*. The prosecutor is satisfied that no offence was committed, or that the evidence is insufficient to provide a realistic prospect of conviction, or that prosecution of the offence is not in the public interest
- *civil recovery*. Where a prosecution is not possible or appropriate, the prosecutor can seek a civil recovery order in the High Court to recover 'property obtained through unlawful conduct'. However, English criminal courts consider that it will rarely be appropriate for criminal conduct by a company, that can be established to the requisite standard of proof, to be dealt with by means of a civil recovery order
- *prosecution on an agreed basis ('plea agreements')*. The company and the prosecutor can agree the charge and the facts upon which a guilty plea will be entered. This offers the possibility that the corporate may receive substantial

credit on sentencing. At present, however, the sentence cannot be agreed and is in the discretion of the court.

Remedial action

In the event that a corporate has been involved in a criminal investigation, regardless of liability, the steps that its senior management takes by way of remedial action can play a significant role in (a) persuading the prosecutors to take no, or more limited, action; (b) repairing reputational damage; and (c) mitigating future risks. Such remedial actions may include:

- an independent or other senior-level review of events to understand what went wrong
- organisational changes to remedy any weaknesses in the control environment
- redress to affected third parties
- the use of compliance monitors
- appropriate disciplinary action against employees.

Conclusion

A fraud investigation can be deeply damaging to a corporate, regardless of the outcome, in terms of its share price, its employees' morale and its future prospects. It is unlikely to be possible ever to eliminate that risk. However, both before and during an investigation, there are active steps that a company can take to manage the risks.

In accordance with the duty of directors to have regard to the interests of a range of stakeholders in performing their roles to promote the success of the company, those steps will require a careful balancing of the financial resources of the business, the demands of investigators, the needs of employees, the interests of shareholders and the desires of customers.

• *The authors would like to thank Michelle de Kluyver, Oliver Rule, David Pygott, Laesha Smith and Trevor Withane – part of the global anti-corruption team at Allen & Overy – for their assistance in researching and writing this chapter.*

24

Finding the silver lining in a cloud of chaos: a practical guide to managing an external corporate fraud investigation

Andrew Gordon, Partner, and Robert Wilson, Senior Manager PwC

Nobody reading this book will imagine that having the police or other law enforcers come through your office door at 6am (and simultaneously your chairman's, chief executive's, financial director's and junior sales manager's *home* doors) is going to be a fun experience. But have you thought just *how bad* it could be? The ensuing crisis can bring a business to its knees, not to mention setting the share price tumbling, if you don't manage the process carefully and proactively. So what are the practical things that can help minimise the impact and how, if at all, can you turn the situation to your advantage?

Plan, prepare, plan again

You already have a disaster recovery and business continuity management plan, don't you? It's on the shelf with your risk register and fraud response plan, ready to be refreshed regularly for your changing environment and business needs. Excellent – you already have the majority of what you need; you just need to think through a few extra scenarios to which you can apply the processes.

It's not too difficult to see that losing your records in a fire is pretty similar to having them seized by the authorities. Maintaining your 'business as usual' processes in as orderly a manner as possible could make the difference between survival and failure.

Take the other scenarios you have already prepared for and then consider their relevance to all other similar risks, such as loss of records, loss of staff, loss of power and systems, loss of premises – as many of the so-called 'black swan' events as you can think of. Get your team involved – brainstorm similarities and differences between scenarios, thinking of contingencies and consequences. Learn from previous events. You should find that preparing for fraud strengthens your broader crisis-response plans.

If the worst happens

Don't take it personally; be professional; it's just another part of business. Whether you are responding to a dawn raid or a letter asking you to attend a meeting, start by calmly assessing what the requirements of the investigators are. Be clear what the agenda is and what it isn't:

- what are the areas of focus?
- is it the entire business or particular areas or subsidiaries?
- how broad is the scope of the investigation?
- what other parties are involved?
- what individuals are involved?
- are you the target or do you just have relevant information?

It may not be possible to answer these (and the many other questions you will think of) immediately, but achieving some clarity on the outcomes desired by you and the investigators from the start will help you manage your way through the investigation.

To help answer these questions, engage quickly and positively with the investigators. Openness and transparency should be your guiding principles from the start, within the limits of the provisions of the search warrant, of course. Be constructive and friendly and don't be afraid to clarify any of the requests. Careful and accurate disclosure will help both parties; the investigators will not have the time, resources or desire to wade through irrelevant material. Building trust early on will help in the long run. It is also sensible to agree reporting channels and points of contact (internally and externally) to manage the flow of information.

If the investigators are seizing documents, take copies of key items that you need to continue your business. Warrants are usually obtained on the proviso that investigators will endeavour to minimise their impact on the ongoing business, and the investigators and police we have worked with have all been sensible and pragmatic. You will also want a copy of the search log to determine exactly what items the investigators have taken.

The overarching aim of any search will be to secure potential evidence; this is in your interest too as you will not want to breach your obligation not to destroy relevant material. It is, however, worth making sure that you have a sensible document-retention policy that you follow through – in other words, during the normal course of business (not during an investigation), don't keep documents you are not legally obliged to keep for longer than you need them. If you are raided, you will regret having 20 years' worth of back-up tapes and archive material.

Searches of premises, particularly private residences, are by nature very intrusive; courts do not grant search warrants lightly. Investigators generally understand fully the sensitive nature of what they are doing and respond professionally to reasonable requests – for example, avoiding certain areas of the office to minimise disruption. Talk to the person in charge to agree a mutually acceptable way of working together.

Get help

You hopefully won't have been through this process before (and you won't want to again). That means you will not have the in-house expertise to deal with all the intricacies of an external fraud investigation. Good advisers appointed early on will make a huge difference to the outcome.

It is important to think of the structure that this team takes. For example, it will be sensible for your in-house counsel or law firm to instruct the investigators in order to maintain legal privilege. You should ensure that the person in your business overseeing the work is not tainted by the accusations; it often helps for this role to be taken by a non-executive team or the audit committee.

You may want to consider the use of a specialist criminal legal team if your usual lawyers do not already have the expertise. You could also hire your own independent investigators. There are several benefits to this approach:

- the experts will be able to focus quickly on the key issues (the need to restore back-up tapes, say) and will know how to deal with problems (the tapes have been lost)
- law enforcers or other external regulators will feel more comfortable relying on independently prepared material (see 'seize the moment', below)
- your stakeholders will see you are taking the

matter seriously and that you are acting decisively to resolve the issue
- it will reassure staff and other stakeholders that there will be no 'cover-up'
- you will be freed up to get on with business as usual
- it will be easier to treat the matter dispassionately, causing less internal disruption and tension, which can be of particular benefit when it comes to disciplinary matters.

You may also want to consider engaging specialist PR help; you will certainly need to get your external communications strategy agreed and planned carefully. You will also want to …

Seize the moment

Take the initiative and control the information flow from an early stage of the investigation. This is easier than you might think; law enforcers and regulators, operating on constrained resources, may not have the time to review high volumes of paper and electronic data quickly and efficiently. Indeed, in certain circumstances, they might prefer you to conduct your own investigation and self-report to them.

But they will want to know they can rely on your findings and that you have been thorough and completely transparent. This is *not* an opportunity to sweep things under the carpet.

Taking control of the investigation in this way has three main benefits:

- it allows you to set the pace, which will help you to maintain business as usual
- it can shorten the investigation; no one else understands your systems and data as well as you, so you will be able to find things more quickly
- you can control the way the information is presented, although you will obviously not want to misrepresent the facts.

The risk with any form of self-reporting is that someone could accuse you of not giving full disclosure. In our experience, it is often a matter of individual judgement whether specific documents are relevant to an investigation, and prosecutors and defendants will frequently argue the point. Deciding what is relevant requires not only a clear understanding of the specific information request but also the purpose for which the information will be used, which may not always be obvious. For example, the investigators may want documents that seem unrelated to the inquiry but help them to give background to their case.

You can use this principle to your advantage by providing information that the investigators may not have thought were relevant but which might help any defence you wish to make.

Our advice on self-disclosure is to give more rather than less. This maintains trust with the investigators and demonstrates your willingness to be open and transparent. The law enforcement officers we have worked with have always treated sensitive information with appropriate respect and professionalism, and so you should not be afraid to confide in the person leading the investigation. Helping the investigation team to deliver the outcome they are looking for will ultimately work in your favour.

And while you are collecting all of this data and knowledge about your business, you can do something productive with it:

- map out your systems and processes
- assess what is fit for purpose or ready for renewal
- reassess your contracts and third-party suppliers
- look at ways of increasing efficiency among your processes.

Keep the pressure on them

You don't want this to drag on, particularly if you have done nothing wrong. The legal process can often seem to move at a snail's pace. Look for ways to resolve the matter as quickly as you can and keep in touch with the lead investigator to make

sure they are dealing with the matter. They too will be under pressure due to targets and resource constraints.

Sometimes there will be little you can do, at which point you should try to set the matter to one side. This will be easier if you have been in control of the situation and have carefully kept records, enabling you to put the work on hold and restart it again quickly when required to.

One vital ingredient for a smooth investigation is effective project management from the start. If you have the experience needed, all the better, but if not, call in a professional project manager who can, among other things:

- manage the flow of information and requests
- plan the investigative and reporting tasks, looking for dependencies and overlaps
- keep everyone up to date with appropriate management information.

This really does speed up the process and removes a huge burden from you and the investigators.

Cometh the hour

As a modern business leader, you are already trained in engaging your staff and transforming your business. The only difference now is that your staff will be actively looking for this leadership. The basic skills will never be more important:

- communicate
- be authentic
- set the tone.

Your staff will be looking for reassurance – if you can, be reassuring but don't duck the big issues. Be straight with people and be positive; encourage them to help resolve the matter and come forward with relevant information.

Come out stronger

So where is the silver lining? The experience will undoubtedly hurt your business but there will be opportunities to take a good, hard look at the way you work. Use the investigation to:

- assess your governance and internal controls – what were the failures that stopped you seeing this coming?
- root out other problems – you don't want the investigators back
- retrain and refocus your staff – make sure lessons are learnt and demonstrate that you will not tolerate bad behaviour
- implement change – you are already in a state of disruption, so push through any other business and process changes you were thinking of
- consider whether you are setting the right tone at the top – do you need to make some cultural changes to regain the confidence of your staff?
- demonstrate strength and leadership to staff, the board, markets, stakeholders, regulators and potential recruits through effective communication.

You should also consider what remedial action you can take:

- are you insured?
- who can you recover funds from (if it is cost effective to do so)?
- do you need to take disciplinary action?
- should you consider strengthening your team with additional or replacement staff?

Opportunities to rebuild or improve may not be that obvious, so take time to talk to your team and your advisers in order to learn the most about what went wrong and how you can act differently in future.

Every business will suffer some form of fraud. Prevention is better than cure, but some simple advance planning can ensure that you are ready to deal with any crisis effectively.

25

Internal corporate investigations: avoiding the pitfalls

Robert W Henoch, Partner (London), and Brad H Samuels, Associate (Washington DC) Kobre & Kim LLP
PwC implementation focus Tony Parton and Tracy Gill

Against the backdrop of increased white-collar crime enforcement in both the UK and US, an effective strategy for the internal investigation of potential wrongdoing has become a critical component of good corporate governance. A well-executed internal investigation can help a company identify and remedy misconduct, evaluate the pros and cons of disclosing wrongdoing to the authorities, and potentially limit criminal or civil exposure and reputational harm. Conversely, the failure to conduct a well-tailored and impartial investigation when facing allegations of potential misconduct could make prosecution more likely and subject the company to greater liability and reputational damage.

The current enforcement environments in the UK and the US also require that companies are prepared to conduct cross-border internal investigations. Numerous UK and US laws touch on cross-border conduct. For example, the UK Bribery Act extends to any company, wherever incorporated, if it "carries on a business, or part of a business, in any part of the United Kingdom". Similarly, the US Foreign Corrupt Practices Act provides the US with jurisdiction over any company with securities traded on a US exchange, any company or individual if an act of misconduct occurs within the US, and any US citizen or company operating anywhere in the world. Export control, money laundering and securities laws also can touch on cross-border activity.

The potential far reach of these laws means that a company could face simultaneous and overlapping cross-border investigations by enforcement agencies and regulators in the UK, the US and throughout the industrialised world. It also means that the conduct at issue, documents and witnesses could be located anywhere in the world or in several different locations. This chapter examines some key considerations in conducting an effective internal investigation with an eye to avoiding common pitfalls.

Who should conduct the investigation?

Specialised outside lawyers with expertise and objectivity

Two considerations are paramount when choosing who should conduct an internal investigation. First, the firm selected should have the savvy, independence and experience to conduct a targeted, efficient and effective investigation. Second, it must be able to proceed with sufficient objectivity

to protect the integrity and credibility of the investigation. These factors weigh heavily in favour of engaging specialised outside lawyers.

In-house attorneys or auditors may not have expertise in conducting complex internal investigations, especially with the host of domestic and foreign laws that could be in play. The high-stakes nature of a government enforcement or regulatory action means that the company cannot afford to undertake an investigation that fails adequately to identify and remedy all wrongdoing.

Significant civil monetary penalties are regularly imposed for violations of UK and US laws, and criminal liability could result in steep fines, corporate monitors, and significant prison terms for executives. Since 2009, the US Office of Foreign Assets Control alone has levied over US$1 billion in fines, including many against non-US entities. Even small mistakes could result in serious consequences, such as the loss of critical evidence, inadvertent disclosure of privileged or proprietary company information, and wasted time and resources. Companies should not risk these fates by engaging inexperienced law firms and investigators.

Use of in-house lawyers or internal auditors can also create the impression, even if incorrect, that the investigation was not sufficiently removed from the alleged misconduct or there were incentives to under-report or hide misconduct. An effective internal investigation can be an important tool in convincing enforcement authorities that misconduct was isolated or that the company has adequate controls to identify and remedy misconduct. If the company hopes to gain favour for its efforts, even the perception of bias could be damaging.

Ensuring that lawyers are sufficiently removed from the company's actions is also important to avoid a scenario where the investigators themselves become fact witnesses. For example, if during the course of the inquiry it becomes clear that in-house or transactional lawyers approved of inadequate procedures or were consulted regarding unlawful or inappropriate conduct, those attorneys would have to be interviewed.

If prosecuted, the company might choose to rely on an 'advice of counsel' defence, which could require the company to waive the attorney-client privilege for all communications with its attorneys, including communications related to the investigation. Because it is not always clear at the beginning of an inquiry whether in-house attorneys or transactional lawyers were connected to the alleged misconduct – or any other unrelated misconduct that might be uncovered – it is wise for companies to avoid using those lawyers to lead an internal investigation.

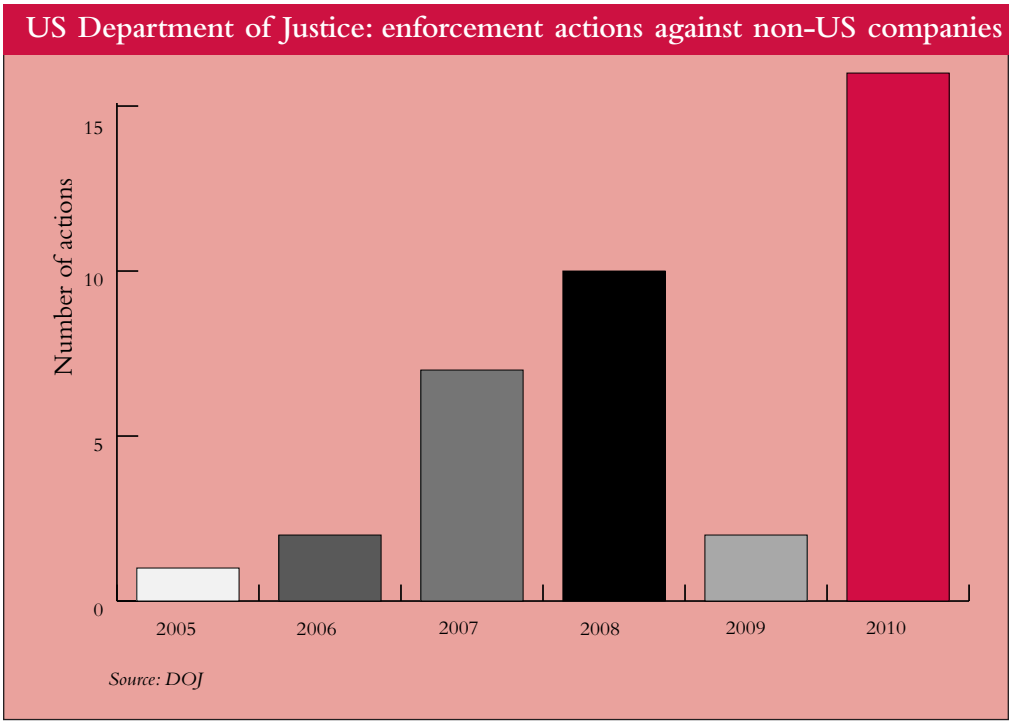
Cross-border investigations may require outside lawyers

In the context of a cross-border investigation, the involvement of outside lawyers may also be necessary to protect attorney-client privileges. Many countries outside the US do not recognise an attorney-client privilege for in-house lawyers, and many of those who do offer only limited protection. Within the European Union, for example, only about one third of the 27 member countries recognise the privilege for in-house lawyers. While the UK, Spain and Portugal are among the countries that do, several significant jurisdictions, including France, Italy, and Sweden, do not. Moreover, despite recognition of an in-house lawyer privilege by several member nations, the European Court of Justice has held that, in the context of European Commission investigations, communications between in-house lawyers and company employees are not privileged.[1]

At the outset of an investigation, a company cannot be sure that the conduct under scrutiny will not fall under the jurisdiction of the European Union or another jurisdiction that does not recognise a privilege for in-house lawyers. The use of outside attorneys can therefore maximise a company's ability to protect its privileged investigation-related communications and reports from disclosure.

Internal management of investigations

Just as with selecting lawyers, independence and objectivity are important considerations in



identifying the appropriate party to manage the investigation. Care must be taken to ensure that the investigation is managed internally by company officials who are sufficiently removed from the alleged misconduct. Enforcement authorities recognise that the company itself is in a position to influence the inquiry and its outcome, regardless of whether outside lawyers are involved. Outside lawyers rely on the company to facilitate access to documents and witnesses, to make the final decisions regarding the scope of the investigation, and to set the budget. The company also plays a crucial role in encouraging internal co-operation with the inquiry. Given this level of involvement and potential influence, the government will naturally lend less credence to investigations managed by parties connected to the alleged misconduct.

There are numerous choices in who should manage the investigation from the company side, including the management or officers, the board of directors, a standing committee of the board, such as an audit or executive committee, or even a special committee created for the purpose of managing the inquiry. Whoever is chosen should have adequate independence and authority to investigate misconduct objectively.

Considerations in conducting the investigation

Flexible work plans

The company and the investigating attorneys should agree at the outset on the initial scope of the investigation, and a work plan should be drafted. The work plan should adequately address the alleged misconduct and be sufficient to uncover additional related misconduct. Although the company's instinct may be to limit the scope in order to save money or minimise disruption, too narrow a focus may not serve its interests. The investigation and any

PwC's implementation focus: internal investigations

Tony Parton, Partner, and Tracy Gill, Senior Manager, PwC

Whether facing a whistleblower allegation, suspected malpractice or any other possible economic crime, a fraud response plan, setting out guidelines as to how to handle an investigation, is vital. All too often, when faced with what appears to be serious fraud, the response of victim organisations is a 'knee-jerk' one that can jeopardise valuable evidence and reduce the possibility of criminal and/or civil action.

The fraud response plan should identify a member of senior management to take responsibility for the investigation. The plan should also set out clear aims, be well designed and flexible, involve suitably qualified personnel and clear reporting lines, and discuss how evidence will be collated and analysed.

Objectives and scope of the investigation

When it comes to investigating fraud, consideration should be given at the outset to the action that the organisation is likely to take if the allegations are found to have merit, as this will have an impact on how the investigation is structured. The organisation should consider if it is going to take civil action against any perpetrator(s) – with the aim of recovering assets, gaining compensation, or both – and/or to seek to punish the perpetrator through criminal action. These two options have different burdens of proof and so require evidence to be handled and documentation to be prepared to different standards.

There is compelling evidence to suggest that the stronger the response of an organisation to possible economic crime, the greater the deterrent to further malpractice. By making it clear to potential fraudsters that criminal action will be (and has been) taken, it is likely to be less prone to the risk of fraud in the future. When faced with serious economic crime, therefore, it is useful to enter into an early dialogue with law enforcement agencies.

The way in which the investigation is carried out is also important. A covert inquiry reduces the risks of tipping off perpetrators (potentially allowing useful evidence to be destroyed) and of adverse publicity, although it could also lead to inaccurate speculation among employees.

An open investigation, made widely known among the organisation's management and staff, has the advantage that a clear signal is sent to would-be criminals. On the other hand, it may create ill-feeling among employees if they interpret the need for an investigation as lack of trust. Each case must be considered on its own merits and it may be that a combination of covert and open investigation techniques is engaged.

Any factors that may affect the duration of the investigation should be considered. For example, material fraud may give rise to error in the financial statements, and the need to report financial results to the market or file statutory accounts will create a time pressure around the investigation while the extent of the fraud and the culprits are identified. It is important that these time pressures are not allowed to affect the quality of the inquiry.

The scope of the investigation should be determined with reference to all the allegations made or concerns raised. That requires detailed analysis of any written communication from a whistleblower or of transcripts of verbal reports. Care should be taken to identify every individual, department and/or location mentioned or potentially relevant. It is important that the scope of the investigation remains flexible and is reviewed on a regular basis in light of the evidence found, with the ability for the inquiry to be expanded or reduced appropriately.

It is also important to identify at the outset how the results of the investigation are to be reported and who is to receive this information. In serious cases, the audit committee will want to be kept informed. Where senior management are, or could be, implicated in the fraud, the audit committee should set the scope of the work.

Who should carry out the investigation?

The skills required to lead an internal investigation will depend on the nature, scale and complexity of the alleged or suspected crime, as well as the suspected

corresponding remedial efforts may be of little value in convincing the government that a problem has been identified and fixed if the government perceives that the investigation was incomplete or ignored potential red flags.

The scope of the inquiry can and should be revised as it takes its course, and the lawyers should advise the company of this potential for evolution at the outset of the investigation. The investigating lawyers should also keep the

culprits. In some cases it will be necessary to engage external, independent, forensic accountants as well as lawyers.

The investigator will need knowledge of, or access to, the organisation's procedures and policies, and potentially employment contracts as well because it may be important that these are complied with throughout the investigation to avoid the risk of employee tribunals. Where foreign jurisdictions are involved, the investigator will also need to be aware of local legislation and regulations, including those on reporting requirements, whistleblower protection and data protection. These may affect the information to which investigation teams are allowed access and whether it can be transported across borders.

It is important that adequate resources are made available and that the members of the investigation team have the necessary skills and are independent of the business or individuals under review.

Undertaking the investigation

The identification, preservation and management of evidence is vital. Accurate documentation is required of the chain of evidence showing how and when information was obtained, who has handled it, how it has been transported and where it is stored. Without this chain, there is a risk that any evidence gathered may be compromised and therefore inadmissible in later proceedings.

The perpetrator(s) of fraud are often unknown at the start of an investigation, and in some cases where there are known suspects it may be that they are not isolated quickly enough to prevent access to potential evidence, with the risk it is destroyed or contaminated. It is vital the investigation team identify any routes by which evidence may be lost. For example, it is common for employees to have access to the organisation's IT networks from home or via portable devices, and often this is overlooked when restrictions are put in place.

Electronic data has become a vital source of evidence, so it is necessary to look beyond hard-copy documents and information stored on the computers of suspects and witnesses. Other sources of data often overlooked include external drives, mobiles and data backups. An experienced forensic technology expert will be required to assist with data collection, analysis and, in some cases, recovery of deleted data.

Where evidence could be located in a number of locations, it may be important that the investigator does not provide notice of site visits and, where possible, has team members attending all sites concurrently to limit the opportunities for tipping off, amending or destroying documents. In addition, valuable information such as creation and modification dates and the identities of the users are stored within the metadata of electronic files, and these can be lost if forensic images of hard drives are not taken before the files are reviewed.

Interviews, of course, are also a valuable source of information. Whenever possible, employees who are likely to have knowledge of the matter under review should be spoken to before the suspects themselves are interviewed.

The aftermath of the investigation

At the end of the investigation, it is important to reflect not only on the consequences of the findings for the perpetrator, but also on how the organisation can take steps to ensure the crime or malpractice doesn't happen again.

While companies may prefer to keep the investigation and its findings confidential, this may provide the wrong message to would-be future criminals as no obvious deterrent is put in place. Communication of the investigation – its findings and the consequences for the perpetrator – across the organisation acts as a strong disincentive to crime.

Remediation steps may be required to amend, tighten or create financial controls where weaknesses have been identified during the investigation. Fraudsters will try to seek out deficient procedures and weak controls, so regular reviews are good practice. It may also be necessary to roll out training to remind employees of the organisation's policies and procedures, including any whistleblowing regime.

company updated as the investigation progresses so that disciplinary actions, policy changes or modifications to the scope of the investigation can be carried out if necessary.

Management of the budget also depends on regular communication with the company. The investigation, not to mention the client relationship, will almost certainly break down if the budget has been expended before the investigation is complete.

Careful preservation and collection of company documents

A thorough review of the company's documents, including electronically stored data and emails, is crucial to the lawyer's ability to understand the conduct at issue. In addition, documentary evidence, whether helpful or damaging, can be particularly persuasive with the enforcement authorities. A successful internal investigation therefore depends on the careful preservation, collection and review of the company's documents.

At the outset of the investigation, lawyers should send a document-preservation notice, sometimes referred to as a 'legal hold' in the US, to sources of potentially relevant material within the company. In the US, an entity is obligated to preserve relevant information when it reasonably anticipates that litigation or an investigation is probable. Although there is generally no such obligation in the UK, or in many other countries, a timely preservation notice is nonetheless important to prevent the inadvertent destruction of relevant documents and will be helpful in preventing or defending against any later claims of spoliation or obstruction. The notice should inform employees of the substance of the investigation only to the extent necessary, and instruct them to retain and preserve all relevant documents and electronically stored information. The notice should describe the relevant material in a manner sufficient to ensure compliance.

Large-scale preservation and collection efforts can significantly disrupt a company's normal operations by taking employees away from their duties and straining IT capabilities. Lawyers should therefore work closely with the company to understand the relevant sources and where documents are located. For example, with the company's input, lawyers might avoid wasting time sifting through irrelevant documents by searching only the files of designated custodians. They might also determine that search terms can be used to target relevant electronic documents. If a government investigation is open at the time of the internal investigation, however, lawyers should consult the authorities (after getting a sign-off from the company) about the use of search terms or custodians to avoid any subsequent complaints that the company's methods were insufficient.

Timely interviews with employees

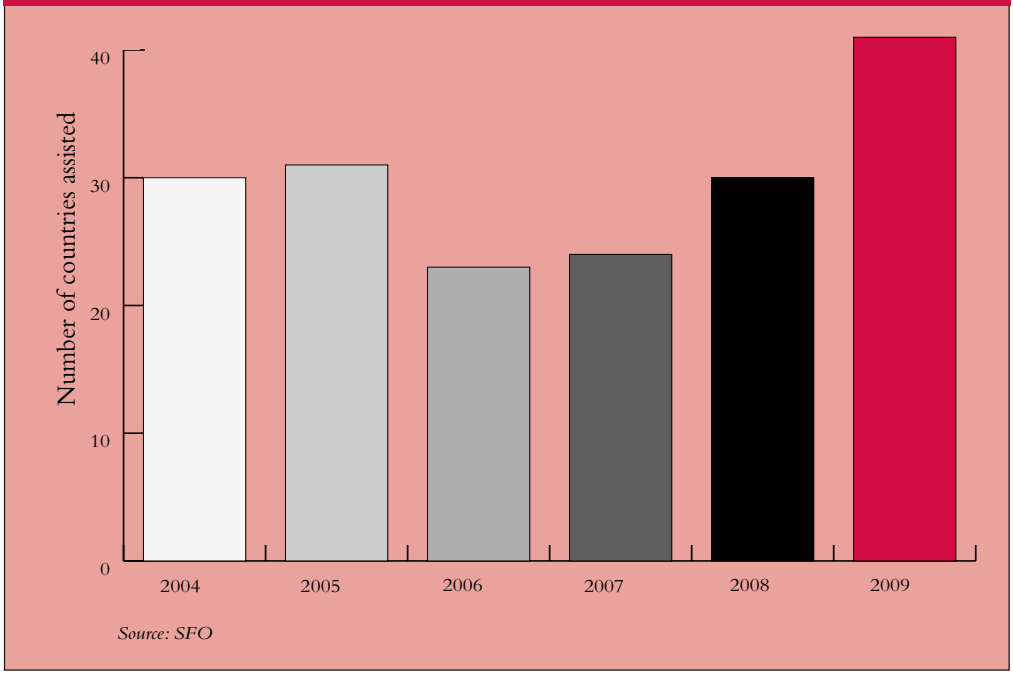
Timely interviews of all employees who may be familiar with the relevant facts are essential to understanding the company's conduct. Generally, lawyers should start with more peripheral or lower-level employees and move up the ladder, so that by the time they get to the most central figures, they have a good knowledge of the company and the relevant issues. Careful consideration needs to be given to the decision on whether to interview former employees. These people will often fall outside the scope of attorney-client privilege, and neither the company nor investigating lawyers can control what third parties will do with information they learn through the interview.

When interviewing witnesses, lawyers must take care to maintain the integrity of the fact-finding process. Lawyers should avoid telling witnesses what other witnesses have said. Use of documents during interviews can be helpful, to learn more about those documents or to refresh a witness's recollection, but the lawyers will need to make a tactical decision about whether to show documents to a witness before the interview. The lawyers may want to test a witness's memory or to avoid tipping a witness as to peripheral issues that may be referenced in a document.

In some instances, selected employees will have to be interviewed at the outset, prior to the completion of document review, so that lawyers can begin to understand the issues and properly frame the document collection. In addition, if, because of the nature of the conduct at issue, lawyers knows that an employee will need to be disciplined or fired, that employee should be interviewed immediately with the assumption that the lawyers will not get a second interview.

Regardless of when or how many times an

UK Serious Fraud Office: cross-border co-operation



employee is interviewed, lawyers should advise at the beginning of each meeting that the lawyers represent the company, not the employee, and that the attorney-client privilege therefore belongs to the company, to be waived at the company's discretion. Lawyers should explain that the company has discretion to disclose the substance of the interview to third parties, including enforcement and regulatory authorities, but that the employee is expected to keep the interview confidential.

These warnings, commonly referred to as the 'Upjohn warnings', for the US Supreme Court decision holding that the privilege belongs to the company, not the individual employee, reflect concern that the employee might mistakenly believe that he or she is represented by the investigating lawyers.[2]

In certain jurisdictions, standards of ethical conduct may further require lawyers to advise employees with criminal exposure that those employees need individual representation. If the *Upjohn* warnings are not given, a US court might later find that the attorney-client privilege belongs to the employee interviewed rather than the company, and that the employee, not the company, can control whether his or her statements will be disclosed.

Do not fall foul of data protection and privacy laws

The collection and review of documents, as well as witness interviews, are all the more complicated in the context of a cross-border investigation. In addition to the obvious problems created by cultural and language barriers, local data protection and privacy laws can place restrictions on employee interviews and the exportation of employee data to third parties. For example, the EU generally restricts the transfer of employee

data, even intra-company, to any country that does not have adequate data protection. Outside of certain protocols discussed below, the US is not included among the countries that the EU deems to provide adequate protection. Labour and privacy laws in some countries include even greater restrictions, allowing employees to refuse to submit to interviews with investigating attorneys, or entitling employees to be represented by their own attorneys during the interview.

Data protection and privacy laws vary from country to country, but generally can carry significant fines, as well as potential civil and criminal liability, if violated. Lawyers therefore need to understand local laws at the outset of an investigation.

In many instances, data transfer restrictions can be overcome by meeting certain requirements. The US and the member states of the EU, for example, have negotiated a set of protocols that must be followed in order to export personal data from the EU to the US. In addition, the UK Data Protection Act generally allows transfer where it is necessary, (a) in connection with any legal proceedings (including future proceedings not yet under way), (b) to get legal advice, or (c) to establish, exercise or defend legal rights.

Although there are exceptions to restrictions, lawyers should engage in a detailed review of local laws before collecting documents or interviewing witnesses. In order to avoid violating data protection and privacy laws, it is advisable for investigating lawyers to hire local lawyers to assist with the analysis.

Preserve privilege and work product protection

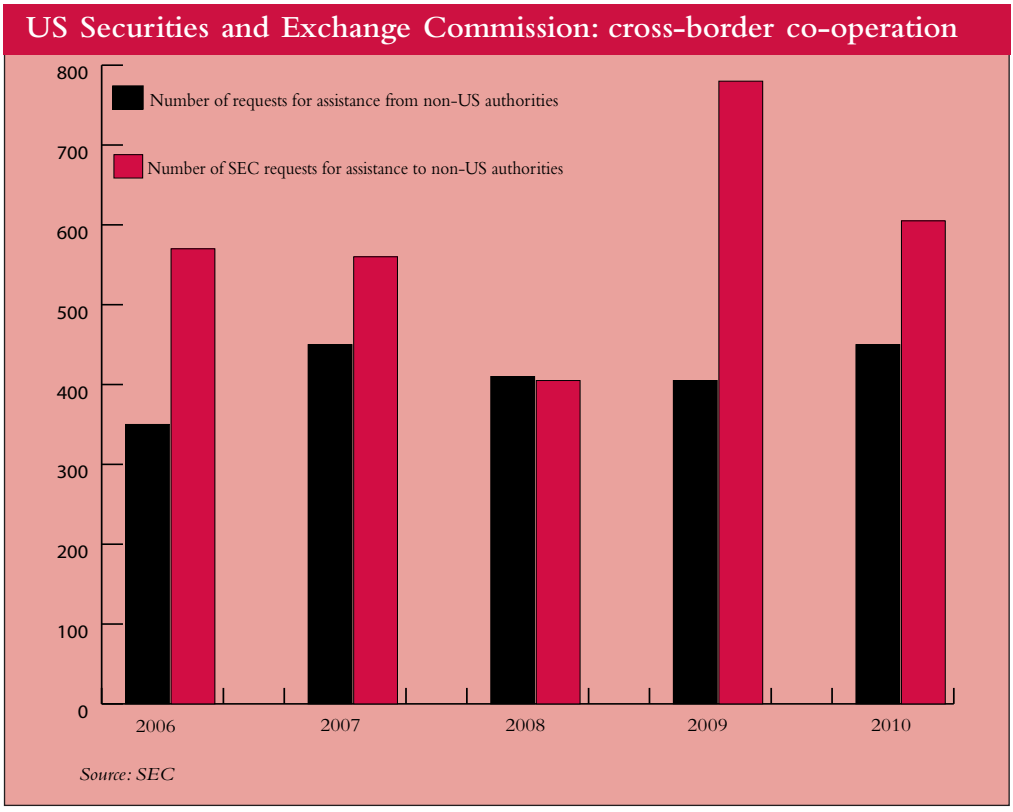
In order to maintain the confidential nature of an internal investigation, lawyers must vigorously preserve attorney-client privileges from the outset. Without the protection of attorney-client and work-product privileges, investigation materials may have to be produced in response to government subpoenas or requests from civil litigants. In the context of a cross-border investigation, maintaining privilege can prove difficult. While attorney privileges in the US and UK are relatively broad, most other countries have a much narrower view, and practices vary by country. A detailed survey of international privilege law is beyond the scope of this chapter, but suffice it to say that when conducting a cross-border investigation, lawyers must have an understanding of privilege rules in all relevant jurisdictions.

In the US, communications with attorneys for the purpose of giving or receiving legal advice are protected from compelled disclosure. In addition, attorneys' work product – their mental impressions and legal analyses – is protected if created 'in anticipation of litigation'. The standard is generally met where an internal investigation is initiated in response to the perceived threat of a government action. Because the US affords such broad protection to attorney work product, lawyers should be careful to attempt to maintain that protection, even when creating documents outside of the US.

Although no action guarantees protection from disclosure, certain measures provide evidence of privilege to any US court making a post hoc evaluation.

For example, all communications with lawyers, as well as all documents created by lawyers, should clearly be marked 'Privileged & Confidential Attorney-Client Communications'. Every interview should begin with the *Upjohn* warnings discussed above, and employees should be regularly reminded of the confidential nature of the investigation.

Employees should be instructed not to create any additional documents, including emails, related to the investigation, and certainly not to destroy or delete any evidence or emails. When creating memoranda or interview summaries, lawyers should include legal analysis, rather than a mere recitation of facts, in order to enable a valid claim of work-product protection. Where applicable, attorney-created documents should include a paragraph that clearly states that the material includes the opinions of attorneys and was drafted in anticipation of litigation.



Companies facing cross-border investigations must be aware that when documents are disclosed outside of the US, including the UK, those documents may no longer be considered confidential in the US and, therefore, may lose the protection of the attorney-client privilege in the US. Although this consequence may be unavoidable, lawyers nonetheless should take the protective steps discussed above, regardless of the jurisdiction, and should vigorously assert the privilege in the face of document requests by any authority.

Such measures may be used to persuade a US court that the confidential nature of the communications was not intended to be compromised and that the privilege should remain intact.

What to do with the results of the investigation

Consider the risks and benefits of creating a written report

The obvious downside of a written report is that it contains a record of potential misconduct that could severely damage the company if leaked. In addition, if a written report is shared with a third party, a court might find that the company has waived any privilege and could compel disclosure of the report to other third parties or enforcement authorities. To protect the confidentiality of the results, the client may choose to receive an oral briefing or a limited written report that provides only a broad summary of the investigation.

Lawyers and the company, however, should carefully consider a decision not to create a

complete written report of the investigation. Should misconduct eventually be disclosed, the failure to create a written report may be perceived as an attempt to minimise or conceal misconduct. Moreover, given the complexity of most investigations and the volume of material that must be summarised, a detailed written report might be necessary to properly inform the company of the results and allow for adequate consideration and remediation. If a report is written, concerns for maintaining privilege protection should guide who will have access to it internally. Generally, any disclosure to a third party, including shareholders, will probably waive the privilege protection, and lawyers should consider privilege laws in all relevant jurisdictions before distributing the report internally.

How much detail to include in the report will depend on the specifics of the investigation, but care should be taken to provide a thorough and balanced approach, especially if public disclosure or disclosure to an enforcement or regulatory authority is possible. After taking so much effort to conduct an independent and objective investigation, lawyers should not risk credibility by creating a report that omits details or could be seen as biased or misleading. The report should note if key witnesses were not available or if sufficient evidence could not be found to support a conclusion one way or another. Contradictory evidence should also be noted, as should questions of credibility of witnesses or accuracy of evidence.

Self-reporting to authorities to lessen criminal exposure

When unlawful conduct has been uncovered, the company must make a determination as to whether the wrongdoing should be disclosed to the authorities. There are pros and cons to self-disclosure. As mentioned above, if the investigation report is disclosed, any privilege that is otherwise attached will be waived. A company may try to obtain a confidentiality agreement before disclosing the report to an enforcement authority, but courts are loath to protect a document once it has been distributed to any third party, including the government.

The other obvious negative impact of voluntary disclosure is that it alerts the enforcement authorities, and possibly the public, to wrongdoing that otherwise might not have been exposed. Disclosure could result in criminal prosecution, civil liability and damage to business.

Notwithstanding the potential risks, it is widely believed that a timely and thorough internal investigation can reduce criminal exposure if the investigation leads to appropriate remedial actions. Although it is unclear what credit a company actually receives in terms of whether misconduct is charged criminally or of determining the extent of punishment, guidance provided by authorities in both the US and UK indicates that companies are encouraged to investigate, remedy and report any unlawful conduct that they uncover.

For example, in the context of overseas corruption, the Serious Fraud Office (SFO) has stated that the prospect of a criminal investigation is greater where the company "was aware of the problem and had decided not to self report". The SFO instructs its lawyers that a company's "failure to report wrongdoing within reasonable time of the offending coming to light" and failure to "report properly and fully the true extent of the wrongdoing" weigh in favour of prosecution.

Guidance in the US is somewhat analogous. The Department of Justice (DOJ) provides that "the corporation's timely and voluntary disclosure of wrongdoing" will be a factor in determining whether to bring criminal charges.

This guidance underscores the need for companies to engage in a thorough internal investigation if they learn of possible misconduct. In addition, lawyers should assume from the outset that disclosure of wrongdoing to enforcement authorities is a strong possibility.

The case for co-ordinated disclosure

Government enforcement authorities around the world, particularly among industrialised nations,

increasingly co-operate with each other and share evidence for use in cross-border investigations. In the US, for example, mutual legal assistance treaties with over 60 countries, including the member states of the EU, facilitate co-operation in enforcement efforts.

Through these treaties, other countries provide the US with evidence for use in US investigations and proceedings, and vice-versa. Similarly, the US Securities and Exchange Commission (SEC) has memoranda of understandings with its counterparts all over the globe, providing for sharing of evidence and co-operation.

Given all this, a company that decides to disclose misconduct to one authority must be prepared to do so to all relevant authorities. Further, failure to self-report upon the opening of one investigation may lead enforcement authorities to assume that the company is not properly co-operating or has not adequately remedied the misconduct. The SFO, for example, has stated that it "expects to be notified [of misconduct] at the same time as the Department of Justice" and that if it learns of wrongdoing from "another agency in the UK or elsewhere", it will "assume … that the corporate has chosen not to self report". Credit for disclosure in one jurisdiction may prove pyrrhic if the company is discredited for not having disclosed misconduct in other relevant jurisdictions.

Disclosure to all relevant authorities may be a preferred course for the company because it allows for a co-ordinated settlement. Without this global co-ordination, the company may be forced to conduct separate investigations or separate settlement talks. A piecemeal approach could result in increased costs and individual penalties that result in a greater aggregate amount.

Lawyers and the company, however, should carefully consider the implications of disclosure in each of the contemplated jurisdictions before self-reporting misconduct to any authority.

26

E-discovery and serious economic crime: a European approach to the e-discovery model

Greg Mason, Partner, and Frances McLeod, Partner Forensic Risk Alliance

E-discovery. The term chills the heart of the most experienced corporate lawyer. The sheer volume of data to identify, preserve, collect, process, search and analyse triggers alarm bells about high costs and logistical struggles – before the data is even used to establish fact patterns or formulate a defence. And in the context of cross-border serious economic crime (be it a regulatory action, internal investigation or follow-on civil litigation), this is just the first threshold of challenges.

Still to be grappled with are several European and US legal hurdles: European blocking statutes and data privacy and secrecy laws, privilege law that varies from country to country, and the hard logistics of managing terabytes of data without inadvertently transferring it across jurisdictions or to the 'wrong' party.

US e-discovery

As a way of background, under a patchwork of US criminal and securities laws, as well as civil discovery rules, there is an obligation to preserve paper and electronic documents. Under the discovery rules applying to civil, as opposed to criminal, litigation, the established – if subjective – standard is that once a party 'reasonably anticipates' litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold'[1] to ensure the preservation of relevant documents in existence and under its control. A party or anticipated party must retain all relevant documents in existence at the time the duty to preserve attaches, and any other relevant documents created thereafter. This preservation requirement is constant throughout the litigation process and failure to adhere to it can result in serious sanctions.

Despite these obligations and despite a company's best efforts, it is sometimes the case that information is lost, damaged or destroyed either intentionally or accidentally. Spoliation of evidence is the intentional or negligent withholding, hiding, altering or destroying of evidence relevant to a legal proceeding. Technology has increasingly complicated spoliation issues. Digital data disappears all too quickly and easily. A company found to have spoliated evidence can face severe sanctions, such as adverse inferences, summary judgment, and having to pay an opponent's attorneys' fees (which, under US rules regarding fee shifting, is a very rare event).

Similarly, under a variety of criminal and securities laws (including those put in place by the Sarbanes-Oxley law passed after the fall of Enron and

prosecution of Arthur Andersen), companies or persons must preserve paper and electronic data upon notice of an investigation or a 'contemplated' investigation – essentially meaning such holds should be put in place at the initial detection of potential wrongdoing. Failure to do so can result in, among other things, prosecution for obstruction of justice.

Regardless of the potential criminal sanctions, destruction of data is viewed dimly by all enforcement agencies, and even if criminal actions are not brought, lost or destroyed evidence will often cause enforcement agencies to redouble their investigation into a company and create scepticism of the company's motives and honesty in the investigative process.

Context: e-discovery's relevance beyond the US

European companies and their legal advisers need to recognise that with continued aggressive enforcement activity from US authorities in the area of serious economic crime – under the Foreign Corrupt Practices Act (FCPA) and anti-trust and financial fraud laws etc – and with the equally aggressive plaintiffs' bar, there is frequently a US angle to international e-discovery.

Due to possible US proceedings – from criminal prosecutions to civil actions for money damages – an effective litigation hold must be implemented and enforced, often in cultures and systems where such a thing may be unknown, so as to avoid data destruction and potential spoliation. There are also practical reasons for ensuring preservation. For example, a raid by an enforcement agency is a scenario that removes the control inherent in a typical e-discovery exercise, and requires the reverse engineering of what has been seized and why, before the universe of data can be assessed and analysed.

If a company puts in place a US-style preservation order when first alerted to possible malfeasance, then it can be confident knowing it has what the raiding authority has taken into its possession. The company has not lost pieces of information that may be relevant or necessary for responding to the raiding authority at a later date. This reverse engineering exercise – essentially mirroring what the raiding authority has seized – protects the company because it is taking proper steps to gather all of the data that is in the hands of the raiding authority. As a result, it will not be running the risk of not knowing or having access to what the raiding authority has. If a smoking gun exists, the company will know just as much as the raiding authority.

European (and possibly other) data protection issues need to be respected. A single mis-step can have serious ramifications for a client: a breach of data protection laws in many countries carries with it criminal sanctions and heavy fines, while the inadvertent transfer of documentation into another jurisdiction may expand the scope of an investigation, driving the risks and costs ever higher.

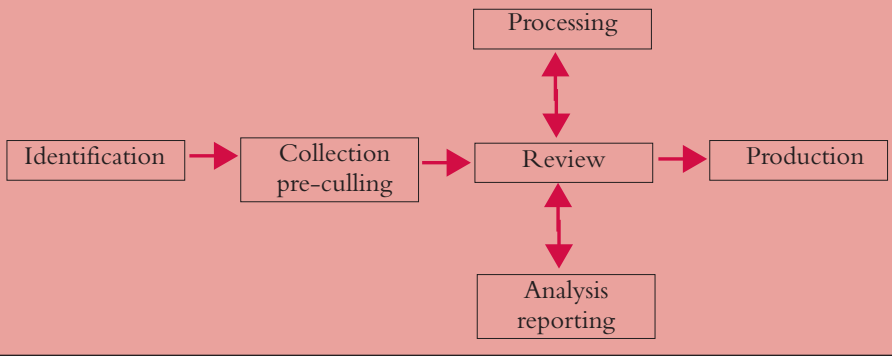
In short, there is a clear case for developing an international e-discovery model drawing on some of the processes established in the US market, where the approach is more established and defined, and calibrating them to the legal system and issues at hand. This would not only enhance the system, but help to properly and efficiently respond to multi-jurisdictional litigation. There may be a particular benefit to applying e-discovery technology in European markets where law firms are typically smaller and more resource-constrained than their US counterparts, where disclosure is much narrower or non-existent, and where it is necessary to consider jurisdiction-specific legal issues such as data protection.

Developing an international model

We would argue that a well-run UK or European e-discovery exercise will have drawn on the lessons learnt by non US-based companies that have gone through an investigation with a US connection, either because of inter-agency co-operation or US litigiousness in general. Many of the 'dos' and 'don'ts' of e-discovery have been borne out of these experiences.

E-discovery processes and legal rules have had decades in which to mature in the US. Much of

The steps to electronic discovery



the current technology, and the well-established protocols, were developed there. Applied in a nuanced manner in a European context, e-discovery can add real value to the exercise of identifying and analysing data that may be required as part of compliance with a serious crime investigation and the formulation of defences.

An example of such a process is the application of the litigation hold, which involves making sure the hold notice is clearly and comprehensively drafted, effectively disseminated to all concerned parties, fully understood (organisations should consider translation into native languages if necessary) and adhered to. It is our experience that practices created in response to US requirements may be tailored as needed in other jurisdictions.

Identifying relevant data

Efficient identification of potentially relevant data is critical to a cost-effective and successful e-discovery exercise, particularly when the stakes are as high. Too frequently, the potentially overly inclusive US model is used and custodians (data owners) identified before the nature of the business and its activities, practices and protocols are fully understood. This approach can lead to unnecessarily large volumes of data being processed, without necessarily increasing the amount of relevant data. Taking time at the beginning to identify the most relevant custodians and the location of their data can save time and money and increase the usefulness of the information collected.

Often, in complex matters related to corruption, fraud or money laundering, identifying all the potentially relevant parties may be difficult. However, instituting a data 'lock down' at the outset means that not only is a wide pool of information secured, but it will also be possible to start narrowing down the field – eliminating file types that aren't useful, duplicated information or low-yielding data – so the most relevant data is isolated. The application of software search mechanisms can also be considered to allow for the pre-culling of certain data sets.

Critically, early identification of sources can speed up the analysis of information and allow for the development of leads. For example, in the process of reviewing financial data – which will need to be extracted from the relevant accounting systems and analysed by running algorithms to identify potentially high-risk or anomalous transactions – potentially relevant payees (vendors, customers etc) and custodians may be revealed. This will also have the benefit of supplementing the search term list, which can be used to identify further relevant information on the issue.

Key 'dos' and 'don'ts'

The best practice for electronic discovery is adhering to the protocol prescribed in the Electronic

Discovery Reference Model (EDRM). This sets out a comprehensive and structured method for analysing and identifying relevant data for an investigation. The diagram on the opposite page sets out the general steps that are involved. When responding to requests for data and documentation in a serious economic crime, we recommend taking the following points into consideration:

- It is important to have a thorough understanding of the litigation hold and what is required to comply for US-based matters or matters that potentially have a US connection. Failure to comply and lock down data can result in spoliation issues, which can in turn lead to hefty sanctions.
- The scope of the investigation should be refined and focused as quickly as possible. In jurisdictions outside the US, there is generally a more refined approach to disclosure, so avoid being overly inclusive in the data collection and ending up with a 'needle in a haystack' when it comes to reviewing documents for relevant information. Very helpful in this context are intelligent software solutions that can be used to organise a collection of documents according to a 'relevance score'. This score is computed by the software based on initial input from an experienced reviewer, using statistical and self-learning techniques to rank documents for their importance so they can be prioritised for review.
- Companies need to recognise jurisdictional hurdles and data protection laws and requirements in foreign countries and take the necessary steps to avoid inadvertent transfer, such as limiting access to data reviewers in the jurisdiction of origin of the data. For example, with the French Blocking Statute – which simply put prohibits the removal of French data from the country to be used in foreign litigation – if the review platform is web-based, only allow reviewers in France to log into French data located on a French server.
- Assess the potential for conflicts of law. Develop a solution that avoids compliance with a US subpoena, for example, if there is a risk of violating EU data protection law.
- Do not allow the tail to wag the dog. Understand from the beginning that the e-discovery exercise should serve to inform the legal and forensic accounting exercise, not the other way around.

Sample search term report

Description	Total records	Non duplicates
All data	**28,140,320**	**12,616,155**
By search term		
brib*		10,923
cash		328,483
commission		125,428
corrupt*		24,031
entertain*		55,780
FCPA		1,789
fictitious		2,390
grease		52,083
hide		39,557
illegal*		41,203
improper		46,207
incentiv*		99,309
kickback*		3,515
middle m*n		466
off the books		673
off-shore		104,665
off-the-books		673
shell		113,963
suspic*		11,979
unlawful*		26,431

Arriving at effective, efficient filtering criteria

In a world of email communication, payment documentation and complex financial transactions, the ability to identify the documents and the data that tell the story, in a sea of information, is critical.

One mechanism for doing so is the application of search terms. The more time spent at the outset carefully considering and adjusting the terms to be applied to the body of data gathered and

processed, the better. We recommend rigorous testing of the efficiency of the search terms, measuring hit rates, negotiating and agreeing with the other side for the removal of terms that generate too many false positives, or introducing appropriate foreign-language terms or nuanced search strings. (See the sample search term report on the previous page. This shows the total number of records [documents] and a list of search terms, with the hit rate associated with those records.)

The result is a higher proportion of potentially relevant documents and, accordingly, a reduced review time for the lawyers. This may also translate into the ability both to produce documents for the other side promptly and to reduce review costs.

We propose taking the following approach:

- Build up, edit and enhance a list of keywords, drawing on the expertise of the lawyers and forensic accountants. Try not to involve generic phrases; rather, focus on those relevant to the matter at hand. Interviews, ongoing document review and analysis of the financial system will inform the search terms.
- Complete a technical review of each keyword in light of the relevant data against which it must be searched, enhancing the syntax as required to limit 'false positives', expanding as necessary, and noting possible additional keywords of interest.
- Run the keywords in combination and examine the search results in context, ensuring that the rate of false positives is acceptable, and make adjustments as necessary.
- Assign the documents responsive to these search terms to the legal review team to test for relevance, and refine the terms as necessary.
- Consider the use of intelligent text-analysis software (there may be cost constraints) that evaluates the relevance of the entire body of documents and ranks it for review.

Once search terms have been applied, there may still be large volumes of documents for review, which on closer inspection may not yield high ratios of relevant material. There are several potential solutions to this problem:

- Instead of reviewing documents one at a time, the process could be carried out in the context of grouping documents with similar subject matter relevant to the investigation.
- Specific information could be assigned to specialists in that area. For example, financial documents could be read by financial reviewers, and French documents by French speakers.
- The review process could be refined by collaborating with financial analysts.
- While software solutions may not remove the requirement to review all documents – there may be a need to certify the thoroughness of the review with a court in the US or the US Department of Justice, for example – the use of software can assist in getting to the heart of the matter more quickly.
- The need to review successive highly similar documents can be limited if decisions are allowed to be inherited from the original review (note that, depending on the venue of the issue, there are risks associated with taking this approach). It is also important to measure current decisions against previous decisions to ensure consistency.

Clearly it is important to maintain a full audit trail, not only of the processing, culling and relevance testing, but also of review determinations throughout the exercise. This allows the client and the lawyers to defend the approach taken if required.

Legal challenges

Data protection

Serious economic crime frequently involves the movement of funds across borders and the involvement of individuals and corporate entities

in multiple jurisdictions. Where this is the case, jurisdictional considerations concerning data protection[2], banking secrecy (which is a protection whereby a bank is restricted from disclosing personal and account information about their customers unless certain conditions are met)[3], commercial secrecy (such as Swiss law prohibiting the search for manufacturing or trade secrets in order to make them available to a foreign court or governmental agency)[4], blocking statutes (such as the French Blocking Statute which prohibits (a) most business-related communications, if harmful to France, to foreign public authorities by persons having a presence in France, and (b) the gathering in France of business-related information to be used in foreign litigation)[5], employee rights and sovereignty issues need to be addressed when the investigative strategy is being developed; severe penalties may be imposed should these considerations be ignored. For example, the simple act of transmitting data across a border can result in the breach of existing protections, with subsequent criminal penalties or civil fines.

Whether and how data can be produced across jurisdictions should be determined by experienced local and lead lawyers in consultation with e-discovery advisers on a jurisdiction-by-jurisdiction basis. The mechanism agreed – for example, a mutual legal assistance treaty (MLAT) under the Hague Convention[6] – will still need to be structured in a practical and compliant manner. It may be necessary to get feedback and input from European Privacy Commissioners, and to take into consideration internal communications within the company.

Where rights associated with data protection are concerned, it may also be necessary to involve the company's data protection officer/privacy officer and/or representatives of the workforce. Our experience shows that an EU-sensitive approach should be taken to data collection – offering, where possible, explanations and assurances to custodians to avoid possible hold-ups and associated cost increases.

In general, we recommend the following practical and effective approach:

- If a sub-set of data is to be transmitted outside the jurisdiction, the mechanism for doing so, and what is involved, needs to be agreed with input from the lawyer and competent authorities.
- Where possible, robust advice should be sought from local lawyers with expertise in data protection, commercial secrecy, banking secrecy and other potentially relevant laws.
- Any issues surrounding data movement should be communicated to the other side, whether it is a regulator, opposing lawyers etc.
- Where data protection is an issue, written consents need to be obtained from employees, who may need to be given the opportunity to identify 'personal' information prior to processing. These consents need to be jurisdiction-specific as laws vary from country to country. In France, for example, we have found it effective to allow custodians to create 'private folders' on their laptops prior to collection; that way, personal data can easily be excluded from processing. Further, certain file types can be excluded automatically from processing, such as music and photographs.
- Depending on the jurisdiction, the company's internal data protection officer/privacy officer, if one exists, should be involved. Under certain circumstances, it may also be advisable to obtain guidance from the authority – for example, the Privacy Commissioner where personal data is involved in an EU jurisdiction, or the State Secretariat for Economic Affairs (SECO) in Switzerland if commercially sensitive data is involved.
- Data should be processed and culled on dedicated servers in the country of origin and stored on those servers[7]. All data must be collected in such a way that a clear audit trail exists from the point of collection, through to review and production, with a clear chain of custody being documented and tracked. This is

critical in establishing the provenance and integrity of the data, should it be required, as well as certification for regulators and courts if necessary.

- We advise that the review be conducted in the country of origin. This ensures that only potentially relevant data leaves its jurisdiction via the means agreed and in a compliant fashion. Equally, it avoids inadvertent transmission to another jurisdiction, which could have serious strategic ramifications. We do not recommend viewing data over the internet from another jurisdiction. For example, there may be a risk in reviewing information remotely from the US; the definition of data 'processing' has not been sufficiently tested in many EU jurisdictions and the 'processors' may find themselves in violation of data protection laws by viewing the data. Equally, US authorities may deem that the data has been transmitted into the US just by virtue of being viewed, and therefore it can be 'discovered'.
- If the investigation 'joins up' across jurisdictions or as the result of inter-agency co-operation, creating a data room to allow for the sharing of work product between the lawyers, advisers and company can ensure the data continues to reside where it should, while allowing for multiple bodies to have access to relevant materials on a controlled basis. In our experience, source documentation may be shared depending on what production protocol has been established, but the rule of thumb is to maintain control and/or access to that documentation within its jurisdiction of origin.

Privilege

There are significant differences in privilege protections in the US, UK and Europe. For example, in the US an email and its attachments may be withheld in their entirety if one of the elements is privileged, whereas in the UK the non-privileged elements would be disclosed.

Legal privilege is one of the most important considerations in e-discovery, requiring significant effort to ensure that all privileged data is properly withheld and secured. Privilege asserted on certain documents must be carefully defined according to the rules in the jurisdiction(s) in question, and the e-discovery processes and controls must be set accordingly. The protocols should pay particular attention to flagging and resolving possible conflicts prior to disclosure, to ensure that privilege is not inadvertently waived. Maintaining a complete and automated audit trail is critical both for negotiations with the other side, and in order to ensure that where multi-jurisdictional matters are concerned, there is protection against failing to assert privilege in one jurisdiction, where it may be possible to do so in another.[8]

Finally, the client could consider having its external lawyer engage other advisers such as forensic accountants and e-discovery experts so as to be able to assert work product-related privilege in US matters, or where there is a risk that a US body or claimants' firm seeks to assert US jurisdiction.

The risk of follow-on litigation or investigation

In recent years there has been a marked increase in follow-on investigations and civil litigation in the context of serious economic crime. This has been the case in the anti-corruption arena (the United Nations oil-for-food programme, for example), as well as in serious financial fraud (such as Bernard Madoff) and anti-trust (air cargo) matters.

Developing a far-sighted e-discovery strategy that takes into consideration risks beyond the immediate matter can help mitigate the risk of follow-on actions. A sophisticated team composed of lawyers, forensic accountants and e-discovery advisers should be able to develop a strategy that, to the greatest extent possible, controls the information flow across borders or from the criminal to the civil arena.

The challenges of a raid

It is an unfortunate but increasingly common reality that enforcement efforts associated with

serious economic crime and related investigations may start with a raid in which data and documents are seized. This in itself presents a distinct set of challenges – first, because control over the data (and the strategic benefit it can provide) has been lost; second, because the targeting and seizing of data may be the result of guesswork by the enforcement agency; and third, because the exercise will, by definition, involve 'reverse engineering' the data.

At least for a time, the targeted company and its advisers will be on the back foot while they try to work out exactly what has been taken and why. The e-discovery advisers will be critical in helping to formulate a strategy, which will need to take into consideration the following:

- Ultimately, the company and its advisers may have to work on the assumption that all raided data will be reviewed by the raiding entity. An effective approach to prioritising the data that poses the highest risk will need to be developed. Here, technology will be critical, as will ascertaining where the richest caches of documents may lie. One advantage to be exploited is that the company will have a better understanding of its own data and custodians.
- The e-discovery advisers must work with the lawyers and the company to review all of the raided data to identify: (a) which material could be relevant to the investigation (so as not to duplicate any further collections in connection either with a parallel internal investigation or subsequent demands for additional data); (b) any 'hot' documents that might be included in the seized data; (c) any information that may not seem relevant but could lead to follow-on litigation or expand the scope of the current investigation; and (d) any privilege issues that may need to be addressed.
- The company and its advisers will also need to take into account how the information has been handled by the raiding agency in case there are any data destruction issues that may need to be addressed and/or defences formulated.

Conclusion

While, given the increasingly global nature of business, e-discovery in cases of serious economic crime will often touch on US requirements, we advocate a measured, nuanced approach that avoids the excesses of the US system. We believe the key is to develop a European strategy suited to the legal system(s) involved, while cherry-picking the latest processes and technologies developed and refined in the US. This allows the respondent and its advisers to identify and process data in a manner better suited to European legal requirements, resources and budgets.

An e-discovery adviser, fully integrated into a team responsible for responding to such complex and challenging regulatory and litigation matters, can make a profound difference to the success of the matter, as well as helping to manage the associated costs.

27

Cross-border co-operation in the investigation of fraud – mutual criminal legal assistance

Chris Colbridge, Partner, Harkiran Hothi, Partner, and Chiraag Shah, Partner
Kirkland & Ellis International LLP

Most complex corruption and money-laundering cases cross national borders – and, increasingly, national prosecution authorities are seeking to investigate and prosecute companies and individuals for fraud committed outside their own countries. The implementation of the Bribery Act 2010 will, no doubt, lead to a greater focus by the Serious Fraud Office (SFO) on acts that are committed beyond the UK.

It is in this context that mutual legal assistance (MLA) in the investigation and prosecution of fraud, particularly money laundering and corruption, is becoming more and more relevant. MLA refers to the way in which countries can co-operate with each other in obtaining evidence in one jurisdiction to assist with a criminal investigation or prosecution in another. Forms of MLA can include the provision of documents and evidence, the summoning and taking of witness testimony, the service of legal documents and the execution of requests for searches and seizures.

A regime of international MLA has developed over time. It is composed of various multilateral and bilateral conventions, treaties, domestic laws and other informal arrangements. While the first European Convention on Mutual Assistance in Criminal Matters was entered into in 1959, the current extensive MLA regime is a relatively recent development and is continuing to take shape. For example, the United Nations Convention Against Corruption (UNCAC) – the MLA convention with the widest potential for application in the investigation of corruption across jurisdictions – only came into force in 2005.

MLA between jurisdictions is necessary since the principle of sovereignty prevents national prosecution authorities from being able to take steps in the investigation of a crime in another territory, without the consent of that jurisdiction. Critical evidence that is required to link a defendant to a fraud is often located abroad; without it, a successful prosecution of a defendant may be impossible.

The use of MLA by prosecuting authorities should be considered when an investigation into a company or an individual is likely to concern cross-border elements and transactions.

Ways in which MLA can be granted

The UK has a relatively open approach to mutual legal assistance. An MLA request does not have to be based on a treaty or formal arrangement; the UK can assist any country whether or not that country is able to assist the UK.

MLA can be granted or requested internationally through a number of channels:

- multilateral conventions, treaties or arrangements
- bilateral treaties or agreements
- domestic legislation, such as the Crime (International Co-operation) Act 2003, which provides for MLA
- informal procedures such as letters rogatory (letters of request).

Any combination of the above can be available for a prosecution authority, and none of these options are mutually exclusive.

Multilateral conventions, treaties or arrangements

A number of multilateral conventions and treaties contain binding rules that oblige the signatories to provide MLA. In addition, the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions also requires that signatories provide MLA to each other to the fullest extent possible under their respective laws. In this regard, there is a complex and often overlapping regime of conventions and treaties applying to the area of MLA.

The conventions that may be the most relevant to the investigation and prosecution of fraud are as follows:

The European Convention on Mutual Legal Assistance in Criminal Matters 1959

This was the first multilateral MLA convention. It has since been supplemented by the Additional Protocol to the European Convention 1978 and the Convention on Mutual Assistance in Criminal Matters between Member States of the European Union 2000, modernising it in line with developments in cross-border co-operation, and strengthening the ability of prosecution authorities to fight fraud.

The UK is a signatory to the European Convention, which requires parties to commit to grant each other the widest measure of MLA in proceedings undertaken by the requesting party. MLA also extends to proceedings before administrative authorities. The forms of assistance envisaged include the provision of documents, summoning of witnesses and the execution of search warrants.

Requests for MLA may be made directly between judicial authorities in different member states, and the European Convention also permits a spontaneous exchange of information (in other words, without prior request) between parties regarding criminal offences the investigation or prosecution of which falls within the competence of the receiving authority.

In cases that concern two or more parties, the European Convention contains provisions for the setting up of a joint investigation team, where relevant, for a specific purpose and for a limited period.

Switzerland has entered into the Co-operation Agreement between the European Community and its member states, which came into force in 2008. This agreement, although stated to be designed to combat fraud at every stage – administrative and criminal prevention, detection, investigation, prosecution and enforcement – is only applicable in very specific cases. The definition of 'illegal activity' does include corruption, however, and it does provide for MLA in respect of banking records.

United Nations Convention Against Corruption

UNCAC is the MLA convention with the widest potential for application in the investigation of corruption across jurisdictions. It has over 140 signatories and aims to overcome legal differences to create a common set of principles through which MLA can be provided. Like the European Convention, it also provides for parties to grant

each other the widest measure of MLA in investigations or prosecutions concerning corruption.

In addition, UNCAC provides that dual criminality shall be deemed to be fulfilled, irrespective of the legal formalities, if conduct constitutes a criminal offence under the laws of both parties. In the absence of dual criminality, UNCAC provides that a party shall, where consistent with the basic concepts of its legal system, render assistance that does not involve coercive action. In effect, UNCAC encourages parties to adopt measures that will enable a wider scope of assistance.

The forms of MLA that can be granted under UNCAC are very broad and range from the supply of evidence to the freezing, tracing, seizure and recovery of the proceeds of crime. In effect, it provides for any form of MLA that is not contrary to the domestic laws of the requested party. MLA requests cannot, however, be refused on the grounds of banking secrecy.

Similar to the European Convention, UNCAC also permits a party to provide information relating to criminal matters to a competent authority in another party's jurisdiction if they believe that such information could assist the authority in undertaking or concluding criminal proceedings.

The procedure for MLA requests under UNCAC is by way of request to central authorities, which are designated for this purpose. In this regard, the UK has a Central Authority that deals with incoming requests.

UNCAC also encourages the establishment of joint investigative bodies for investigations or proceedings that concern one or more parties.

Although both UNCAC and the European Convention provide for extensive international co-operation in the investigation and prosecution of fraud, there is no uniform method of implementation across jurisdictions. The provisions of multilateral treaties and conventions are often drafted in a general manner, given the number of parties involved, meaning that currently it is difficult to predict the level of co-operation.

The Harare Scheme

This is a voluntary scheme for MLA between Commonwealth countries. It provides for assistance by a competent authority in respect of criminal matters arising in another Commonwealth country. The standard forms of MLA can be provided under the Harare Scheme, such as the serving of documents, search and seizure, examination of witnesses, and tracing, seizing and confiscating the proceeds of crime. Requests for MLA are to be made through central authorities. Grounds for refusal include the absence of dual criminality.

Bilateral treaties

There is a wide network of bilateral treaties dealing with MLA. These, much like multilateral treaties, contain binding obligations on the parties, and often the parties to multilateral treaties may also have concluded a bilateral agreement between themselves.

The UK has entered into a number of bilateral MLA treaties over the years as part of a drive to improve co-operation in the cross-border investigation and prosecution of fraud. For example, it recently concluded a treaty with Malaysia and also, unsurprisingly, has a bilateral MLA agreement with the US.

The treaties can be tailored to the requirements of the signatories, so making it more likely that MLA requests will be sought under bilateral agreements, where they exist, rather than multilateral ones.

Domestic legislation

The Crime (International Co-operation) Act 2003

CICA is the UK's main domestic law in this area and provides a streamlined and modernised framework for both making and executing requests for MLA. CICA has a very broad application and enables the UK to assist any country or territory in the world, irrespective of whether it would be able to help the UK – save for certain specific exemptions such as the exercise of search and seizure powers, restraint and confiscation matters,

or requests for banking evidence, all of which are specialised requirements restricted to the parties participating in those agreements. In addition, CICA does not in general require dual criminality, except for MLA requests involving fiscal offences (in the absence of an agreement) or the use of search-and-seizure powers.

Part I of CICA deals with MLA in criminal matters and addresses, inter alia, the mutual service of process, the mutual provision of evidence, search and seizure, the hearing of evidence through television links or by telephone, and requests for information about banking transactions.

Of particular relevance to prosecution and enforcement authorities are the provisions relating to the supply of evidence. Under CICA, UK judicial authorities may request assistance in obtaining evidence outside the UK where an offence has been committed or there are reasonable grounds for suspecting that an offence has been committed, and proceedings have been instituted or the offence is being investigated. Interestingly, it is not just prosecuting authorities that may apply to the judicial authorities but also the person charged with an offence. The same right applies for overseas authorities to request assistance from the UK.

One additional point of significance is that CICA provides for freezing orders to be issued by the UK judicial authorities for the preservation of evidence that is in a foreign jurisdiction pending its transfer to the UK. Such an application may be made where the evidence is likely to be of substantial value to the proceedings or investigation.

Letters rogatory

This is a more traditional form of assistance that may come into play if there is neither an existing treaty between jurisdictions nor domestic legislation in the requested jurisdiction that provides for MLA. Letters rogatory involve the transmission of requests for assistance through diplomatic channels, relying on a promise of reciprocity or comity between the states. Essentially, a formal communication (request) may be made between the judiciary and a prosecuting or law-enforcing authority in one jurisdiction and its counterpart in another jurisdiction. It is a longer process than the other options highlighted above because it involves diplomatic formalities.

With the coming into force of CICA, and the broad-ranging nature of its application to MLA, this process is now of lesser importance from a UK perspective.

The process for MLA requests in the UK

Requesting assistance from overseas

Requests from the UK to a foreign authority may be issued by judicial authorities in England, Wales, Northern Ireland and Scotland (magistrates courts, crown courts and the High Court) and a number of designated prosecution authorities including the Attorney General (for England and Wales and for Northern Ireland), the Director of Public Prosecutions (and any crown prosecutor), the director and other designated members of the SFO, and the Financial Services Authority. Judicial authorities may also issue requests on behalf of the defence once proceedings have been instituted.

All of these authorities are able to send MLA requests directly to member states of the EU without having to go through the UK Central Authority. However, direct transmission is not possible for requests for restraint and/or confiscation, the transfer of a prisoner to appear in court or assist an investigation, requests relating to banking information, or a request where a state's legislation does not allow for it.

Getting assistance from the UK

All requests for MLA from the UK must be addressed to the central authorities appointed by the Home Office. For England and Wales and Northern Ireland, this is the UK Central Authority, and for Scotland it is the International Co-operation Unit, Crown Office. Requests for MLA relating to certain tax matters are sent to the MLA Department at HM Revenue & Customs.

Under CICA, a request for assistance may only

be made by: (a) a court exercising criminal jurisdiction, or a prosecuting authority; (b) any other authority that appears to the UK Central Authority to have the function of making such requests; or (c) the International Criminal Police Organisation or another similar body or person recognised as being competent to make a request of this kind under the Treaty on European Union.

Where an MLA request appears to concern serious or complex fraud, the government may refer it to the director of the SFO. If the director has reasonable grounds to believe that serious or complex fraud is involved in the offence, he or she will arrange to obtain the evidence that he or she considers appropriate.

The government will obtain confirmation from the overseas authority that any statement made by a person in response to a requirement imposed under the SFO's investigatory powers will not be used in evidence against them.

Typically, in the investigation of fraud, the categories of evidence that will be sought from the UK include:

- voluntary witness evidence
- compulsory witness evidence
- search and seizure of evidence
- production orders (for example, for banking information).

If the requesting state's legal system does not require evidence to be taken on oath, the witness or suspect will be asked to consent to an interview. If they refuse to attend an interview voluntarily (and the requesting state decides to send a formal MLA request for the witness to be summonsed before a court), or if evidence is required to be given under oath, the witness or suspect may be summonsed to appear before a nominated court.

Schedule 1 of CICA makes it clear that a person cannot be compelled to give any evidence before a nominated court that he could not be compelled to provide in criminal proceedings in the UK, or in the requesting state if the criminal proceedings are being conducted there. MLA requests for search and seizure require dual criminality and justification by the requesting state as to why they are necessary.

In cases of serious and complex fraud that are referred to the director of the SFO, it will be the SFO, as the executing authority, that applies to the court for the search-and-seizure order. Similarly, MLA requests for the production of specific documents will often be dealt with through applications by the SFO to the relevant court.

MLA requests must be in writing and will be in the form of a letter of request (LOR). This must be on the headed notepaper of the issuing authority, signed by the issuing authority and provided in duplicate. If the LOR is not in English, an English translation must be provided.

When dealing with requests for MLA, the UK Central Authority tends to prioritise what can be considered more serious or urgent requests. These will generally involve serious criminal offences, relating to corruption or wide-scale fraud, where evidence is at risk of being destroyed, the safety of the public is at risk, or a trial is imminent in the foreign jurisdiction.

Additionally, a clear nexus must be established between the facts of the case (or the offence in question) and the evidence requested. A mere statement that the requested material is relevant will not suffice; it must also be shown how it is relevant and how it would advance the case in question. The MLA request needs to be as detailed and informative as possible if prompt and adequate assistance is to be provided.

The information provided by the UK, in response to a formal MLA request, should only be used for the purpose stated in that request. In circumstances where a requesting state wishes to use the information for another purpose or share the evidence with a third country, a new MLA request must be submitted explaining the new purpose and the reasons behind it.

Challenging a request for assistance

The extent to which an MLA request can be challenged is limited. A witness is entitled to

withhold information that is protected by legal privilege. In circumstances where legally privileged information has been taken as part of a search-and-seizure order, it will be for independent counsel to review that information using the same procedure as for the seizure of privileged information for domestic prosecutions. Additionally, where the SFO has seized documents, it is likely that material broader than the MLA request will have been seized. It may be possible to seek to exclude the irrelevant material by engaging with the SFO.

It may also be possible to resist the disclosure of confidential information on the grounds that the individual's human rights have been breached. In *Hafner & Others, R (on the application of) v City of Westminster's Court & Another* (2008), the administrative court considered a challenge to the disclosure of confidential material in the context of the application of Article 8 of the European Convention on Human Rights. It endorsed the point that the fact the correspondence was of a business character did not exclude the protection of Article 8 in respect of both 'private life' and 'correspondence'. The fact that the documents were sought in proceedings in which the claimants were not initially concerned did not exclude the protection of Article 8.

Public authorities that obtain documents by compulsion engage the right to respect for private life and correspondence in respect of each step of their measures – the obtaining, storage and subsequent use of the material.

An individual is entitled to a privilege against self-incrimination when attending interviews under an MLA request. Where witnesses are interviewed by the SFO under Section 2 of the Criminal Justice Act 1987, they are not entitled to rely on the privilege of self-incrimination, but for domestic proceedings the information disclosed cannot be used against the witness. In those circumstances, the SFO obtains confirmation from the overseas authority that any statement made by a person in response to a Section 2 interview will not be used in evidence against them, unless evidence relating to it is adduced or a question relating to it is asked in the proceedings by, or on behalf of, that person.

Conclusion

If the sophisticated MLA regime in place were to be used to its full potential, prosecution authorities could have at their disposal a very powerful tool for the investigation and prosecution of fraud. While there are no reliable statistical sources as to the number of MLA requests made internationally, anecdotal evidence would seem to suggest they are on the rise year on year. According to the Home Office, the UK Central Authority has a current caseload of approximately 5,000 MLA cases, while an OECD review in 2008, 'Mutual Legal Assistance, Extradition and Recovery of Proceeds of Corruption in Asia and the Pacific', reported that the number of MLA requests made by Australia had doubled between 2001-02 and 2005-06.

As the cross-border prosecution of fraud increases, so will the reliance of authorities on the various MLA treaties, conventions and agreements to obtain the evidence needed for prosecution.

28

Forensic accounting and serious economic crime – 'follow the money'

Toby Duthie, Partner, and Frances McLeod, Partner Forensic Risk Alliance

__Bob Woodward__: The story is dry. All we've got are pieces. We can't seem to figure out what the puzzle is supposed to look like …
__Deep Throat__: No, heh, but it's touching. Forget the myths the media's created … The truth is, these are not very bright guys, and things got out of hand.
__Bob Woodward__: Supposedly he's got a lawyer with $25,000 in a brown paper bag.
__Deep Throat__: Follow the money.
__Bob Woodward__: What do you mean? Where?
__Deep Throat__: Oh, I can't tell you that.
__Bob Woodward__: But you could tell me that.
__Deep Throat__: No, I have to do this my way. You tell me what you know, and I'll confirm. I'll keep you in the right direction if I can, but that's all. Just … follow the money.
All The President's Men (1976, Warner Brothers Pictures)

Forensic accounting is central to investigating economic crime. It falls into two broad categories: establishing, assessing and analysing the fact patterns and data of an economic crime; and quantifying the financial and economic consequences of the event. It can be utilised reactively (in response to a regulatory inquiry) or as a preventive measure (in other words, compliance or internal audit functions). Typically, the task involves identifying and establishing the credibility of evidence and, in this context, 'following the money' is often pivotal – dividing real events from conspiracy and innuendo.

In this chapter we look at how forensic accounting is used, what it can do, what it cannot do, and what developments are in the pipeline.

Investigation: the proof is in the financial data

Allegations can be sweeping and amorphous in character at the outset of a financial accounting investigation, but the factual proof of an economic crime is typically found in the financial data and the surrounding documentation. Therefore, a key task is to identify, collect, verify and analyse the financial facts.

The places to look include accounting databases, annual reports, management accounts, bank records, market data, contractual documentation, correspondence and testimony. The nature of serious economic crimes varies – bribery and corruption, investor and market fraud, money laundering, anti-trust violations, procurement fraud – but in all cases the forensic accountant

looks to collate the financial facts and pull together an empirically based story on what actually happened, or did not happen, from the perspective of the financial transactions.

Furthermore, while the law may change significantly from jurisdiction to jurisdiction, the fundamental financial, accounting, business and economic principles remain constant in most cases, subject to local nuance. The way accounting records are compiled and details recorded for individual transactions is typically based on common practices.[1] Bank transfers are cleared in similar ways whether in Switzerland, the UK or Russia. Financial instruments (even complex ones) tend to follow international commercial standards – and, if they do not, red flags are raised.

The forensic accounting process can therefore help to provide a comprehensive factual overview of financial events overall and across borders – for example, how much was paid to whom, over what period and in respect of what, and how was it authorised and accounted for?

Investigation: coping with expanding data and increasingly complex cross-border transactions

Amid the globalisation of the economy and increasingly sophisticated financial structures, the skills and experiences of the forensic accountant have had to broaden beyond pure accounting work to include, for example, IT, banking and capital markets, as well as specific industry sectors.

Cross-border aspects complicate matters in terms of the legal obligations and restrictions, cultural differences and logistics. The forensic accounting team may need to operate in conflicting legal environments, in multiple languages and cultures, and to reconcile and analyse data captured from disparate accounting systems, in different formats and according to varying processes.

These challenges can be exacerbated in cases involving companies that are acquisitive and/or multinational. Accounting systems, in particular, are rarely – indeed, almost never – fully integrated or operated consistently, especially if the investigation stretches back over a number of years. Furthermore, depending on the scope and type of investigation, it may be necessary to mine data from various 'non-accounting' databases, such as the supply chain/procurement, asset management, logistics and payments. Data and personnel mapping is extremely important to ensure evidence is being properly identified, collected and preserved. A clean audit trail is essential, and is greatly enhanced through the proper use of technology to mine today's vast sets of financial data. The upside of increased data volumes is that they should improve the scope and reliability of the analysis.

Often there are legal considerations around the gathering of evidence. Whether it is via electronic data or interviews, local laws relating to blocking statutes, data privacy, employment, bank secrecy etc need to be understood and adhered to. It is also essential to recognise potential legal conflicts as early as possible so that one country's law is not breached to comply with that of another.

Investigation: establishing the reliability of data

Financial data often lies at the heart of an effective response strategy as it can empirically counter or support the credibility of the innuendo and implications contained in documentation and testimony. It is important, depending on the context, to drill down to, and distinguish between, the types and credibility of evidence; just because an accounting system records that a payment was made does not mean that it actually was – bank payments can be returned, journal entries reversed, credit notes issued, off-book transactions made, and so on. The faster the net benefit and associated cash movements can be established, the better. Equally, the more empirical and comprehensive the data (and the audit trail), the more reliable the analysis and findings will be.

These activities assist with the creation of a factually accurate narrative, on which key legal responses can be founded. It is also worth noting that databases can be especially interesting sources of information, as often the users themselves have

limited (or no) ability to delete current or historic information.

It is also important to test, benchmark and 'sanity check' the data universe – to understand and rank the scope, scale and reliability of the data. This can, in part, be done by reconciling data with third-party sources – for example, shipping documentation, bank statements and audited financial records – where available. It may also be sensible to run some statistical analysis on the data by sector, date ranges, geography etc to test the credibility and completeness of the information.

Compliance analysis, pre-emption and remediation

Forensic accounting can also pre-empt crime. Specifically, it can assist in the assessment, testing and enhancement of a company's compliance policies and controls.[2]

The quality, effectiveness and suitability of financial controls – as well as the quality of staff charged with maintaining the controls and actual practice on the ground – is an important assessment run in tandem with the analysis of the financial data.

The nuts-and-bolts review of high-risk transactions identified by a combination of algorithmic queries and best judgement provides a good test as to the extent to which a company's written compliance polices and controls are (a) sufficient and (b) adhered to. These algorithms can also be used to identify transactional samples of high-risk areas. This kind of controls testing can help provide an insight into which departments, offices and individuals were involved in the underlying transactions (from initiation to approval and payment).

Forensic accountants have long assisted companies in overhauling their controls and compliance infrastructures to pre-empt economic crimes, but that role is particularly important now in the context of the UK Bribery Act 2010. The risks are significant under the new legislation and may be based on payments that are unlikely to be material in the context of a company's operation. These will not necessarily be picked up by an internal audit, or the external auditors in their assessments of financial statements.

An adequacy review of a company's policies and internal controls should involve a top-down (industry, country, sector etc) analysis, along with a bottom-up analysis of the financial data, as outlined above. There should also be a review of key account codes, cash usage, procurement policies etc.

Higher-risk areas are typically subject to tighter controls, which can mean that areas where risks are perceived to be lower may be more prone to abuse. It is essential to develop a system of risk mapping that works across the board and for the controls to be adjusted to facilitate easy and efficient testing as part of a company's various audit functions. This can be especially relevant in matters that involve so-called 'books and records' charges – where the key to the prosecution's case is a breakdown in controls rather than an actual transgression – and in matters where the defendant needs to prove a negative, such as "I didn't bribe that person" or "I didn't launder money".

Understanding the operational context is essential in compliance reviews, and will often require and benefit from local- and/or industry-specific knowledge – say, customs practices in Nigeria or capital markets pricing in Austria – and specialist advice either from within the forensic accounting team or from outside experts. Invariably, it will also require that the forensic team establishes a rapport with the company's financial and accounting staff, who often, knowingly or unknowingly, point the way.

Penalties and confiscation

Forensic accountants should always be part of the discussions and calculations relating to penalties and confiscation – the forced surrender by wrong-doers of their illicit gains. Confiscation is also intended as a deterrent to future violations and, implicitly or explicitly, it lies at the heart of most regulatory action.

The forensic accountant's job is to calculate the scale of such gains, taking into account the related economic and financial arguments that may increase or decrease this sum. What a company or individual may or may not have gained from an

economic crime is usually not a straightforward arithmetic calculation; consideration will also need to be given to factors such as the nature of the crime, the period over which the gain was realised, how it was realised, whether costs or related losses could be deducted (and then what type of costs), and the ability to pay. This will become more involved the more complicated the crime and the larger and more complex the corporate defendant.

In certain jurisdictions, such as the United States, disgorgement calculation is a well-trodden, but still somewhat arcane path. For example, sentencing guidelines exist in the US and are seemingly adhered to, but precise calculation methodologies are not published (unlike with judgments, settlement agreements and deferred prosecution agreements) and a great deal of prosecutorial leeway is allowed. The US courts tend not to object to the majority of settlements reached by the Securities and Exchange Commission and the Department of Justice.

Fines and asset recovery in criminal and civil proceedings: recent trends in the UK

In the UK, this area is currently in flux. Forensic accountants are retained typically to play a central role in the calculations that form the basis of:

- **civil recovery orders** (CROs)[3] under Part 5 of the Proceeds of Crime Act 2002 (POCA). These allow a court to order the return of property that is established to be the proceeds of 'unlawful conduct'. Although CROs were first introduced in 2002, they have only been available to the Serious Fraud Office (SFO) since April 2008,[4] opening a door to defence solicitors seeking alternative ways to conclude SFO investigations into companies
- **confiscation orders** under Part 2 of POCA. These are obligatory once a criminal conviction has been made by a judge sitting in a crown court. They are designed to prevent offenders from benefiting from the proceeds of their crime, and achieve this by confiscating an amount equivalent to the 'benefit'. It is normal SFO policy to apply for a confiscation order once a conviction has been secured, unless there are compelling reasons not to do so. The confiscation regime is recognised to be both complex and severe, limiting any judicial discretion that might soften its effects. A confiscation order is limited to the assets still available for confiscation,[5] and here the need for qualified forensic accountants is apparent.

In tension with this new trend towards American-style negotiated settlements was the decision in the 2010 case of *R v Innospec Ltd*, where the UK-headquartered and US-listed chemicals company was accused of bribing officials in Indonesia to prolong the use of lead-based fuel in cars, as wells as of paying kickbacks to the Iraqi government in respect of the United Nations oil-for-food programme. This was the first example of a global settlement in respect of criminal proceedings in both the UK and US. In *Innospec*, the court held that under current procedural rules, the SFO had no authority to enter into agreements with offenders as to the penalty for an offence. The judgment emphasised that sentencing rested with the court and not with the SFO through global settlement agreements or plea bargains.[6]

Similarly, in Southwark Crown Court's December 2010 review of the BAE Systems settlement in a case involving a military radar deal with Tanzania, the plea bargain between BAE and the SFO, concluding a six-year corruption investigation, was attacked as "loosely and perhaps hastily drafted". Handing down a £500,000 fine and £225,000 in costs, Mr Justice Bean said he was "surprised" the prosecutor had given BAE indemnity for all past offences, disclosed or otherwise, as part of the deal.[7]

Given the above, there is, as yet, no legal certainty (or even a balance of probabilities) or economic incentive that might encourage a company to co-operate or self-report with the authorities. In most cases, the corporate body and its shareholders, should they become involved in

economic crime, are not criminal enterprises per se in the same way that a drug dealer is, for example.

From a financial perspective, it makes sense that the benefit derived from any illegal act should be measured in terms of profit (or even incremental profit) rather than total revenue. It would also make sense to allow the prosecutors leeway to broker deals and arrange for discounts to take into account various legal, procedural and economic factors (affordability, debarment, level of co-operation).

As is frequently the case in the US, though more rarely if recently in the UK, the concept of a profit-based confiscation should be the preferred path. In this context, the forensic accountant adds a great deal of value in terms of setting out the various profit scenarios over time and the relevant deductions that should, or should not, be considered. Technical issues dictated by legal argument, such as statute of limitations and jurisdiction, may also feature in the profit calculation.

Conclusion

The key benefit of forensic accounting in the context of economic crime is the capacity to identify, analyse, test and present financial evidence. The more empirical and impartial the analysis, the more reliable the evidence. Globalisation and growing data volumes have introduced a clear need for strong IT skills, as well as an understanding of how to operate across jurisdictions and in various cultures. These tools are valuable in terms of reaction (regulatory responses and litigation), prevention and confiscation, and need to be part of the core forensic service.

We foresee greater cross-border co-operation and information-sharing between the enforcement agencies and a greater desire in many jurisdictions to use an American-style model based on plea agreements, prosecutorial leeway, confiscation of profits, individual prosecutions and whistleblowers. But equally, the disparities between the different penalty regimes make global settlements very challenging from an economic perspective, as well as a legal one. We assume this will have to be addressed in some way or other so that corporate double (triple and more) jeopardy in the context of follow-on investigation and litigation does not become common and result in companies paying out repeatedly to various authorities for the same offence.

We also foresee a growing awareness among companies of their exposure to such risks through their supply chain, joint ventures, and mergers and acquisitions activity. In many sectors, this has already led to the merging of ethical and commercial interests as companies vet themselves and their business partners.

Some companies are starting to adopt a more integrated approach to compliance reviews: rather than periodic reviews and sampling, they are trying to look at all of the data all of the time. They use their IT systems and databases to highlight irregular, high-risk transactions as they are processed, to enable intervention before the transactions can be completed. This has some significant positives:

- **greater coverage of transactions**. For example, it is easier to collect, review and analyse data in large volumes of individual transactions
- **the ability to stop high-risk transactions**, pending further authorisation
- **100 per cent transactional testing**. The ability to review and analyse individual transactions is a core requirement, increasing the scope and scale of the testing and therefore the reliability of the analysis
- **lower review costs** resulting from a standardised and automated process
- **illicit activity** tending to diminish as employees and business partners come to understand that the likelihood of their being able to hide something is diminished.

However, experienced forensic advisers look set to remain highly valuable. Even large companies are unlikely to have sufficient experience of economic crime, and regulatory enforcement actions, to equip them with the comprehensive knowledge gained by a forensic adviser through repeated exposure to such situations.

PART IV

Special focus

29

The Bribery Act and its implications for non-UK companies listed on the London Stock Exchange

Satindar Dogra, Partner, Jane Larner, Managing Associate, and Christopher Kerrigan, Associate Linklaters LLP

The Bribery Act 2010 captures non-UK companies involved in bribery in the UK, while any UK nationals working for a non-UK company will be personally caught for bribery anywhere in the world. Beyond those simple headline facts, however, the tentacles of Section 7 of the Act will reach out to ensnare non-UK companies or partnerships that fail to prevent bribery for their benefit by 'associated persons', if those companies or partnerships carry on business of some sort in the UK (see the diagram opposite).

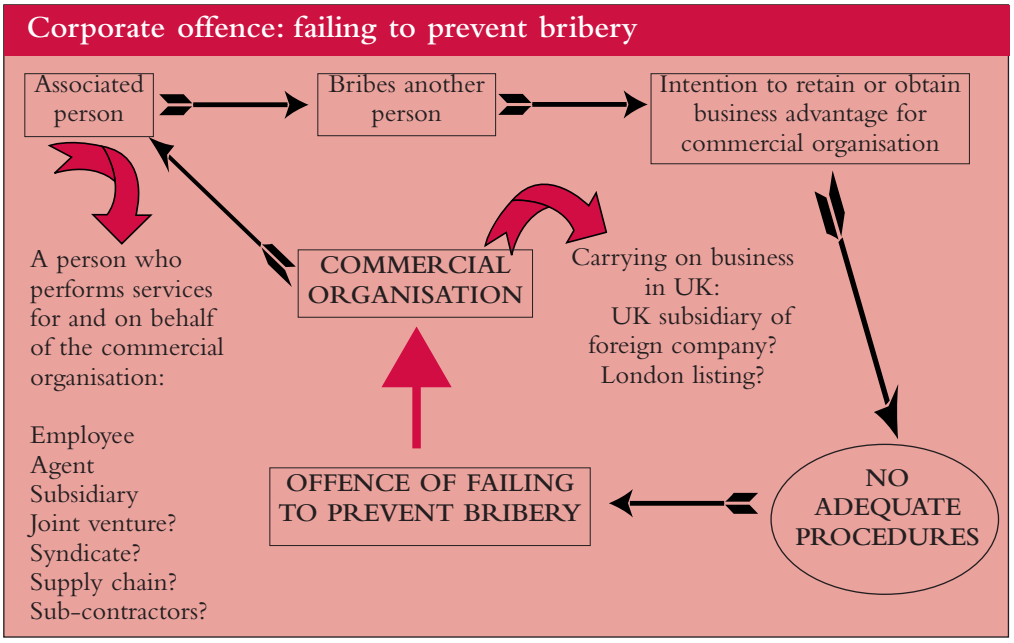
The key question, therefore, for non-UK companies is what amounts to carrying on business in the UK. Is a listing enough? Is a British subsidiary enough? Is raising finance enough? Who counts as an 'associated person'?

These are all difficult questions. The Ministry of Justice's (MoJ) guidance on the Act sheds some light, but inevitably non-UK companies will tread a murky path of uncertainty pending clarity from the UK courts. This causes understandable anxiety against the background of a criminal offence penalised by an unlimited fine.

Carrying on a business or part of a business in the UK

The jurisdictional scope of Section 7 has caused much concern within the global business community, particularly in circumstances where the Serious Fraud Office (SFO) has expressed an intention to interpret it widely. The SFO has further indicated that companies should not rely on an overly technical or clever interpretation of the Act to try and avoid liability, and that where somebody commits a bribe on behalf of a non-UK company which creates a competitive disadvantage for a UK company, it will consider prosecution. It is expected to prioritise the most high-profile, high-value and egregious cases.

By contrast, the guidance on the Bribery Act issued by the Ministry of Justice is more conservative in its interpretation of the jurisdictional scope of Section 7. It has said that it expects a 'common sense approach' to be taken to its interpretation and envisages that businesses which do not have a 'demonstrable business presence in the UK' ought not to be caught by the provision.



Listing in the UK

The MoJ's guidance also addresses a specific concern from the market, saying the government's expectation is that admission to the UK Listing Authority's Official List, and therefore trading on the London Stock Exchange (and presumably, by implication, any other UK exchange), will not be enough 'in itself' for a foreign company to be regarded as carrying on a business, or part of a business, in any part of the UK.

This was a welcome clarification from the government. However, it should be read with caution for two reasons. First, the SFO has indicated it will be interested in foreign companies that raise finance in the UK. It is difficult to reconcile this statement with the government's expectation that a listing (which is a method of raising finance) will not be enough 'in itself' for a foreign company to fall within the jurisdiction of Section 7. Second, as the guidance itself acknowledges, the courts will be the final arbiter on matters of interpretation of the Act. Ultimately, the guidance merely sets out the government's 'expectation' and, while influential, will not be binding on the courts.

The best indication of how the courts will interpret the scope of 'carrying on a business, or part of a business, in the UK' is how they have done so in analogous past cases (although, unfortunately, past cases have all been determined in the civil context and there is no criminal precedent case law).

So far as listings are concerned, there is precedent for a company that raises finance in the UK to be regarded as carrying on business in the UK. In *Actiesselkabet Dampskibs Hercules v Grand Trunk Pacific Railway* (1912) (*Dampskibs*), the Court of Appeal found that a foreign company that raised capital in England for a railway to be built, even though it was in the business of building and operating railways in a different country, was carrying on a business in the UK and so was capable of being served with a writ. Lord Justice Buckley found that:

"This company makes contracts in this country for the purpose of raising loan capital; it

is here by its agents who make such contracts on its behalf and at a fixed place. The cardinal factors are that the company does acts within the jurisdiction which are part of its business as a company, and does them at a fixed place within the jurisdiction. The raising of this loan capital is part of the company's business, and it is done here by a London committee constituted of the directors resident in England. They are the company's agents in this country for that purpose. The result is that the defendant company is resident here and is carrying on business here so as to be capable of being served with a writ."

Thus, while it may be the case that a listing 'in itself' will not be enough for a foreign company to be regarded as carrying on business in the UK, factors increasing the risk that a company that is listed will be regarded as carrying on business in the UK will include:

- making contracts in the UK
- conducting business through a fixed place in the UK
- creating a committee in the UK for the purpose of listing
- actually receiving funds in the UK.

It is not clear from *Dampskibs* which factor in particular was the most important; it seems likely it was the cumulative effect of all the factors that led the Court of Appeal to its conclusion. It may be the case that the courts will draw a distinction between a company that is already listed – and whose shares are merely being traded between third parties on an exchange which happens to be in the UK – and a company that is going through the process of listing, making contracts, holding meetings in the UK at a fixed place with banks and investors, and receiving the funds from a listing into a UK account. All these activities would, consistent with previous case law, be indicators of carrying on a (albeit ancillary or incidental) business in the UK.

In light of the government's guidance, it seems unlikely that simply being listed will be enough for a company to fall within the scope of Section 7. However, businesses will need to consider their particular appetite for risk, especially in circumstances where listed companies will be attractive high-profile targets for the SFO. At the very least, listing on the London Stock Exchange, when combined with other indication(s), may be enough to persuade a court that a foreign company is carrying on a business in the UK, or to convince the SFO to commence an investigation that could damage a reputation. It is therefore important to bear in mind the factors described below.

Physical presence in the UK

A physical presence in the UK will be a strong indication that a foreign company is carrying on a business here. The greater the permanence or profile of the presence, the stronger the indication. In making such an assessment, the court has in the past considered whether the foreign incorporated body can be contacted at a UK address and whether the premises are an established place from which it can conduct trade. A company need not own or lease premises in the UK, so long as there is a permanence or association with that company (*Re Oriel Ltd*, 1985). However, an occasional place of business such as a hotel at which one of the company's directors regularly resides is unlikely to be sufficient (*Cleveland Museum of Art v Capricorn Act International SA*, 1990), and neither is the mere presence of directors in their private residence in the UK (*Re Oriel Ltd*).

It is also unlikely that a company would be found to be carrying on a business merely by holding assets (such as shares or bonds) that are located within the UK.

Business activity

Recent case law has moved away from an emphasis on physical presence since much of modern business does not require a constant physical presence, constant activity or even regular employees.

However, there are certain business activities that, cumulatively, may be more likely to lead to a finding that a foreign company carries out business or part of a business in the UK. These include:

- using a UK address on its letterheads
- contracts being entered into in the UK
- the requirement for notice under contracts to be given to the UK address
- holding UK bank accounts
- the fact that it does not appear that the company conducts any business other than from the UK.

It does not matter that the business activity carried on in the UK is subsidiary or incidental to the foreign corporate's main business activity. Furthermore, under Section 7 of the Act, it is only necessary for the foreign company to carry out 'part of a business' in the UK. Raising capital in England for the building of a railway elsewhere was held to be sufficient (*Dampskibs*). Similarly, a foreign bank that had an office in England solely for the purpose of gathering information and managing relations with other banks and financial institutions, and not for banking transactions (which was its core business), was regarded as carrying on business in the UK (*South India Shipping Corp v Export-Import Bank of Korea*, 1985).

Neither the Act nor the guidance addresses the question of whether or not an organisation that is ordinarily resident for tax purposes would be regarded as carrying on a business in the UK, but it is likely that it would be.

Transfer of funds through the UK

In the context of the Money Laundering Regulations 2007, it has recently been held that the transfer of money and the processing of money in the UK through agents is enough for a foreign company to be carrying on business in the UK, given the multinational nature of modern business (*Moneygram Payments Systems Inc*, 2010).

This decision is consistent with the move away from an emphasis on physical presence, reflecting the international and non-corporeal nature of money transfer, and increases the risk that a listing, and the receipt of funds from it, may be regarded as the carrying on of part of a business.

Location of central management

Another factor that the courts will take into account is where the central management of the business is conducted. The issue has been considered when ascertaining whether a company is resident in the UK for tax purposes. The highest level of control, such as the taking of true business decisions as opposed to the day-to-day management of the company, is relevant here (*News Datacom v Atkinson*, 2006). If these are made within the UK, the court may find that the company is carrying on business in the UK.

Carrying on a business through a subsidiary

If a foreign company carries on business in its own right in the UK (for example, through a branch or agency), it is almost certain to be caught by Section 7. However, the guidance clarifies that a foreign company would not necessarily be regarded as carrying on a business in the UK merely by virtue of having a UK subsidiary – "since a subsidiary may act independently of its parent or other group companies" (guidance Paragraph 36). So, independence of the subsidiary will be key and the size of the shareholding will be important. Whether the parent and subsidiary have common directors is also likely to be considered.

The nature of the relationship between the parent and the subsidiary will also be a key factor. In the Court of Appeal in *Adams v Cape Industries Plc* (1989), Lord Justice Slade said: "In deciding whether a company is present in a foreign country by a subsidiary, which is itself present in that country, the court is entitled, indeed bound, to investigate the relationship between the parent and the subsidiary. In particular, that relationship may be relevant in determining whether the subsidiary was acting as the parent's agent and if so, on what terms."

The Court of Appeal went on to set out the following general factors to take into account when determining presence:

- whether or not the fixed place of business from

which the representative operates was originally acquired for the purpose of enabling him to act on behalf of the overseas corporation
- whether the overseas corporation has directly reimbursed him for (a) the cost of his accommodation at the fixed place of business; and/or (b) the cost of his staff
- what other contributions, if any, the overseas corporation makes to the financing of the business carried on by the representative
- whether the representative is remunerated by reference to transactions – for example, by commission, or by fixed regular payments or in some other way
- what degree of control the overseas corporation exercises over the running of the business conducted by the representative
- whether the representative reserves (a) part of his accommodation, and/or (b) part of his staff for conducting business related to the overseas corporation
- whether the representative displays the overseas corporation's name at his premises or on his stationery, and if so, whether he does so in such a way as to indicate that he is a representative of the overseas corporation
- what business, if any, the representative transacts as principal exclusively on his own behalf
- whether the representative makes contracts with customers or other third parties in the name of the overseas corporation, or otherwise in such manner as to bind it – and if so, whether the representative requires specific authority in advance before binding the overseas corporation to contractual obligations.

The court cautioned that this list was not exhaustive and the answer to no single question necessarily conclusive. Rather, every such case would involve an examination of all the facts, with inferences being drawn from a number of facts adjusted together and contrasted.

However, it seems that the last of these factors may have particular significance. Lord Justice Slade held that "the fact that a representative, whether with or without prior approval, never makes contracts in the name of the overseas corporation or otherwise in such manner as to bind it must be a powerful factor pointing against the presence of the overseas corporation".

It is also possible that a court might find that a parent is carrying on business in the UK through its subsidiary if the parent and the subsidiary are held to be operating as a 'single economic unit' or 'piercing the corporate veil'. However, the threshold for these tests is very high.

Group companies

Just because a company is regarded as carrying on business in the UK, this does not mean that all its subsidiary or affiliated companies are automatically also regarded as doing so. Their position will depend on the relationship between the companies, and the same principles as outlined above would be applied to any determination. However, as described below, there is a clear risk that subsidiaries, depending on their relationship with the parent, could be regarded as 'associated persons' for the purpose of Section 7 of the Act.

Who is an 'associated person'?

Once it has been established that a non-UK-incorporated company is carrying on a business in the UK, it becomes potentially liable for bribery offences committed by 'associated persons'.

'Associated person' is defined very widely in the Act as a person (either natural or legal) "who performs services for or on behalf of" the company, regardless of their capacity. They may include, for example, the company's employees, agents, subsidiaries and joint venture partners. The guidance confirms that the broad definition of 'associated person' is intended to embrace "the whole range of persons connected to an organisation who might be capable of committing bribery on the organisation's behalf" (Paragraph 37). This is to be determined by all relevant circumstances and not merely by reference to the

nature of the relationship between that person and the organisation. (Under the Act it will be presumed, unless the contrary is shown, that an employee will be performing services on behalf of his or her employer and is therefore an 'associated person'.) In addition, in order for the organisation to be liable, the bribe paid by its associated person must have been intended to benefit the organisation.

The guidance includes some helpful analysis as to whether suppliers, contractors and joint ventures fall within the definition.

Contractors and suppliers

Contractors can be associated persons to the extent that they perform services for and on behalf of an organisation. Suppliers who do no more than sell or supply goods to an organisation are unlikely to fall within the definition.

However, if they are also performing services for an organisation, such as services for equipment supplied, they may also be an associated person.

Supply chains

In relation to supply chains or a project involving a number of sub-contractors, the guidance takes a contract-by-contract approach, recognising that an organisation is likely only to exercise control over its immediate contractual counterparty. Persons who contract with that counterparty are likely to be viewed as performing services for the counterparty and not for the organisation or other persons in the chain.

Mitigation of risk

That said, to mitigate bribery risks in a supply chain, the guidance recommends that an organisation should use anti-bribery procedures in its relationship with its contractual counterparty and should request that the counterparty adopt a similar approach with the next party in the chain. Failure to do so could potentially lead to questions being raised as to whether procedures were adequate in the circumstances.

Joint ventures

The guidance differentiates between joint ventures that are conducted by its participants through a separate legal entity, and those that are operated through contractual arrangements. However, there remains some lack of clarity on how the Act will operate in practice.

Separate legal entity

Where the business is operated through a separate legal entity as a joint venture enterprise (JVE), a bribe paid by the JVE may lead to liability for the members of the joint venture if the JVE is performing services on behalf of its members and the bribe was intended to benefit them. However, a bribe paid by one of the JVE's employees or agents on its behalf should not trigger liability for the members of the joint venture simply by virtue of their benefiting indirectly from the bribe through their investment.

Contractual joint venture

Where the joint venture is being conducted through a contractual arrangement, the guidance suggests that the degree of control that a participant has over the arrangement is one of the relevant circumstances likely to be taken into account when considering the liability of that participant for bribes paid in the conduct of the joint venture business. Employees and agents of one participant will be presumed to be performing services on behalf of that participant alone and not all the other participants in the joint venture. A bribe paid in order to benefit that participant would not usually, therefore, result in liability for the other joint venture participants.

While control is not stated in the Act or the guidance to be a factor in determining whether a person is 'associated' or not, it may be one of the factors taken into account when determining the relationship between joint venture partners.

Subsidiaries and corporate ownership

Even where it has been established that a person is performing services for an organisation, liability

will only be incurred by the organisation where a bribe paid by that person was intended for its benefit. The guidance stresses that a bribe made on behalf of a subsidiary by one of its employees will not automatically involve liability for the parent company or the other subsidiaries of the parent, unless it can be shown that the bribe was intended to benefit the parent.

That an organisation benefits indirectly from a bribe – for example, through an investment or receipt of dividends or a loan from a subsidiary – will be unlikely, without more, to amount to proof of the intention required for the offence. Since a subsidiary may act independently of its parent and on its own account, having a UK subsidiary would not in itself mean a non-UK parent company would be liable for the acts of that subsidiary.

However, independence of the subsidiary is likely to be key. The courts will be the final arbiter on such questions, depending on the facts of each individual case.

Penalties

The substantive bribery offences carry prison sentences and/or unlimited fines for guilty individuals and unlimited fines for guilty companies (together with debarment from public procurement processes). The Section 7 offence, however, results in an unlimited fine only for the company (there is no penalty for any of its directors and employees) and the government has said it will not lead to mandatory debarment under the public procurement regulations. That still leaves, of course, the risk of a discretionary debarment.

30

The problems of creating criminal corporate liability in the investigation of fraud: establishing criminal responsibility at board level

Stephen Gentle, Partner, and Elly Proudlock, Solicitor Kingsley Napley LLP

The impact of the criminal law is being felt in boardrooms as never before. Businesses well used to managing commercial risk must now engage with a world where, increasingly, directors and senior officers are fixed with criminal liability not only for their own actions but also for the conduct of those whom they manage and for their company as a whole. Assessing that potential liability requires a clear understanding of the legal framework within which it arises, and an awareness of its impact on the day-to-day operation of a business.

In this chapter, we will look at how criminal liability might attach to companies and to individual senior officers, and consider how corporate criminal liability may develop in the future. It is clear that companies and their senior personnel will have to grapple with this worrying aspect of corporate life in a far more comprehensive way than perhaps has been the case in the past, or face the severe consequences of failing to do so.

Establishing the criminal liability of corporations

A company is a legal 'person' and is therefore capable of being prosecuted unless a statute indicates otherwise.

In essence there are two types of criminal offence for which a corporate body may be criminally liable: offences involving a 'fault' element where, generally, intention, knowledge or recklessness is required; and, second, offences of strict liability where there is no requirement to prove a mental element for the criminal offence to be committed. Examples of the first might be money laundering or conspiracy, and, of the second, the new offence under Section 7 of the Bribery Act where, unless it has 'adequate procedures' in place, a 'commercial organisation' will be guilty if it fails to prevent a person associated with it from engaging in bribery on its behalf.

The identification, attribution and delegation principles

Unlawful conduct by a company that involves a fault element will only attract criminal liability where the commission of the offence can be attributed to someone who at the material time was the 'directing mind and

will' of the company or 'an embodiment of the company'. Corporate criminal liability may also arise where the board of directors has delegated part of its management functions and the delegate has full discretion to act independently of instructions from them.

The case law is littered with elegant judicial phrases, metaphors and analogies. Among the most illuminating of these are the comments of Lord Reid in what remains the leading modern authority on corporate liability, *Tesco Supermarkets Ltd v Nattrass* (1972):

"A living person has a mind which can have knowledge or intention or be negligent and he has hands to carry out his intentions. A corporation has none of these: it must act through living persons, though not always one or the same person. Then the person who acts is not speaking or acting for the company. He is speaking as the company and his mind which directs his acts is the mind of the company. There is no question of the company being vicariously liable. He is not acting as a servant, representative, agent or delegate. He is an embodiment of the company or, one could say, he hears and speaks through the persona of the company, within his appropriate sphere, and his mind is the mind of the company. If it is a guilty mind, that guilt is the guilt of the company. It must be a question of law whether, once the facts have been ascertained, a person doing this is to be regarded as the company or merely as the company's servant or agent."

It will normally only be senior officers of a company, at or close to board level, whose acts are capable of being identified with the company in this way, as opposed to those acting merely as the company's agent or servant. For example, in *Tesco v Nattrass*, the supermarket group was prosecuted under the Trade Descriptions Act 1968 for displaying a notice indicating that goods were being offered at a price less than that at which they were actually being offered. This happened because the manager of one of Tesco's branches had negligently failed to notice that he had run out of the low-price packets.

The House of Lords considered that the branch manager could not be held to embody the company as a whole, which made available to Tesco the defence under Section 24 of the Trade Descriptions Act 1968 – in essence, that the commission of the offence was due to the act or default of another person, despite all due diligence having been exercised.

That said, corporate criminal liability may arise where the board of directors has delegated part of its management functions and the delegate has full discretion to act independently of instructions from them. In other words, the person who is acting with delegated authority is acting as the company.

A fine distinction

As with much of the analysis of corporate criminal liability, it may be difficult to draw the line between an employee who is acting as a mere agent and one who has the full authority of those who would normally be deemed to be the directing minds of the company.

However, there are cases where that line would be drawn by the courts. By way of example, in the *Tesco* case, the branch manager could not be identified with the company because the board never delegated any part of its functions and the acts or omissions of shop managers were not acts of the company itself.

More recent case law suggests that the courts are moving away from a blanket application of the identification principle towards a more critical examination of the particular statute creating the offence that the company may have committed, applying the normal principles of statutory construction. This will involve a sophisticated analysis of, for example, the roles played by, and the knowledge to be imputed to, the relevant company employee.

It is worth noting that the Law Commission supports this approach and proposed in its 2010 consultation on 'Criminal Liability in Regulatory Contexts' that the courts examine the underlying purpose of the relevant statutory scheme, rather

than simply applying the identification doctrine as the default doctrine of liability.

Who is identified with the company?

The identification, attribution and delegation principles significantly restrict the class of people who might be identified as company officers. In effect, it is those senior executives whose actions can be regarded as the embodiment of the company, those who are entrusted with executive functions under the memorandum and articles of association (also referred to in *Tesco v Nattrass*), or those to whom the board has delegated an independent discretion to act.

Of course, in small companies, it may be relatively straightforward to attribute the acts of the company to a senior individual. To do so in a large corporation where the board will be acting at some distance from the day-to-day actions of employees is far more difficult. Commentators criticise an unfairness at the heart of the theory of corporate liability that means, in the words of Professor James Gobert, that "corporate liability works best in cases where it is needed least and works least in cases where it is needed most" – that is, in the modern medium- to large-scale commercial enterprise.

The concept of a 'directing mind or will' is somewhat cumbersome and in stark contrast to the aggregation test that is employed in federal cases (and in some states) in the US. There, a corporation may be held criminally liable for the acts of any of its agents (including employees) if an agent commits a crime within the scope of his employment and with intent to benefit the corporation. The position of the agent in the hierarchy of the business is irrelevant and it is not necessary to prove whether any particular individual had the necessary intent. Collective knowledge held in the corporation is therefore aggregated and imputed to the corporate entity.

Additional legal limitations on corporate liability

The principles described above provide the legal framework within which corporate criminal liability operates. In addition to those parameters (and, of course, the evidential basis required for any prosecution) there are certain limits on corporate liability. Among the most important are that:

- the offence in question must be punishable with a fine. This would therefore exclude offences such as murder or piracy
- a company cannot be criminally liable for offences that cannot be committed by an official of a company in the scope of their employment – for example, rape.
- a company can be party to a criminal conspiracy, but only with at least two other conspirators who are human beings – including at least one who is an appropriate officer of the company and acting within the scope of his authority
- there are certain offences that cannot be committed by a company, such as insider dealing under the Criminal Justice Act 1993 or cartel offences under the Enterprise Act 2002.

Liability of individual directors – consent and connivance

There are a number of situations in which – where an offence is committed by a company and it is proved to have been committed with the consent, connivance or (in some cases) neglect of a director, manager or other senior person – that person is also guilty of the offence. In other words, he or she will be guilty of the same offence as the company, not a separate offence of consenting or conniving in the criminality of the company. There are many statutes containing such a provision but the most relevant are the Theft Act 1968, the Fraud Act 2006, the Companies Act 2006 and the Bribery Act 2010.

'Consent' and 'connivance' imply both knowledge and a decision made on the basis of that knowledge. In *Attorney General's Reference No 1 of 1995*, the Court of Appeal considered that 'consent' required that the accused knew the material facts constituting the offence by the body corporate and had agreed to conduct its business on the basis of those facts. Ignorance of the law was no defence.

In *Huckerby v Elliott* (1970), the divisional court

stated that a person is said to have connived in an offence when: "He is equally well aware of what is going on but his agreement is tacit, not actively encouraging what happens but letting it continue and saying nothing about it." Connivance therefore encompasses willful blindness.

The meaning of 'consent' and 'connivance' (and 'neglect') was considered by the House of Lords in *R v Chargot Ltd* (2008), in relation to an offence under Section 37 of the Health and Safety at Work Act. Presiding over a case in which an employee had been fatally injured in an accident involving a dumper truck, Lord Hope stated:

"Here too the circumstances will vary from case to case. So no fixed rule can be laid down as to what the prosecution must identify and prove in order to establish that the officer's state of mind was such as to amount to consent, connivance or neglect. In some cases, as where the officer's place of activity was remote from the workplace or what was done there was not under his immediate direction and control, this may require the leading of quite detailed evidence of which fair notice may have to be given. In others, where the officer was in day-to-day contact with what was done there, very little more may be needed."

Lord Hope went on to agree with the definition of consent as given in *Attorney General's Reference No 1 of 1995*, but added that consent and connivance can also be established by inference as well as by proof of an express agreement:

"The offences that are created by Sections 2(1) and 3(1) are directed to the result that must be achieved by the body corporate. Where it is shown that the body corporate failed to achieve or prevent the result that those Sections contemplate, it will be a relatively short step for the inference to be drawn that there was connivance or neglect on his part if the circumstances under which the risk arose were under the direction or control of the officer. The more remote his area of responsibility is from those circumstances, the harder it will be to draw that inference."

In addition to liability for consenting and conniving in an offence, a senior officer may be liable as an accessory to corporate criminality – that is, for aiding and abetting that criminal conduct. However, the legislative context for the investigation of corporate fraud is more likely to involve the specific consent-and-connive provisions in the relevant statute (commonly the Fraud Act 2006 or the Bribery Act 2010), where investigators would rely on the provisions in the criminal statute rather than on the separate legislation that sets out accessory liability.

Problems with the current law

The dearth of corporate prosecutions is testament to the difficulty in establishing criminal liability at board level. This, as we have said, is the prerequisite for a prosecution of both the corporate entity and the responsible directors. The problems with the current law can be summarised as follows:

- It is difficult to prosecute companies for serious economic crime as the threshold for criminal liability attaching to a corporate entity is high. A company can only be criminally liable if it can be shown that the directing mind – the board or the people at the most senior levels of the organisation – was involved in the commission of the offence (in other words, that the offending was almost systemic). Compare this with the US, where companies can be prosecuted for crimes committed for their benefit by their employees or agents. Although not concerned with fraud, it is also interesting to note that the Corporate Manslaughter and Corporate Homicide Act 2007 sets the liability threshold substantially lower than director level. Under Section 1 of that Act, an organisation can be guilty of the offence if the way in which its activities are managed or organised by senior management is a substantial element in the relevant breach.
- It is often difficult to identify a directing mind, particularly in a world where decision making is increasingly decentralised and businesses can operate at a multinational level.
- Because it can be difficult to pin the

responsibility at the appropriate level in the company, the offences of which companies are convicted often do not reflect the seriousness of the offending by individuals within it. For example, in July 2011, Macmillan Publishing reached a civil settlement for a sum in excess of £11 million with the Serious Fraud Office (the SFO's fifth such 'deal') over bribery allegations after admitting it had made improper and unauthorised payments to local officials in Sudan in an attempt to win contracts.

- The Law Commission argues that the law is potentially unfair to smaller companies, since the smaller the business, the more likely it is that the directors will have played an active role in the commission of the offence. Although this may not be problematic per se, it may provide a perverse incentive for companies to operate through devolved structures in order to protect directors or equivalent from knowledge of what their managers/employees are doing. It also provides an incentive to prosecutors to pursue smaller companies, where convictions will be easier to secure.

Alternatives

The Law Commission concluded its consultation on 'Criminal Liability in Regulatory Contexts' in 2010 and the responses were being analysed at the time of writing with a view to publication in spring 2012. Among other issues, the Commission was looking at the scope and status of the doctrines of consent and connivance, identification and delegation.

In relation to the identification principle, the Commission proposes:

"Legislation should include specific provisions in criminal offences to indicate the basis on which companies may be found liable, but in the absence of such provisions, the courts should treat the question of how corporate fault may be established as a matter of statutory interpretation. We encourage the courts not to presume that the identification doctrine applies when interpreting the scope of criminal offences applicable to companies."

As explained above, it seems the courts have in some cases adopted this approach. One example here is *Meridian Global Funds Management Asia Ltd v Securities Commission*, where the Privy Council – in determining that a senior officer's failure to give the required notice on the acquisition of shares could be imputed to the company – had regard to the policy behind the relevant section of the Securities Amendment Act 1988.

To avoid having to grapple in each case with the often difficult concept of 'a directing mind', it may be that a separate 'failure to prevent' offence coupled with a due diligence defence would be more sensible. This is the approach that has been adopted in the Bribery Act 2010.

In relation to the doctrine of consent or connivance, the Law Commission considers that this should not be extended, although discussion is continuing as to whether, in circumstances where a company's offence is attributable to neglect on the part of an individual director or equivalent person, the culpable individual's conduct should be captured by a separate offence of negligently failing to prevent the commission of the offence by the company.

It is interesting that there is little or no appetite for a broadening of English law on corporate liability to reflect the aggregation principles adopted in the US.

Conclusion

Establishing corporate liability in the boardroom remains a source of frustration for investigators and prosecutors.

Investigating and prosecuting an individual will focus on that individual and the evidence suggesting his or her wrongdoing – which is conceptually relatively straightforward.

Contrast that with the investigation of a case where corporate liability is the issue: the evidence must support not only criminal conduct by an individual but also the contention that the

individual was in fact a directing mind of the suspect company and that, as such, he or she carried out the criminal acts with the necessary intent.

Little wonder that the Serious Fraud Office is encouraging corporate self-reporting of misconduct, although these reports are often made by a new board, which will pin the blame for previous criminal acts on its former members. It remains one of the most peculiar aspects of English criminal law that a company (as a separate legal person) may enter a guilty plea based on evidence of what the current directors perceive as criminal acts by former directors, yet those former directors may choose to contest a trial based on the same facts – precisely what occurred in the *Mabey & Johnson* case where the engineering group and three of its senior executives were convicted over kickbacks paid to the Iraqi regime of Saddam Hussein.

The English law of corporate criminal liability has remained broadly unchanged for over a century, and although there is a new appetite for corporate prosecutions, the legislative framework is not one conducive to the regulation and policing of ethical and lawful corporate behaviour. We rely on companies, particularly large ones, to mitigate their own corporate criminal risk.

This is plainly sensible. But with the Law Commission consulting and the impact of legislation such as the Bribery Act being felt, we can expect businesses to be operating in a changed environment where corporate criminal risk will be one of the most important compliance challenges that they face in the future.

31

Fraud, bad faith and dishonest conduct: the civil element

Jonathan Cohen, Barrister Littleton Chambers
Harry Travers, Partner, and Robert Lawrie, Barrister BCL Burton Copeland

This is a book substantially about fraud and criminal liability. However, where there is the commission of a criminal offence, there will invariably be the creation of civil liability with its own consequences. In addition, civil litigation in fraud claims may itself generate criminal action, because such has been the attitude of the courts and legislature to the traditional privilege against self-incrimination enjoyed by civil litigants that it may now be thought to be effectively non-existent, or at least of very limited utility.

This chapter will look at some of the common areas that might generate liability for fraud (or similar) in civil litigation. It will address the potential claims that might be made or faced, and defences to liability. It will consider what conduct might give rise to such claims and their possible consequences.

Fraud and dishonesty

There is no cause of action in English civil litigation by the name of 'fraud'. Instead, a fraudulent standard of dishonesty is the key ingredient of numerous different types of action, each of which may be applicable to a particular fraudulent exercise depending on the way in which that exercise is performed.

One of the most common types of action based on fraud is fraudulent misrepresentation, otherwise known as the tort of deceit. A misrepresentation is a false statement of fact that is intended to induce another person to act in a particular way, most usually to enter into a contract.

A person who claims he has been the subject of this tort must prove a fraudulent intention. But what does 'fraud' mean in this context? It means that the party committing the tort has made a representation knowing it to be untrue, without any genuine belief in its truth or recklessly – not caring whether it is true or not. Put another way, if the maker of a representation does not have an honest belief in its truth, the representation has almost certainly been made fraudulently.

Fraud and fiduciary duties

Directors owe enhanced duties towards their company; those duties, formerly applied by the common law but now codified in the Part 10, Chapter II of the Companies Act 2006, are known as fiduciary duties. Directors are not the only fiduciaries; senior employees, agents and others trusted with particular responsibilities might owe fiduciary duties. Trustees owe very similar duties.

Fiduciary duties require those subject to them to act towards their principal with loyalty and the utmost good faith. A breach of those duties does not necessarily require 'fraud' in the dishonest sense, though directors who allow a company to trade fraudulently may assume personal liability, in particular to contribute to the assets of the company in the event of its insolvency.

However, it would be wrong not to consider fiduciary duties in the same context as fraud, for in a commercial environment a fiduciary claim will generally be an easier route to liability than strict fraud. Further, while not expressed in terms of dishonesty, breaches of fiduciary duty can be regarded just as seriously; they will often lead to the same remedial consequences as a finding of fraud and it is debatable whether a finding that a director or other fiduciary has acted in bad faith carries any less opprobrium. A director who has acted in bad faith might well find himself disqualified as a result of that conduct. Outside the scope of this chapter but addressed elsewhere in this book are the many criminal offences that may be committed by virtue of the same conduct, which gives rise to civil liability for breach of fiduciary duties.

A director or other fiduciary must, as set out above, act in the utmost good faith towards his principal. He must not make a profit from the trust placed in him. He must not place himself in a position of conflicting interests. He must not act so as to benefit himself or a third person by taking a business opportunity that would come within the scope of the business of his company. Common examples of obvious breaches of fiduciary duty include the receipt of bribes or 'kickbacks' and the diversion of business for the fiduciary's own benefit.

Where a director breaches these duties, the law recognises that the benefit obtained cannot be retained. It is the property of the company and must be returned to the company. In addition, any further profits made must be returned to the company.

The ability of a victim of fraud to recover his money or assets from a third party in receipt of the proceeds of a fraud is considered later in this chapter. Such recovery is not merely a question of finding a cause of action against the third party, but also tracing the proceeds. These are 'proprietary claims' – following and tracing the victim's property to its new location.

Causes of action and third parties

The law recognises two particular personal causes of action that apply to third parties who assist a fiduciary to breach his duties. These are 'personal' because they do not require that the third party is in fact in possession of the victim's assets or property (or indeed, in the case of dishonest assistance, that the third party has ever enjoyed such possession).

The first cause of action is dishonest assistance. This is an equitable remedy available against non-fiduciaries. It is a species of accessory liability. It requires only that a third party has assisted a fiduciary to breach his duty, not necessarily by the actual receipt of property abstracted in breach of that duty. Dishonest assistance does not require that the fiduciary has himself been dishonest (as set out above, a fiduciary can breach his duties without being dishonest), but the cause of action does require that the third party has been dishonest.

Dishonesty for these purposes has a subjective element. The third party must know that his conduct would be regarded as dishonest by honest people, but dishonesty does not require the third party to have actually reflected on normally acceptable standards of honesty. He must merely be aware of matters that, by normal standards, would render the transaction dishonest. Thus, dishonesty might involve mere suspicion, combined with a conscious decision not to make inquiries.

It follows that a third party does not need to know that a director or fiduciary has breached any duty, providing he is suspicious that a transaction or the source of property appears dubious and chooses deliberately not to make further inquiries.

This is, on any analysis, a low standard of dishonesty.

The second cause of action that might apply to third parties who become involved in breaches of others' fiduciary duties is 'knowing receipt'. This bites against third parties who have actually received property in the knowledge that it has been abstracted in breach of fiduciary duty. Unlike dishonest assistance, dishonesty in the strict sense is not required, though the state of mind of the recipient of the property must be such as to make it unconscionable for him to retain the benefit. Liability is not created by the receipt of property alone. In the circumstances, as with dishonest assistance, knowing receipt might also be regarded as a 'fault'-based remedy.

Cartels and anti-competitive behaviour

Companies that enter into agreements or otherwise collude by way of a concerted practice to fix prices, limit or restrict production, share markets or 'rig' bids will almost certainly face criminal action, together with their directors and those who are responsible for the anti-competitive practices, under UK or European legislation. The criminal aspect of anti-competitive behaviour is addressed elsewhere in this book. It should be noted that the powers of the Office of Fair Trading are not merely criminal. The OFT is able, on a civil standard of proof, to impose substantial fines, with a right of appeal to the Competition Appeal Tribunal.

Private civil law claims

However, another important aspect of civil liability must be considered, and that is the ability of victims of anti-competitive behaviour to bring private civil law claims.

In March 2007, the UK consumer association Which? began the first-ever 'representative action' in a cartel case on behalf of several hundred named individuals. The action related to the OFT's decision in 2003 that a number of parties had fixed the retail prices for replica football shirts for Manchester United and the England team. In January 2008, an agreement was reached with JJB Sports to settle the damages action, under which each named individual who was party to the representative action received a payment of £20.

Because group litigation in England essentially requires a positive 'opt-in' by named individuals, liability in cases of this kind is significantly smaller than, for example, in the US, where representative actions are brought on an 'opt-out' basis.

There have been two further recent developments in this rapidly evolving field.

Commercial litigation

The first is the deployment of allegations of anti-competitive behaviour as a tool in major commercial litigation, where the victim of price-fixing seeks to recover the loss that it suffers as a consequence of paying a higher price for products or services than it ordinarily would.

One difficulty often faced by the commercial victim in such a situation is showing loss; a higher price paid for goods or services has simply been passed on to the customer. In 2008, Devenish Nutrition, a supplier of animal feed that had been the victim of a cartel in the vitamin industry (vitamins being a key ingredient of animal feed), sought to avoid the difficulty of establishing loss by seeking to recover the profits made by its anti-competitive supplier. The Court of Appeal (*Devenish Nutrition Ltd v Sanofi-Aventis SA [France] & Ors* [2007]) refused to allow this, restricting the claim of a victim of anti-competitive behaviour to lost profits only.

Of course, where the victim of anti-competitive behaviour is the end user of products or services, no such difficulties will arise. The most recent example of litigation of this kind is that brought by the National Health Service against Reckitt Benckiser, the supplier of the Gaviscon heartburn treatment.

Actions against directors

The second recent development in this field, and one that will create considerable fear in the boardrooms of companies, is the claim by Safeway

(now Morrisons) against a number of its former directors for having permitted and endorsed anti-competitive activities.

Having been fined in 2007 for its part in a dairy price-fixing cartel, Safeway attempted to affix some of its then directors with liability for this conduct and to recover damages from them, representing the damages that it has had to pay in fines. The directors attempted to strike out the claim but that application failed. In the Court of Appeal they succeeded, on the basis that Safeway was affixed with the dishonesty of its directors and could not rely upon that dishonesty to mount a claim. The position, it appears, would have been otherwise if Safeway had simply suffered a civil liability rather than a criminal sanction; in such circumstances, dishonest directors might face the full force of a claim. In addition, since directors' and officers' insurance policies generally exclude liability for fraud, the consequence of a finding of dishonesty against a director can be ruinous.

Bribery and secret commissions

The new Bribery Act 2010 is concerned with bribery in a criminal context. However, bribery and secret commissions are often the subject of civil litigation. There is some academic debate as to whether bribery is in itself a cause of action (by way of tort) in English law or whether it is simply conduct that falls within other torts, for example the tort of deceit. That debate does not need to be resolved here, though it is right to say that in a number of authorities a separate and distinct tort of bribery has been recognised.

Bribery is established where the briber has persuaded or procured the bribed agent to act in a particular way as a result of the provision of payment or another benefit, in circumstances where the principal of the bribed agent is not aware of that payment or benefit.

A claim in damages lies against both the briber and the bribed agent. There is a strong presumption that any price paid by a principal for goods or services has been increased by at least the amount of the bribe. In addition, the principal can claim for any further losses that it has suffered and ordinarily has a claim against the bribed agent to recover the amount of the bribe.

Asset tracing and proprietary claims

Where stolen assets or the proceeds of a fraud can be found in the hands of a person who is not their owner, a common response of the courts is the imposition of a trust. By that device, the court recognises that the current possessor of the property (either the fraudster or a third party), even if he has acquired legal title, is not the true beneficial owner. Property in the form of a tangible or intangible asset (land, negotiable instruments etc) has remained with its true owner. The remedy of the court is therefore to hold that the current possessor of the property has it 'on trust' for the true owner.

The concept of a third party being found to hold property 'on trust' for the true owner recognises that it is not just those who perpetrate a fraud who may potentially become liable for the consequences of it. One of the most powerful remedies available to the innocent victim of a fraud is the ability to 'trace' the destination of funds or assets that have been misappropriated. Once those funds or assets have been traced to the hands of a company or person, the innocent victim may be able to recover them, notwithstanding that the fraud was perpetrated and the funds or assets originally abstracted by a third party.

Tracing claims

The purpose of a tracing claim is to ascertain what has happened to a victim's assets. In particular, it is designed to locate the value or assets that may be taken to represent assets of the victim and to which he asserts ownership. Thus, for a tracing claim to succeed, a court must be able to identify the original funds or assets, or identifiable substitutes.

In common law, the rules of asset tracing are wide. A victim can trace the original asset belonging to him, a substitute for all products of

the original asset, and even profits obtained from the original asset or substitute.

However the rules do not go so far as to allow tracing to a mixed fund, nor the banks' clearing system. Once funds or assets have been mixed so as to lose their purity, they can no longer be the subject of tracing. Some commentators take the view that this can lead to unfortunate results. Thus, an electronic transfer will defeat common law tracing at a stroke because the very nature of it is to mix the transmitted funds into the wider bank clearing system.

Some of the harsh rigidity of the common law is relieved by the rules of equitable tracing. Equity will permit tracing into and through a mixed fund. Detailed rules have been developed in equity so as to govern, in respect of a mixed fund, the status afforded to payments in and out of that fund and the priorities that are applied to the various potential owners.

Further, equitable tracing does not invariably require a breach of trust or fiduciary duty, so equitable tracing has been permitted where contracts have been induced by fraud, where mistaken payments have been made and in cases of pure theft.

The 'innocent recipient'

The remedy of tracing is clearly exceptionally useful where one is a victim of a fraud. But what if one is an innocent recipient of property? Is there, in such circumstances, a risk of another person asserting a proprietary claim against that property so that it is, in effect, confiscated? The answer depends on the state of knowledge of the recipient of the property and whether he is truly an 'innocent recipient'.

If a person is, to quote the traditional expression, a 'bona fide purchaser for value without notice', he will not be vulnerable to a proprietary claim against funds or assets that have been received. The expression is not difficult to understand. If assets have been paid for, and if the person making the payments is not aware or has no notice of the fraud, and he is otherwise acting in good faith, the defence will stand. Purchasing a used car in the local pub for half of its market value does not qualify as acting in good faith, but purchasing the same car from a dealer at fair market value plainly would.

'Change of position'

A further important defence to a tracing claim is 'change of position'. This will be available to a person who, on the basis of funds or assets received, has in some way suffered a change in his circumstances. According to Lord Goff in one of the leading House of Lords authorities: "Where an innocent defendant's position is so changed that he will suffer an injustice if called upon to repay or to repay in full, the injustice of requiring him so to repay outweighs the injustice of denying the plaintiff restitution."

Civil recovery

While the effect of a successful tracing claim may be de facto confiscation of assets, there is now a more direct means by which funds or assets may be recovered: direct action under civil recovery legislation by the state.

In 2002, the UK introduced the Proceeds of Crime Act (POCA)), although the parts of the Act that pertain to civil recovery did not come into force until 2003. Elsewhere in this book, the consequences of that Act from a criminal perspective have been addressed at length. It is important to remember, however, that Part 5 of POCA 2002 created a new statutory scheme for the recovery in civil proceedings of property which is, or represents, property obtained through unlawful (ie criminal) conduct without the requirement for a conviction.

Chapter 15 to this publication (by Covington & Burling) sets out the various cases where the SFO has sought civil recovery, and discusses the current policy of the SFO in the light of the judicial criticism in *R v Innospec Ltd* (2010) of the use of civil recovery proceedings in cases of the corruption of foreign public officials.

As far as the jurisprudential basis of the jurisdiction is concerned, the key factor is that the

enforcement agency is required to prove its case only to the lower *civil* rather than *criminal* standard of proof.

The enforcement agency does not even need to prove the commission of a specific crime (for example, fraud, money laundering or drug trafficking) as long as the matters alleged to constitute the particular type of criminality by which the property was obtained are set out.

It is not even clear whether proceedings under the Act for civil recovery enjoy the criminal protections in Article 6 of the European Convention on Human Rights. That issue is currently being visited by litigation in the Supreme Court (*Gale v SOCA*). At the time of writing, the Supreme Court has not handed down judgment, but given that the European Court of Human Rights has consistently held civil recovery to be civil in character rather than criminal, it seems relatively unlikely that the Supreme Court is likely to find otherwise.

Further, in the UK the courts have held that, when properly applied, the civil recovery laws do not arbitrarily interfere with property rights so as to contravene Article 1 of Protocol 1 of the European Convention on Human Rights. In the circumstances, the legislation is a very powerful weapon indeed.

The complex workings of the civil recovery jurisdiction provided by POCA 2002 are outside the scope of this chapter. However, there is a defence here that operates in a very similar way to the '*bona fide purchaser for value*' defence that we have already seen is applicable to a tracing claim. Thus where property can be traced to crime but the new owner of that property has acquired it in good faith, for full value and without notice of the crime, no recovery order will be made under the Act.

The privilege against self-incrimination

Given the likelihood of fraud giving rise to both civil and criminal proceedings, it is clearly in the interests of an accused person to exercise care in the civil proceedings, if those come first, and not to say or do anything that might increase the risk of exposure to criminal sanction. The law recognises this by the imposition of a privilege against self-incrimination. By that privilege, a person has a right not to answer questions or give information if it would tend to expose him to criminal penalty.

Prior to the enactment of the Fraud Act 2006, the following part of this section would have been rather longer than it is today; the privilege was important and its extent and application had been the subject of numerous judgments. However, pursuant to Section 13 of the 2006 Act, the privilege has been abrogated for any offence involving any form of fraudulent conduct or purpose.

In late 2009, in *JSC BTA Bank v Ablyazov & Ors*, the Court of Appeal determined that Section 13 had such wide impact that it applied to offences without fraudulent conduct or purpose, if the offence involved conduct that had a fraudulent 'quality'. Thus there was no privilege against self-incrimination in respect of conduct that might give rise to an offence under Section 328 of POCA (entering or becoming concerned in an arrangement that facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person), because that offence involved a degree of deception.

In the circumstances, there is now almost no scope whatsoever for exercising any privilege against self-incrimination in civil fraud proceedings, or indeed in any claim alleging some form of financial impropriety.

Considerable care must therefore be taken to determine, at the earliest stage of such proceedings, the effect that any step might have on the risk of exposure to criminal sanction.

32

IP infringement: protecting intangible digital assets from theft and industrial espionage

Julian Parker, Managing Director, London Stroz Friedberg Ltd

The protection of electronic forms of corporate intellectual property (IP) is best achieved through a series of internal and external defences. These span hardware and software solutions but ultimately rely on education and technology monitoring. Moreover, it is crucial to remember that defences need to be reviewed and updated constantly, as the IT landscape is changing at an alarming pace.

The views that follow reflect our perspective as digital investigators. The risk factors highlighted are those that have contributed to many data breaches and instances of information theft. When measures that address these risk factors are implemented, they can help to protect the business from data loss.

Broadly, companies face two distinct types of threat to their intangible digital assets. These are based on the location of the attacker in relation to the corporate network – that is, whether they are inside or outside the firewall. Normally an internal attack on corporate IP will exploit different weaknesses from an external one, reflecting the differing levels of access and knowledge about the company enjoyed by the insider compared with the outsider.

Insiders have a number of obvious advantages, including knowledge of:

- internal IT systems and controls
- system vulnerabilities and how to exploit them
- the existence and location of useful files
- intelligence on competitors and their specific interests.

By contrast, the external attacker typically lacks information on:

- precise details of the nature of the IP. For example, he or she may be unaware of blueprints, client lists, secret formulas and strategic plans
- where IP may be stored within the corporate network
- how IP is protected. He or she must therefore make a series of probing attacks that increase the probability of detection.

As a result, the external attacker will look for lower-risk options such as exploiting an insecure website or stealing a laptop. Alternatively, the attacker may opt to recruit an insider to exploit specific knowledge of the corporate network.

Internal threats and risks

People risks

It seems too obvious to mention, but intellectual property does not steal itself. The only reason IP is under threat is human frailty. It is people, driven to steal by greed, external pressures or indebtedness, who see IP as an asset they can use to their own advantage. Therefore, protection of IP should begin with a focus on the organisation's employees.

Many corporations, and especially those that have not yet suffered a theft of their data, often feel uncomfortable about 'policing' their staff. They believe too many restrictions will create an uncomfortable culture in which employees will feel they are not trusted.

Other corporations, especially those that have suffered IP loss, may view things quite differently. They prefer more controls with respect to data, and see these controls not as draconian but simply safeguards to prevent people from going astray. In reality, good controls represent a balance between giving the workforce enough freedom to operate, while ensuring that important data is well managed.

Education of the workforce also plays a vital role in the defence of corporate IP. In terms of reducing risk, it cannot be over-emphasised how important it is that employees are aware of the company's security policies, how IP is to be treated and what constitutes a breach. It also greatly assists investigations of internal data theft if it can be demonstrated that employees misusing data or committing a breach had to be aware of what they were doing.

Years of experience have shown that effective policing and investigations are worth more than a warning. Many employees perpetrate IP theft in the wake of someone else who got away with it. A corporation's reaction to such a breach sends a loud signal not only to its employees, but also to its competitors. A well-conducted investigation followed by swift and decisive action, including civil injunctions and, where appropriate, criminal sanctions, will deter all but the most hardy or oblivious from attempting a similar theft.

Moreover, if you did nothing the last time an employee walked off with your secrets, you will find it harder to persuade the courts that they should care the next time it happens.

The inherent risks of corporate information

Important data should be protected through restricted access, adequate passwords and other technical measures such as encryption. Physical access to both personal computers and to networks should be restricted, and access to confidential corporate data should be monitored and recorded. It may also be useful to mark key data with an appropriate classification, so that the reader is certain of the confidential nature of the information and how it is to be handled.

Regular audits should be conducted of where corporate information is stored and of access privileges. These will aim to ensure it is retained in the right locations and has not been deliberately or inadvertently copied. High-value corporate IP can sometimes be found in many different and often surprising places as a result of a lack of controls and/or poor IT housekeeping. Audits can also ensure that the system logging-in operation is actually both useful and appropriate. It is a sad fact that information is often logged that is neither useful nor appropriate, much to the frustration of investigators after the fact.

In the same vein, corporations should be aware of how they log emails and internet traffic within their organisation, and how this, and other activity on the network, is stored on their backups. Clear and concise logging can provide excellent evidence of data theft. Once backed up in this way, it cannot be accessed by an IP thief who might wish to try to remove traces of their activity.

The risk from hardware

A serious corporate IT security policy must address hardware issues. These will include the physical security of computers and other hardware

Knowledge box of key points

Key risks – internal	Key remedies
People: Poor security discipline, deliberate dishonesty	Policies and procedures, education, effective policing, investigations and after-the-event remediation
Corporate data: Where stored, how protected	Policies and procedures, passwords, encryption, access controls, regular audits to authenticate and check appropriate log-ins
Corporate hardware: Physical security, third-party (non-corporate) devices	Locks and functionality lockdowns, policies and permissions for non-corporate devices – their access, rights of audit
Key risks – external	**Key remedies**
Third-party software and external sites: Vulnerabilities to Trojans and weaknesses	Constantly updated virus protection, corporate user policy for external software downloads. Consider controlling internet access
Authorised access: Who can log on and with what device, how is it monitored and can data transfer be seen?	Regularly audit remote-access rights. Ensure access is removed once employees leave. Ensure rights of audit for non-corporate hardware used from home. Check and audit remote-access logs
Unauthorised access and advanced, persistent threats: Trojans, denial of service, phishing attacks, unencrypted traffic	Constantly updated virus protection and threat warnings, user education, encryption. Monitor data exfiltration, firewall restrictions
Business travel: Interception/copying of hardware and data, theft of hardware/data, subversion of employees	Threat assessment, whole disk encryption, 'clean machines' for travel, employee awareness, review of hardware upon return

devices such as portable storage media. A corporation may decide to disable certain functions such as the ability to attach external memory devices to PCs and laptops, or to restrict access to data ports.

Increasingly, organisations also need to be aware of third-party devices brought into the work environment by employees and how these can interact with the corporate data set. Such considerations will not only include personal

mobile phones (which increasingly resemble small computers in their complexity and capabilities) but also personal laptops and other processing and storage devices. It is not uncommon to find executives using their own laptop to connect to the corporate network, and in such instances, the IT department needs to be fully aware of the situation and what access should be allowed via non-company-supplied devices.

Consideration should also be given as to whether the corporation has rights of access and audit over personal devices used in the workplace.

An employee may wish to copy all their corporate emails to a personal device for home working or travelling, as they find this more convenient than a solution provided by the company. The IT department needs to make difficult decisions regarding convenience versus security, and then endeavour to supply robust security solutions that meet business requirements and also allow IT to know exactly what the picture is at any point.

A good corporate security policy will constantly re-examine the approach to using personal electronic devices, as the pace of change in this area is fast and users will be quick to take advantage of the latest technology.

External threats and risks

Third-party software and remote websites

Software is continually updated, and the corporate IT department must ensure that the software resident on machines is regularly patched. This is vital, as many hackers rely on vulnerabilities that are removed once patching has occurred. Failure to keep up to date on patching exposes a business to cyber attacks.

It is also imperative that IT has a clear understanding of what software is introduced by employees (or any outsider) into the corporate network. Many corporations have very strict rules on software use, to the extent that it is a disciplinary offence to alter the corporate systems in any way, which includes loading unauthorised software. This explicit restriction is helpful in investigations and disciplinary issues where an employee has downloaded specialist software to try to destroy evidence of their IP theft. That they have done so gives the corporation a lever to apply pressure.

While a business will want to know what third-party software its employees may be using, it will also need to be aware of any third-party networks and websites that its employees visit and restrict electronic access as it deems appropriate. Poor anti-virus safeguards can expose a company to attack from external sources and many of these attacks are initiated via Trojan Horse and other payload devices inadvertently downloaded by employees from third-party websites. In addition, some employees almost live on the web via social networks, chat pages and other media, and this can exacerbate the risks.

The extraordinary preponderance of these sites is also a threat to corporate IP in another form – namely gossip. Many corporations have found that their employees are discussing confidential matters or generally making adverse comments on social networking sites. Therefore, a company policy on the use of such media, and the consequences of misusing corporate data, should be established.

Remote-access risks

More and more employees can now gain access to their corporate data remotely. This is generally a good thing since it helps business to run more smoothly. It can also enhance the productivity of staff as they can be contacted out of hours. However, there are attendant risks for the corporate IP.

As well as knowing exactly who within the organisation has remote log-in privileges, it is important that the access of any user is terminated once they leave the organisation. This sounds obvious but it can easily happen that log-in permissions remain in place long after the employee does. This is a gift to the ex-employee seeking to steal corporate IP and has been cited in many investigations as the chosen method of data exfiltration.

As with access from inside the firewall, access to data from the outside, even when legitimately authorised, should be subject to effective logging and reviews of those logs. IT should check regularly to ensure that the corporation is aware of who has been on the system, and that it can correlate this with other risk events. The logs should be informative enough, and in the right format, to be useful in the event they are required in an investigation or legal process.

If employees are using personal or home computers to gain access to the corporate systems, the company should also ensure that it has rights of access over these devices. Ultimately it must be able to determine what has happened to its data if it has been accessed, stored or processed using these external computers. Getting access to home computers forms the basis for many investigations but can be costly and difficult. Having solid policies in place, to which employees agree in advance, will help in resolving any issues.

External network access and advanced, persistent threats

One of the most common methods used by outsiders to gain access internal to data is hacking the network by exploiting misconfigured or unrestricted firewalls. Corporate IT departments spend a great deal of time and effort ensuring that their firewall defences are as strong and up to date as possible by identifying vulnerabilities and patching them as soon as possible. But the pace of change in the digital environment is so fast that new flaws are constantly being found as the technologies and software evolve.

Gone are the days when hacking was the domain of an underground elite concerned only with proving their ability to disrupt. It is now often the province of the professional criminal or agent who is paid to break in and steal data. Hackers dedicate themselves to discovering 'zero day' (previously undiscovered) flaws, which are then sold and exploited for as long as possible before they are plugged by a new release or dedicated patch. Such flaws are incorporated into specially written programs called malware, which are designed to exploit the specific weaknesses noted above.

Malware needs to get into the corporate system to function, of course, but it can do this in a multitude of ways. The most common is via the ordinary user in so-called 'client-side exploits'. The malware is often buried in an innocuous email message purporting to be something it is not – for example, a message from a 'bank' asking you to click on a link provided. While it is to be hoped that computer users might recognise such a message to be a trap, other attacks are harder to detect. For example, some are actually designed to let the user detect a threat, at which point the danger is believed to have passed. Unfortunately, behind this decoy is the real Trojan Horse, which has now penetrated deep into the internal network. A combination of good IT discipline, appropriate network security measures and common sense on the part of users is the best antidote to such threats.

WiFi-enabled networks are also vulnerable, especially if unencrypted, and can be subjected to so-called 'man-in-the-middle' attacks in which traffic between a user and the network is monitored so that passwords or other information can be stolen.

Another threat to businesses is the 'denial of service' attack – the bombarding of the corporate website with an overwhelming stream of data (perhaps from an army of computers, or a 'botnet'). The point of the attack is to overwhelm the website, rendering it inaccessible to users.

Business travel risks

There are many countries to which corporate staff may travel where the threat of unauthorised access to their data is high.

In some countries, the threat may also come from the government, in which case laptops and other portable data-processing devices run a higher risk of being compromised. That threat is particularly pronounced upon entering and exiting the country, or within hotel rooms. There

are countries where the government can gain access to a traveller's belongings at will if left unattended – and with great sophistication.

When portable devices are accessed in this way, they can be compromised in a variety of forms. In a more sophisticated attack, information might be copied without any evidence of this having taken place (similar to a forensic copy that captures all data and is invisible to the user). In such an attack, it is quite possible that some sort of hacking or monitoring software will be loaded on to the computer, allowing the infiltrators to follow the data trail and enter the corporate network illicitly.

Alternatively, at the lowest level of sophistication, a party interested in attacking a corporate device may simply choose to steal it. In one sense this is easier for the company to deal with as it will know for certain that anything on the device is potentially compromised.

Indeed, some corporations have become so wary of the risks to their data from international travel that they dispatch executives with completely clean laptops and provide only the bare essentials needed to communicate. Such a precaution is reasonably easy to arrange, and may be seen as extremely prudent, especially for corporations owning high-quality, high-value IP.

Finally, corporate travellers should not forget that they are in a foreign environment where different rules of engagement may apply. They should realise that they may be much more at risk from a social engineering approach than is the case on their home turf. The interested stranger at the bar or the fellow businessman on a corporate trip with whom they chat about work may not be who they appear. Loneliness and frustration are highly effective levers for an agent who wishes to break down the resolve of a targeted individual.

33

Corporate intelligence: understanding the implications of breaches of cyber security and knowing how to prevent them

Vijay Rathour, Vice President, London Stroz Friedberg Ltd

The number and severity of data breaches occurring in the UK and around the world is increasing daily. The impact can be enormous. For many organisations, the immediate concern may be the risk of financial harm, through the loss of valuable intellectual property or customer information. However, reputational harm – damage to the public perception of a business – can be both more immediate and more longstanding. Preparing for, managing and regaining control of data breach scenarios is no longer merely an option for businesses but should form an essential part of the contingency planning in any organisation.

A study from the Ponemon Institute LLC found that the average cost of a data breach in the UK in 2010 grew 13 per cent from 2009 – an average of £1.9 million for the various forms of financial fallout that occurred. This included compensation to customers, investigations, improvements to software and hardware architecture, and a myriad of other considerations.

At an average cost of £71 per customer record lost, the financial impact of losing thousands, hundreds of thousands or even millions of customer files can easily bankrupt a smaller organisation and can be painful even for the largest companies. Knowing what information you hold and how much of it is potentially valuable to a hacker is vital to ensure that your defences are robust and cost-effective. Stealing a customer database that holds a million records can be the work of mere minutes or hours by a dedicated hacker, and the financial fallout will invariably outweigh the cost of implementing appropriate defences against theft.

The monetary damage flowing from a breach of cyber security can clearly be great, but while less obvious at first, the longstanding harm can be even more marked. Reporting obligations and regulatory investigations often follow serious security breaches. Highly regulated industries such as the financial sector, and any holding large quantities of 'personally identifiable information' about consumers, are likely to come under considerable scrutiny. The reputational harm resulting from publicly reported breaches can be significantly greater than the pure economic loss. Consumer trust is easily lost, whether the true impact of the breach was great or small. Once lost, that trust is very difficult to regain.

The chances are that if your information is valuable – either to you, your

competitors, or to the black market economy of intellectual property traders and credit card thieves – hackers will have every reason for trying to breach your security. Being prepared for this possibility is paramount. Many organisations have found themselves being forced to make a public statement on the potential damage done to themselves and their customers, without the luxury of time to investigate the breach fully. This can lead to even greater embarrassment and confusion as the circumstances evolve and the facts become clearer. Contingency plans can and should be made. In an age where social media networks can often be tweeting and commenting on a breach even before your staff are aware of it, the time taken to respond to your customers and the world at large is critical.

The legal and regulatory environment

Businesses are generating and processing an enormous volume of valuable personal and commercial data every day. Should the worst occur and you discover or suspect that your organisation has suffered a data breach, there are numerous practical steps to take to stop the breach and mitigate the damage. However, your approach to the problem may be dictated by the legal and regulatory environment within which you operate.

The UK Data Protection Act 1998 (DPA), and equivalent legislation as implemented within the various member states of the European Union under the Data Protection Directive, outlines many of the 'protection principles' that should be implemented by organisations 'processing' personal data. Various regulations and orders have been made under the DPA to supplement this, and other specific pieces of legislation, such as the Privacy and Electronic Communications (EC Directive) Regulations 2003, regulate certain aspects of the collection of personal data and the protection of privacy in the context of electronic communications.

Most organisations that collect data will be 'data controllers' and fall under the rules set out in the DPA with regard to the rights of the 'data subjects'. Breaches of the DPA can have severe consequences for a business. Breach investigations are overseen by the Information Commissioner's Office (ICO), an independent supervisory authority reporting directly to the UK parliament.

The Information Commissioner publishes Good Practice Notes on the management and notification of breaches of data security. Although these are not legally enforceable, the ICO has the power, under Section 55 of the DPA, to issue fines of up to £500,000 for a serious contravention of the DPA that is likely to cause 'substantial damage' or 'substantial distress'. A number of large fines have been issued, although the ICO must first be satisfied that the data controller either deliberately contravened the DPA or knew, or ought to have known, that there was a risk a contravention would occur that was likely to cause substantial damage or distress, and failed to take reasonable steps to prevent it. Although this seems like a high threshold, your organisation's overall attitude to risk and efforts to prevent data leaks will be a factor in the ICO's findings.

A variety of other general and specific regulatory obligations exist in both the private and public spheres. Expert guidance should always be sought when examining how your business takes in, stores and processes data, particularly when it is potentially valuable or sensitive. Failure to have adequate systems and controls in place when dealing with confidential information is a common target of the Financial Services Authority, and numerous high-profile fines have been issued against businesses and senior individuals found not to have taken these precautions.

Legal liabilities for failing to follow proper practice can be considerable, even when the failings themselves are relatively slight or flow from the failings of a third-party sub-contractor. Moreover, vicarious liability and responsibility flowing from the loss of confidential data can make for unwelcome headlines and result in PR damage far beyond the scope of the loss itself. Other consequences of a data breach can include:

Typical security risks

- A rogue employee stealing sensitive company documents or gaining unauthorised access to sensitive material
- External attackers compromising a server and stealing data
- IT administrators abusing privileges and privacy and stealing data
- Supply-chain or business partners abusing access rights to obtain data not intended for their eyes
- IT operations losing unencrypted data or hardware, including backup tapes
- Ex-employees stealing information because they had not had their access rights removed
- A customer service representative (including outsourced providers) inappropriately accessing customer records
- An employee losing a laptop or storage device containing sensitive information
- An employee accidentally emailing or posting sensitive information online
- An employee losing a smartphone.

Adapted from 'The Value of Corporate Secrets', Forrester, March 2010

criminal liability for directors; civil liability for breaches of employment and data privacy legislation; contractual disputes and litigation from customers and partners; and wasted costs spent investigating and preventing similar incidents.

Preventing a security breach

The Information Commissioner's Good Practice Notes provide helpful, high-level guidance on issues to be aware of whenever dealing with valuable or sensitive data, and on when the ICO should be notified in the event of a security breach. However, there are numerous practical steps that can and should be taken in anticipation of a breach being discovered – in the hope of both reducing the risk of an actual security failure and improving the management of it if the worst should occur. Some of these steps originate in legislative guidance, but most are the result of good contingency planning and security awareness.

Schedule 1 of the Data Protection Act states:

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

The DPA provides some guidance on relevant considerations, including the potential harm flowing from the security breach, appropriate technical and legal guarantees of the measures in place to prevent a breach, and the risk of a data breach by employees. ICO guidance also advocates good 'data hygiene' – the implementation of appropriate privacy considerations at the design stage of a data system, including encryption mechanisms.

There are a number of helpful measures that can be put in place in advance of a potential breach, and these are important as regulators and consumers will often be very critical of the speed with which you respond should one occur. In conjunction with a data security expert, you should prepare for cyber attacks so that, if the worst happens, you can demonstrate that your organisation had a contingency plan, that you used it in a calm and controlled fashion, and that it helped to minimise the loss and damage that could have occurred.

Pre-breach security measures

Businesses should take reasonable measures to prevent data breaches. These strategies might include:

- **Implementing appropriate physical and electronic security**. This should include machine lock-downs and enforceable policies on the use of removable media such as USB flash drives and CD burners. In addition, it is important to have controls in place that restrict email or internet access on machines with access to sensitive data. Extremely sensitive data may warrant the use of an 'air gap' to eliminate the possibility of any external network access to the host machines.
- **Restricting employee and contractor access to information, based on a 'need to know' formula**. Standard methods of access control such as the use of robust passwords and rigorous data compartmentalisation are important in the event of a system compromise, as well as in limiting the risk of data leakage by authorised system users and rogue employees. When planning your IT systems and databases, you should incorporate the 'privacy by design' concept and seek to categorise information so that different tiers of security credentials are required for access to different types of sensitive data.
- **Invoking encryption**. All devices that store or facilitate access to sensitive data should provide for adequate levels of encryption. Specifically, you should employ 'full disk' encryption on laptops and mobile devices, and permit only encrypted USB sticks to be used. All sensitive data stored on systems and mobile devices should be encrypted using industry-standard protocols. Device administrators should have full remote control, including remote 'wipe' capabilities, in the event of a device being lost or stolen. With appropriate security controls in place, sensitive data can still be protected, notwithstanding a loss of physical control over the device in question.
- **Securely storing and disposing of electronic data**. You should limit storage of unnecessary but sensitive data and personally identifiable information. Ensure that the ingestion and storage of both physical and electronic data is logged and audited, and use this to enforce a documented data-destruction policy. This policy must also apply to third parties such as sub-contractors.
- **Maintaining protocols designed to reduce the risk of unauthorised access to data**. These written protocols should be provided to employees and other relevant consultants and sub-contractors with assurances that they understand their content. They should require that a suspected data loss or intrusion into third-party systems housing sensitive data is expeditiously communicated to relevant staff in your organisation. Internal policies should address likely 'attack vectors', including internet-based email, USB flash drives and similar media, and non-secure WiFi networks ('hot spots') such as in coffee shops and airports.

It is impossible to plan for all eventualities or for the ingenuity of dedicated hackers. However, by turning to expert advice when designing IT infrastructure and protocols, the risk of data leaks and breaches can be reduced. These protocols should be regularly tested and updated, both internally and also by security experts who will conduct analyses and tests of the physical and IT security measures.

Planning for a breach

Even after the best precautions have been taken, the worst can still happen. If it does, you should be in a position to respond quickly and proportionately to both the expected and unexpected. You should draw up a plan of best practices to follow in the event of a breach and ensure that staff are familiar with it. A response strategy should, at a minimum, cover the following:

- **Define the incident**. A data breach includes situations where confidential information has potentially been compromised, whether by hacking attempts, theft, loss, or accidental disclosure to unauthorised individuals. Loss of data or penetration into your system will not necessarily mean that material can be used by wrongdoers, as long as appropriate measures have been implemented in your IT architecture. The information on a lost data-backup tape will be worthless if it is effectively encrypted, rendering it unusable. Such an incident may cause concerns internally, but will not necessarily pass the threshold of being a 'reportable' breach. Expert advice may be required to determine whether the data has actually been compromised.
- **Create an incident response team**. This team should be composed of legal counsel, internal and IT security personnel, human resources personnel and representatives from your data-security experts. Members should be aware of their responsibilities within the team and how they should contribute to identifying, stemming and preventing breaches.
- **Create a response plan**. The steps to take in the event of a suspected breach will include assessing the nature of the incursion, contingency plans for maintaining operations, and possible public relations statements.

You should also audit and maintain service-level agreements with any third-party service providers. They should implement equivalent security measures, particularly in relation to tracking the chain of custody of data that belongs to you.

Additionally, it is important to put in place protocols guiding employees about when, how and to whom to report a data breach within the organisation.

If a breach occurs, staff, executives and PR teams should be able to respond promptly and at the right level of seniority. Ensure there is effective accountability and lines of communication to senior staff. Specialist media training may also help, taking into account the particular challenges posed by modern social networking systems such as Twitter and Facebook.

Planning for a data breach will assist in the speed and thoroughness of your response. However, these plans should be regularly tested, with thorough, documented risk assessments, to ensure that staff and systems are well prepared.

Responding to a breach

In the event of a cyber attack or data breach, use your pre-planned processes to help ensure legal compliance, identify exposures and minimise costs. Regulators and clients will be very sensitive to the speed with which you react so do not delay unduly. Seek expert assistance from data-security experts to ensure that incidents are thoroughly investigated and appropriately documented.

When investigating the breach, the following steps should be taken:

- your incident response team should be briefed immediately if you suspect that a data breach may have occurred
- assess the facts and circumstances of the incident, seeking to identify the source of the breach and whether or not the incident is ongoing. If it is, seek to stop or mitigate the breach using appropriate physical and IT security measures. Regular audits of firewall policies, operating-system patches and virus-detection systems should ensure these common 'attack vectors' are closed off, but this should be confirmed. Ensure internal weaknesses in the infrastructure are investigated and see whether the breach may have originated from a current or ex-employee
- try to identify the extent of the breach, the categories of data that may have been compromised and the individuals and organisations that may have been affected. Relevant 'data controllers' and 'data subjects' should also be identified
- take advice from your data-security experts and implement measures to retrieve the

compromised data and prevent the use of the exposed information, including changing employee and website passwords and encryption keys. These steps should also help prevent further data exposure through similar weaknesses in the infrastructure

- document the steps taken and the decision-making processes that led to them; regulators will examine the circumstances, the adequacy and appropriateness of the management and actions taken, and the systems and controls put in place. This report could mitigate future legal actions and investigations by clients and other parties.

Notification

Incident response may be an ongoing process. You should seek expert assistance to help assess whether the exposed data has in fact been 'compromised'. If the data is effectively encrypted, incomplete, made anonymous, or otherwise unusable, you may not be required to notify regulators and clients. Other exemptions may also apply.

Consult any applicable contractual provisions, laws and guidance on the requirement to provide notification of the incident. If the data relates to clients or 'data subjects' in multiple jurisdictions, ensure that the relevant policies for each have also been considered and complied with.

Consider who needs to be notified. This might include: 'data subjects'; 'data controllers'; regulators, in particular the ICO; insurers; contractual partners and other third parties; and subsidiaries and related companies, especially if they use a similar IT infrastructure.

Determine when and how to provide notification. Many regulators will expect notification immediately upon discovery of a breach, but you may need time to identify the nature and scope of the incident. There may be significant negative PR fallout among the public or clients if you are perceived to have delayed unduly.

The scale of the breach may dictate the most efficient way to notify individuals – whether by personalised emails and telephone calls or through a general communication in the press. You may need to identify the circumstances of the incident, the nature of the potentially compromised data, the consequences of the breach and the steps being taken to mitigate the risks. Regulators may require continued updates.

Post-breach actions

While investigating the breach, you should seek to take immediate steps to stop it from recurring. After the incident, you should audit and re-evaluate all security protocols, at a global level, particularly if passwords and encryption keys have been compromised.

Consider whether disciplinary action needs to be taken and whether staff require retraining to take account of the lessons learned. If a formal report on the incident document is prepared, ensure that internal or external legal counsel are consulted as to the potential legal and evidential implications of such documents.

A breach report should be maintained, describing the nature of the incident and the response. These incidents may also need to be recorded on a company 'risk register'.

Regulators may investigate whether the post-breach actions were appropriate, and prompt and effective remedial steps should be implemented and recorded.

Conclusion

Security intrusions will continue. Threats can originate from both within your organisation and from outside, and good planning for these attacks can reduce the risk – even if your data is accessed inappropriately or lost – of material being sold on or a notification burden raised on your organisation. Taking steps to prepare your organisation, physically, electronically and psychologically, can help to ensure that you are able to deal with problems quickly and effectively.

34

Due diligence: know your business partners

Charles M Hewetson, Partner, and Tom Webley, Associate Reed Smith LLP

Most commercial organisations will already be familiar with the benefits (or requirements) of carrying out due diligence on their business partners. This has traditionally been done to reduce credit risk and reputational risk, as well as to comply with statutory and regulatory requirements such as money laundering rules. Now, bribery and corruption can be added to the list of areas where specific due diligence is required.

Those organisations with operations or businesses listed in the US will already be familiar with these requirements. The US government recommends that organisations subject to the Foreign Corrupt Practices Act 1977 (FCPA) "exercise due diligence and take all necessary precautions to ensure that they have formed a business relationship with reputable and qualified partners and representatives".

The UK has now introduced its own requirements in this area. On July 1, 2011, the Bribery Act 2010 came into force. Pursuant to this, a commercial organisation may be criminally liable for corrupt acts carried out on its behalf by third parties, and subject to potentially unlimited fines. But an organisation will have a defence if it can show that it had 'adequate procedures' in place to prevent 'associated persons' from committing corrupt acts. The Ministry of Justice's (MoJ) guidance on the Bribery Act, published in March 2011, makes it clear that 'adequate procedures' would include carrying out an appropriate level of due diligence on relevant business partners.

In consequence, organisations need to ensure that they assess exactly what risks each business relationship poses and carry out proportionate due diligence according to the level of risk. The size of the organisation is less relevant to the scope of the due diligence required than the complexity of the relationship and the nature of the transactions with the business partner. Smaller organisations may still face significant risks on account of the nature of their activities and the regions in which they operate.

Potential liability under the Bribery Act

The Bribery Act sets out four primary offences:

- offering, promising or giving a bribe
- requesting, agreeing to receive or accepting a bribe
- bribing a foreign public official
- failure of a relevant commercial organisation to prevent bribery (the 'corporate offence').

In order for a commercial organisation to be criminally liable for the

corporate offence, it must have failed to prevent an 'associated person' from committing one of the first three offences listed above with the intention of obtaining or retaining a business advantage for the organisation. Such liability will be strict if adequate steps are not taken to prevent bribery. No knowledge or intention by the organisation (as opposed to the associated person) is required. It also would not matter that the associated person has not been convicted of any offence.

Relevant commercial organisations

The Bribery Act applies to all companies and firms that are deemed to be 'relevant commercial organisations'. This means either:

- an organisation incorporated (if a company) or formed (in the case of a partnership) in the UK and that carries on business in the UK or elsewhere
- an organisation incorporated or formed outside the UK but that carries on a business, or part of a business, in the UK.

Associated persons

A person (which includes corporate entities) will be 'associated' with a commercial organisation if they perform services for it or on its behalf. This could include:

- subsidiaries and controlled entities
- joint venture partners
- advisers
- distributors
- contractors
- agents or intermediaries.

There is no set definition as to when a business partner will be performing services for the organisation. The MoJ guidance suggests that a third party will only be associated with the commercial organisation if it is a contractual counterparty – in other words, there is a contractual relationship. Such parties are more likely to be performing services. Sub-agents and others with which there is no contractual relationship are less likely to be considered associated persons.

This should offer some comfort for organisations whose business or commercial activities involve complex supply chains or the use of a variety of sub-contractors over which they have no direct control.

It should be remembered, however, that the guidance is not legally binding and that it will be up to the courts to interpret and apply the Bribery Act. Accordingly, where there is a high risk of bribery, an organisation should seek to ensure that its business partners carry out due diligence on any sub-contractors or sub-agents they use to perform services that could ultimately be said to be for the organisation's benefit.

Adequate procedures

Even if the commercial organisation is unable to prevent business partners from committing corrupt acts, the Bribery Act contains a defence to the corporate offence if it can show that it had 'adequate procedures' in place to stop bribery.

The MoJ guidance provides an indication as to what procedures would be considered adequate. It breaks them down into six, somewhat overlapping, principles, one of which is due diligence. These principles are designed to be flexible rather than prescriptive and should be applied according to the level of risk. The theme running through the guidance is that an organisation should take a practical, proportionate and commonsense approach when deciding on what anti-corruption procedures to put in place.

Planning the due diligence

In approaching this issue, an organisation needs to consider, first, what third parties might be considered associated persons. It should focus on any new or existing business partners that provide or potentially provide services to it. Existing relationships should be examined to ensure there is no new risk of liability since the implementation of the Bribery Act and that there

have not been any changes since the last time any due diligence was carried out.

Having identified the parties on which due diligence will have to be carried out, the organisation will have to assess the likely level of risk that they may be involved in corrupt practices aimed at gaining the organisation some benefit.

A systematic way of assessing potential risk is to set up a risk matrix. This should list all of an organisation's business partners down the side axis and the factors relevant to risk across the top. These risk factors should include ones derived from PwC's practical guide to anti-corruption due diligence, which follows this chapter, and then others linked to the relationship itself. For example, they should include:

- the country in which the partner is based
- the industry in which it operates
- the nature of the services provided
- when and how the last due diligence on that partner was carried out
- what 'red flags' or issues came out of the last due diligence (for example, prior unresolved corrupt-payment issues)
- the length of the relationship
- the size and/or quantity of the transactions
- the percentage of business being done with government or public bodies
- when the contract is due for renewal
- any unusual characteristics in the nature of the relationship, including remuneration.

Each entry should then be scored according to the perceived level of risk that it poses. The scoring system will vary depending on the nature of the organisation's business and on the services that the associated person is providing (although the system should be consistently applied within each organisation). Ideally, the total scores from this exercise will guide the organisation as to whether the relationship should be classed as low, medium or high risk.

The organisation will then have to decide on the level of due diligence required in order to gather sufficient information from, and on, the business partner to mitigate the risks of bribery. For more information on this, see Table 4 in PWC's practical guide.

Before carrying out due diligence, there should be an element of 'stepping back' and a consideration of whether particular factors point to alternative ways of mitigating risk. For instance, the associated person in the context of an otherwise high-risk project may be a significant international business or professional partnership that should have its own procedures for controlling its employees and agents. In such circumstances, a robust contractual provision requiring that business partner to adhere to the relevant rules or laws, and to ensure that its people and agents do so too, is likely to be a sufficient alternative.

Carrying out due diligence

Once the level of due diligence required has been established, the organisation will have to consider how best to gather and verify the required information. It will need enough detail to be able to assess the reliability, trustworthiness and transparency of the business partner and, in particular, the level of risk of the partner being involved in bribery.

Timing

Due diligence should always be carried out before any agreement or relationship begins. However, a full appraisal may not always be practical in a fast-moving business as the process could take several weeks. In such circumstances, it may be possible to conduct online checks initially and prepare an interim report flagging any obvious risks, with a more thorough analysis being carried out later. If this is done, it is important to ensure any agreement provides that it is conditional upon acceptable results of the full due diligence and that it can be terminated should any concerns be raised about the business partner.

Gathering the information

A simple way for an organisation to gather information from business partners is to send a

questionnaire for them to fill in. If the organisation enters into a number of very similar relationships, identical questionnaires can be used and possibly completed online. Where the nature of the relationships and activities is different, and will potentially pose different levels of risk, the questionnaires will have to be adapted. The information will need to be verified and other checks may be required, depending on the level of risk and the answers provided.

Sources for these further checks include:

Watchlists and databases of politically exposed persons
Watchlists, often produced by governments or international organisations, flag the names of people and companies over which there are concerns. The names of any companies or key individuals involved in a relationship should be checked against these lists, as well as the lists of politically exposed persons (PEPs).

Corporate registry records
These records should be checked for both the company providing the service and, potentially, others in its group. In some countries, this may involve someone physically looking up the records. Bankruptcy checks should also be carried out. In countries where corporate records are not available, references should be sought from the business partner's bank and a reputable local firm of lawyers or accountants to verify that the partner is properly constituted and able to do the required work.

Litigation records
These will be useful sources of information on any legal dispute in which the partner may have been involved. Searches of these databases can be time consuming; each country may have different courts with different records. So the searches should be focused, and limited to the countries, types of claim and courts that are likely to be of interest.

Local embassies and business groups
It may be possible either to verify information provided in the business partner questionnaire, or to find out more detail, by asking questions at local embassies and business or commerce groups in the regions where the partner operates. Asking the embassy may be useful if there is a suggestion that the partner is wholly or partially state-owned.

Media searches
The internet is a great source of quick and cheap information. But a media search should involve more than just typing the name of the company or individuals into a search engine. Where possible, local engines should be used, and in the local language as well as English. If proportionate to the potential risks, enquiries could also be made of local journalists and newspapers. But care should be taken with the results of such exercises, given the frequent suggestions of local operators unfairly disparaging rivals.

Interviews and site visits
Going to see the business operation and meeting the people involved would also be a good way to check the accuracy of the information provided and to see whether the outfit appears sound and able to perform the services. Although this would seem sensible in all contexts, where resources are tight, an argument can be made for confining this to high-value or high-risk relationships.

Using a third-party provider

It may well be cost-effective to use an external service to carry out the due diligence, either if a large volume of small checks need to be made, or if there are partners that need to be thoroughly investigated in countries where the information is not easily accessible. Before appointing a third-party provider, it is important to check that:

- it understands the purpose of the due diligence
- the due diligence is proportionate to the risks
- the provider is instructed to prepare a report that includes all the necessary information in a way that will be 'user friendly' for the intended recipient
- the information will be gathered legally. It is important to ensure that the third party is

The type of information to be collected

Information	Sources
The business partner's full, legal name, registered address and company number or equivalent.	Business partner questionnaire. Checks of local company registers.
Details of the business partner's shareholdings and shareholders, including wholly and partly owned subsidiaries or parent companies.	Business partner questionnaire. Checks of local company registers.
A list of the business partner's directors and officers, and any other employees who will be carrying out services for the organisation, including providing CVs, proof of citizenship, relationships with any politically exposed persons, references where appropriate and details of other companies in which they are involved.	Business partner questionnaire. Checks of local company registers. Media searches.
Details of other clients of the business partner, or parties with whom they regularly do business (especially public officials and government bodies), and how the business was obtained.	Business partner questionnaire. Media searches. Checks with local business groups and embassies. Watchlists and PEP databases.
Financial information, including accounts and annual reports as well as details of any history of insolvency of the business partner and any of its directors.	Business partner questionnaire. Checks of company registers. Media searches (but try to ensure these are up to date).
Details of any legal proceedings or regulatory investigations involving the business partner or any of its key personnel, with particular focus on matters involving allegations of corruption.	Business partner questionnaire. Litigation records. Media searches.
The precise nature of the intended relationship with the business partner, what services it intends to provide, how and by whom these services will be provided, and how it is going to calculate what remuneration it receives for doing so.	Business partner questionnaire. Contract documentation.
What, if any, anti-bribery and corruption policies and procedures the business partner has in place, and what due diligence it carries out on third parties with which it does business.	Business partner questionnaire.

The search should focus on the types of potential risk included in the risk matrix. The information obtained should then be incorporated into the risk matrix as a checkpoint for further due diligence.

legitimate and has a good reputation in this type of work. It would be unfortunate if an organisation were found guilty of the corporate offence because the company carrying out due diligence on its partners was bribing people to get the information!

Processing the information

The organisation should review the information and prepare a report that sets out all the steps taken to obtain the information, and highlights any particular concerns or red flags (in addition to updating the risk matrix). It is not enough merely to have adequate procedures in place; in order to defend any criminal charge or regulatory investigation, it will be necessary to prove that the procedures are followed, monitored and enforced. This means that all stages of the due diligence must be carefully documented to create a full audit trail, including decisions on the levels of due diligence to be carried out on particular partners.

The recorded due diligence should contain, at the very least:

- a clear and precise executive summary
- the business case for engaging the partner
- the risk assessment made of the partner, and specifically whether it was classified as low, medium or high risk – and why
- a list of the issues identified, and whether they can be mitigated and how
- a method of categorising the issues according to the level of risk (the obvious way to do this would be by using a 'traffic light' system).

If not drawn up by the organisation's legal department, the report should then be sent to it and/or someone in a senior management position to consider how best to deal with any red flags or issues. These considerations will include:

- what steps can be taken to mitigate the risks?
- if the risks cannot be reduced, are they so great that the business relationship should not be entered into or should be terminated?
- is the relationship necessary or is there an alternative way to have the services provided?

Ongoing commitment

Due diligence must involve regular monitoring and review – of the policy and procedures to ensure they are adequate, and of the relationship with each business partner to ensure that neither the nature of the relationship nor the risks involved have changed and no further information is required.

Communication (including training) will be required to make sure that people in the organisation realise the importance of due diligence as part of an overall anti-bribery culture. This must emphasise the genuine business benefits of carrying out due diligence, and overcome any impression that it is merely legal box-ticking.

Different partners will require different levels of ongoing due diligence. It could be annual, every two years or when the contract comes to an end or is up for renewal or renegotiation. It will, however, be worth monitoring watchlists more regularly to make sure none of the business partners or their key personnel's names appear. This can be done cheaply and easily. All information gathered should be properly stored on a document management system, so access is easy should the organisation be investigated.

Conclusion

The importance of carrying out proportionate due diligence on business partners has become even greater since the implementation of the Bribery Act. It will be vital in showing that an organisation had adequate procedures in place to prevent associated parties from engaging in bribery.

What will be required will depend on the specific nature of the business, the relationship and what services are being provided and where. It will range from a cursory background check to detailed enquiries of a business partner and, possibly, thorough investigations by specialist companies.

Given the potential liability for the acts of business partners, organisations must ensure they know who their trading partners really are.

35

Anti-corruption due diligence on business partners: a practical guide

Mark Anderson, Director PwC

For the purposes of this practical guide, we would distinguish between the due diligence conducted on a prospective or ongoing third-party business relationship, and that carried out on a prospective acquisition or equity investment target. The latter tends to be more complex and intrusive, and we have not sought to review it here.

An overview of third-party due diligence programmes

The guidance from the Ministry of Justice (MoJ) refers mainly to due diligence on 'associated persons' as third-party business partners performing services on your behalf, and this emphasis is well reasoned. For most organisations, this presents the single largest risk of illicit payments: a recent study we conducted on corruption investigations by OECD member state enforcement bodies found that approximately 80 per cent of cases involved payments being channelled through an external third party.

Your response to this threat should, however, be proportionate to the risks faced by your organisation, taking into account the number, type and role of the business partners you engage with. In our view, each organisation is unique and faces a singular set of risks and challenges that requires a tailored response. However, there are a number of common components in designing a due diligence programme, as set out in the diagram below.

Figure 1: typical elements of third-party due diligence programmes

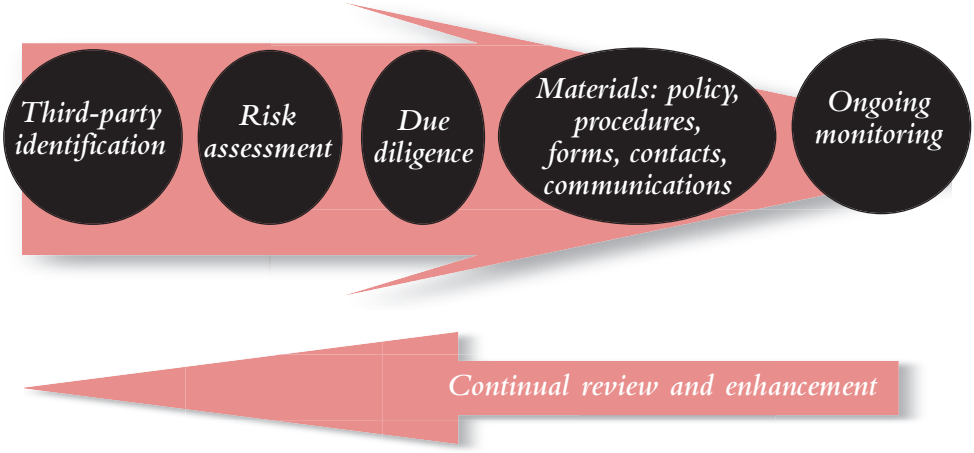


Table 1: range of third parties across the value chain of an organisation

In the supply chain	Core of the organisation	In the distribution channel
Suppliers of goods	Technical consultants	Agents
Sub-contractors	Outsourced services	Intermediaries
	Professional services (lawyers, accountants, corporate finance)	Distributors
	Lobbyists/PRs	Brokers
	Offset partners	Freight forwarders
		Channel partners
		Joint venture partners

Planning your due diligence – identification and risk assessment

A number of different categories of third party could fall under the 'associated persons' definition. Correctly identifying this population can be a surprisingly difficult task, but a vital one. Any policy or procedure you design can only be adequate if it considers all third parties, and in order to ensure this happens, you should consider taking one or all of the following steps:

- interview relevant employees at all business units on this topic, including business development or sales people, and compliance and procurement staff
- review the vendor master file or accounts payable ledgers, any available contract files (such as for agency agreements), and even the email files of key third-party relationship holders (subject to data protection laws)
- review third-party materials, such as correspondence and compliance with existing policies or procedures.

Once you have identified the relevant third parties, you should assess them all for risk. In our experience, the two categories of third party that pose the greatest integrity risk are those organisations or individuals in the distribution channels (particularly those remunerated on a success fee or commission basis) and those operating between your company and a government authority from which you require a licence to operate (such as freight forwarders, planning consultants, lobbyists and technical certification agents). However, the MoJ guidance notes that other third parties, including suppliers, could present a corruption risk where contractual or other control is exercised over their operation.

You should therefore consider a range of inherent corruption risks and put together a rating system such as the risk matrix or assessment proposed in the previous chapter. Practically, this should become a useful tool for inclusion in a selection process for new business partners.

We would therefore advocate a simple set of risk questions – based on key 'red flag' issues and business benefits – which non-compliance or legal personnel can use and which incorporate some objective measures, such as those set out in Table 2:

We would suggest this risk matrix and rating system is tested on a representative sample of third parties before being implemented as an operational procedure. It should then be consistently applied and documented.

Carrying out due diligence – due diligence itself, approvals and materials for engagement

The guidance is clear that due diligence should be proportionate to both the risks posed by the business partner and those faced by the commercial organisation. Any procedure should therefore set out an increasing level of scrutiny in accordance with the risk. We encounter a number of typical dilemmas faced by organisations in planning and executing due diligence (see Table 3).

Table 2: what level of risk is each relationship likely to involve?

Risk Area	Questions about third party	Possible measure/guidance
Business relationship	Is there a clear rationale and business case for taking on this relationship? What were the circumstances of referral? Does it have a reputation and suitable skills/experience?	Consider the rationale for engaging any third party and whether the relationship risk is outweighed by the return. The circumstances of the engagement (is there anything unusual, such as referral by the customer?) and the capability and reputation of the third party to fulfil its obligations (whether other solutions/ candidates have been considered or the organisation has represented you or others in the sector before) are also important factors in determining risk.
Geographic	Does it operate in higher- or medium-risk jurisdictions?	Bribery and corruption are more common in some countries than others. You should consider where the target operates and/or derives its revenue. The Transparency International Corruption Perceptions Index is the most commonly used index to assess country risk. A typical measure might be whether the target is based in, and/or generates 30 per cent or more of its revenue from countries with TICPI values of 6 or above for high risk, and 3-6 for medium risk.
Sector	Does it operate in higher-risk sectors or industries?	Higher corruption-risk sectors are usually those which interact regularly with government customers or regulators. Transparency International also produces a Bribe Payers Index, whose top five high-risk sectors are: public works/construction; real estate/property development; oil and gas; heavy manufacturing; and mining. Pharmaceuticals and healthcare, utilities, and aerospace and defence are also industries that feature high up in the index.
Business opportunity	What services will it perform on your behalf? How will it be remunerated?	If the third party is exercising a sales or agency function with end customers (particularly government) or negotiating with government licensing/regulatory bodies, this will attract a higher corruption risk. Similarly, a commission-based or unusual (eg offshore) payment structure or contract may be a warning sign.
Transaction	Is this a strategic or significant transaction? Is it inherently risky?	Transactions of greater significance for each side have a higher propensity to involve bribery. Consider, for example, whether the transaction represents more than 40 per cent of the revenue of the third party or a significant percentage of your own revenue. Certain types of transaction (eg political or charitable donations, or sales to state-controlled entities) also carry greater inherent corruption risk.

Table 3: dealing with the dilemmas of due diligence

Dilemma	Considerations
Time and cost	Conducting due diligence typically takes between two and eight weeks. For higher-risk relationships it can be expensive – consider cost-benefit analysis early in the process.
In-house or outsourced?	One way to reduce cost and also demonstrate objectivity is to engage an external due diligence provider. A centrally procured contract with a defined scope and cost structure for medium- and higher-risk third parties is a good option to have, particularly for jurisdictions where information availability and reliability is poor.
Central oversight v local ownership	A degree of central or compliance oversight on documentation is advisable, but should be balanced with encouraging business unit responsibility. Approvals for higher-risk relationships should be elevated to higher authorities within the organisation, demonstrating 'tone from the top'.
Linking in other risk factors	For some third parties, it may make sense to link (new or existing) due diligence processes covering other risks (eg sustainability, solvency, regulatory compliance) into one process to avoid duplication of resources.
Use of technology	The due diligence and monitoring process can be quite an administrative burden – one which can be lessened by technology. A number of bespoke and off-the-shelf solutions are available that can incorporate all the stages set out in Figure 1.

.

In our experience, each due diligence exercise should have three core objectives:

Request an appropriate amount of information from the target

Usually this exercise involves a bespoke questionnaire or application form asking for background information on the target – its capabilities and qualifications for the role, structure, key individuals, and clients. This is also an opportunity to ask for evidence of the target's anti-corruption or ethics programme to help assess whether it is managing its bribery risks.

Independently verify that information

Typically, this will involve using a range of information sources, including public and open-source research, and independent enquiries. These options are set out in Figure 2. You should understand the provenance and limitations of each source and summarise information objectively and in context to avoid bias or misconceptions. Research should be undertaken by trained staff and results recorded accurately.

Research and analyse corruption risks or red flags

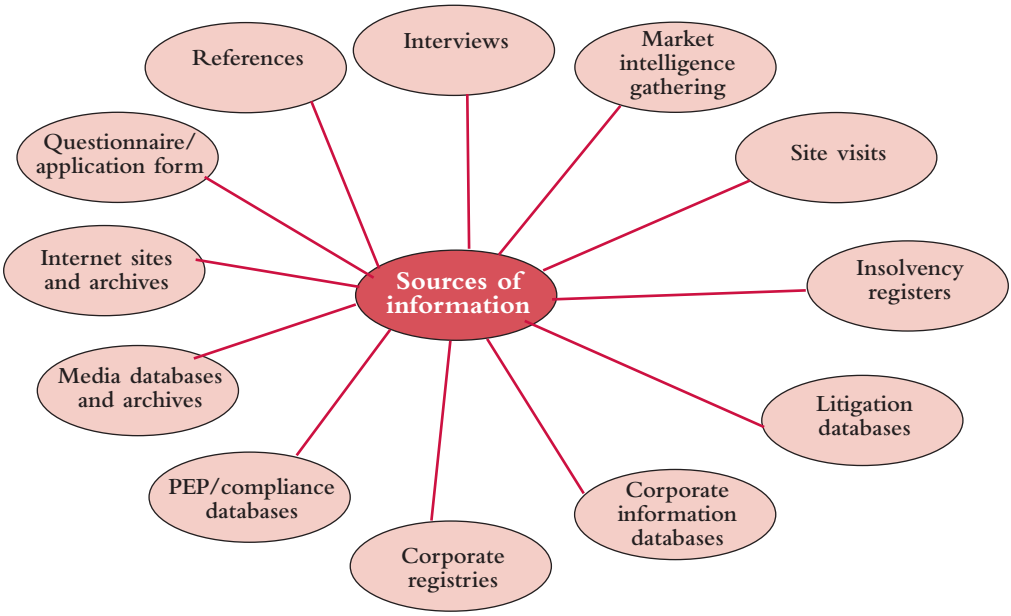
To reduce 'false positive' hits, you should construct an adverse search string for each data source and use other identifying information (such as address details and career history). Research would normally expect to cover both English and the language of the key jurisdiction of operation of the target.

Further details on the types and sources of information (and their usage) that should be considered when conducting due diligence are set out in the previous chapter.

Next steps

Having completed your due diligence, you should be able to address and employ mitigation strategies as appropriate (including, for instance,

Figure 2: range of information sources for due diligence



strengthening contract terms, agreeing monitoring, or rejection) and have sufficient information on the target to:

- gain a clear and transparent picture of the beneficial ownership structure of the target. This may involve researching back through multiple layers and jurisdictions, and understanding the rationale for any opaque or complex structures
- understand its commercial activities, history and operations, and whether it has suitable experience and capabilities for the role proposed
- understand the background and reputation of its key principals, particularly those who will represent you in any negotiations
- know any government, political or military links of the target or its principals. This is rarely a case of searching politically exposed persons (PEPs) and sanctions lists; it usually involves a wider set of information sources and diligence on the part of the researcher
- understand whether it has any history of involvement in corrupt or unethical activities
- understand whether it has a history of litigation or prosecution that would affect its suitability as your business partner
- establish the wider reputation of the target and any additional risk issues (eg solvency, sustainability, regulatory compliance).

In summary, the MoJ guidance sets out some examples of types of third-party relationships that it would categorise as higher and lower risk, and some of the activities that commercial organisations might undertake for each risk category. The guidance does not discuss a medium-risk category, but we set out some suggested activities and example relationships in this category from our own experiences. The activities in Table 4 are additive or accumulative.

Table 4: summary of suggested due diligence activities by relationship type

	Due diligence activity	Types of relationship
Lower risk	Initial risk screening and information gathering	Lower-risk employee roles Suppliers IT contractors
Medium risk	Requests for background information, including compliance programme	Contract partners/sub-contractors
	Independent verification or research from online public data sources	Freight forwarders/Customs agents Offset partners
Higher risk	More in-depth public record research (including off-line in-country archives)*	Intermediaries in distribution or sales channel
	Referencing and/or market intelligence gathering*	Intermediaries engaging with government officials
	Interviews/site visits	Lobbyists
	Internal record reviews (on occasion)*	Joint venture partners

* *Could be undertaken internally or in a report by an external service provider*

Ongoing monitoring

The bringing on board of any third party is only the start of the relationship-management process. There should be a defined responsibility for each relationship (with staff suitably trained) and it should be monitored continually, with the degree of monitoring proportionate to risk.

In our experience, due diligence renewals would typically be conducted on a two- or three-year cycle, or when a material change occurs in the target. Some organisations use monitoring technology to scan more regularly for red flags involving higher-risk business partners, and also obtain annual certifications of compliance as part of a performance review process. Some organisations also offer compliance training to third parties themselves.

You should be able to generate sufficient reporting information to understand the current status of all third-party relationships. This should include the role and risk rating of each third party, where each one is the due diligence and approval cycle, the number of terminations/rejections there have been (and reasons behind those decisions), the contractual terms in place with each one, the third-party relationship holder in your organisation, and the timing of annual certifications or due diligence renewals.

As explained in the preceding chapter, third-party due diligence is an iterative process and the procedure you employ should be continually improved and enhanced to ensure it is proportionate and adequate for your requirements.

36

How to encourage a confidential whistleblowing regime

Tracey Groves, Partner, and Harry Holdstock, Senior Associate PwC

All organisations are exposed to risk when their directors, employees, intermediaries and joint ventures perform services on the organisation's behalf. All too often a business is only alerted to misconduct when it is exposed in the media or it attracts the attention of external regulators and law enforcement agencies. Companies have to rely on the knowledge and resolve of individuals who are prepared to speak up and report incidents before news reaches the public domain.

All businesses should therefore be concerned that individuals are able to report any issues. However, developing and implementing an effective whistleblowing regime is one of the most complex challenges that organisations face. In 'Tone from the Top', a survey conducted in June 2010 by the PwC Fraud Academy, a forum through which members can share knowledge on economic crime, only 46 per cent of respondents reported that they had access to a confidential whistleblowing hotline.

There is no 'one size fits all' for the provision of whistleblowing arrangements, nor is there any guarantee that a bespoke regime will prove to be effective. Some 43 per cent of organisations surveyed in January 2011 by the Fraud Academy for a report, 'Striking a balance: Whistleblowing arrangements as part of a speak up strategy', said their existing arrangements were not effective in capturing information.

Key considerations

Legal and governance

When designing, implementing or evaluating whistleblowing arrangements, organisations should be mindful of the requirements of (and changes to) domestic and international law, both in terms of the obligations placed on organisations and the protections afforded to individuals. Legal restrictions will have a significant impact on the provision and design of whistleblowing facilities. Professional and legal advice should be sought by organisations wanting to provide centralised, cross-border facilities to ensure that these restrictions are addressed. In addition, organisations with overseas operations or activities have found that it is effective to outsource the operation of reporting mechanisms to external service providers with continuous access to interpreters of relevant foreign languages.

Table 1: requirements for whistleblowing in different jurisdictions

Location	Legal framework	Description
UK	Public Interest Disclosure Act	The UK Public Interest Disclosure Act was designed "to protect individuals who make certain disclosures of information in the public interest". Put simply, any worker who believes that he or she would suffer a detriment if they disclosed certain types of issue to their employer is protected in the eyes of the law.
UK	Data Protection Act	Whistleblowing reports that identify individuals are governed by the Data Protection Act 1988. This stipulates that the employer must act reasonably in respect of potential claims that are reported via whistleblowing, and that an investigation should be carried out if there is evidence to suggest the claim is substantiated. Failure to investigate such instances would amount to a detriment. Employers must make sure their staff have given their consent to their data being processed.
UK	Corporate Governance Code	The UK Corporate Governance Code states that organisations "should review arrangements by which staff of the company may, in confidence, raise concerns about possible improprieties". Companies to which the Code applies are required to report on how they have applied its principles or, where they have not, to provide an explanation.
UK	Bribery Act	In the UK, the Bribery Act has created the corporate offence of failing to prevent bribery. In order to defend a charge of failure in this respect, an organisation must be able to show it had adequate procedures in place. The provision of effective whistleblowing facilities is considered to be a key element of adequate procedures.
US	Sarbanes-Oxley	The US Sarbanes-Oxley Act legally obliges organisations to provide whistleblowing arrangements. These should be overseen by the audit committee, and they must allow for anonymous reporting.
US	Dodd-Frank Act	In the US, the Dodd-Frank Act provides for substantial cash rewards to be granted to whistleblowers who voluntarily provide the Securities and Exchange Commission (SEC) with information that leads to the successful prosecution of securities laws violations. Recently a US$96 million reward was made to a whistleblower in accordance with the Act at the conclusion of a $750 million settlement against a UK pharmaceutical company.
Europe	Data Protection Directive	Article 7 of the Directive requires that member states provide that personal data may be processed only if: • the data subject has unambiguously given his consent • processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract • processing is necessary for compliance with a legal obligation to which the data controller is subject • processing is necessary to protect the vital interests of the data subject • processing is necessary for the performance of a task in the public interest • processing is necessary for the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed.

Table 1 summarises some of the legal and regulatory requirements for whistleblowing in the UK, the US and the EU, including the associated issue of data protection.

Culture and environment

The task of developing a strong whistleblowing culture is a business's greatest challenge. Policies and procedures, while they may be well defined, will not on their own create a climate in which whistleblowing is accepted and encouraged. Cultural diversities, different behavioural standards and varying levels of stakeholder requirements – what they want or expect from the whistleblowing regime – must be identified and addressed, as they pose significant challenges to the development of a confidential whistleblowing culture.

For businesses operating in a global environment, the challenges are even greater. Across the world, diversity in law, history and tradition makes the development of an effective global whistleblowing regime problematic. For a whistleblowing arrangement to be effective, these disparities must be identified and managed. The cultural balance is right when there is evidence that attitudes and behaviours have begun to change with respect to speaking up.

Confidentiality v anonymity

There is an important distinction between confidentiality and anonymity. Confidential reporting is where whistleblowers choose to disclose their identity on the condition that their personal data and their identity are protected.

Anonymous reporting, on the other hand, is where individuals do not identify themselves at any stage of the process.

Confidential reporting has a number of advantages:

- information received from whistleblowers who have disclosed their identity is usually more reliable than that obtained from an anonymous source
- information is more easily put into context where the roles and responsibilities of the whistleblower within the organisation are known
- where appropriate, a representative of the response team can correspond with the whistleblower to ask for further clarification in respect of the claim
- details on the progress and outcomes of an investigation can be provided to confidential whistleblowers.

Internally v externally hosted intake mechanisms

Organisations must carefully consider who should host their designated whistleblowing intake mechanisms. At the very least, if hosted internally, they should be within the ethics, compliance, audit or other similar function.

However, more and more organisations are outsourcing the operation of their intake mechanisms to specialist third-party providers. In doing so, they create independent reporting channels that help to increase trust in the objectivity and integrity of the programme. There are a number of well-known external providers in Europe and the US, all of which provide key performance indicators and regular management information.

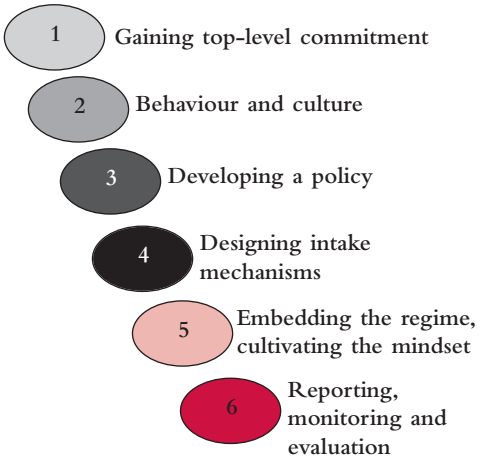
A six-step approach to whistleblowing

Whistleblowing regimes cannot be bought 'off the shelf'. As discussed above, developing effective arrangements is no easy task, particularly where there are legal and cultural challenges. But by following six key steps (as depicted in Figure 1 over page) – each representing a milestone in design and implementation – an organisation can create whistleblowing arrangements that are more likely to be highly effective.

Step 1: gaining top-level commitment

The ethical tone and culture of an organisation is defined from the top down. The attitude of the business to ethics originates from the chief executive, board and senior management and is cultivated through the policies and procedures they design and the example they set through their

Figure 1: the six steps



behaviour and actions. Top-level 'buy in' is fundamental in the development and implementation of whistleblowing arrangements. For a 'speak up' strategy to be effective and sustainable, an organisation's board must openly encourage upward and downward communication among its people.

Lip service is not enough; an organisation's leaders must be actively involved at every turn. That 41 per cent of respondents to PwC's 'Striking a Balance' survey believe more support from senior management would be advantageous suggests two things:

- adequate time and resources are not being allocated
- senior management are not 'oiling the wheels' of the whistleblowing regime as much as they should.

Step 2: behaviour and culture

Individuals will only report concerns if there is no fear of reprisals and they are secure in the knowledge that their concerns will be taken seriously. An environment in which individuals are valued and respected will underpin a culture in which whistleblowing is actively encouraged and perceived as a critical element of a risk-management framework, driven by honesty and transparency. This requires good behaviour (at all levels) to be openly rewarded and recognised, and poor behaviour to be disciplined appropriately. Where a whistleblowing regime is operating effectively, it is recognised as positive for the organisation and its stakeholders in upholding core values and standards of conduct.

Step 3: developing a policy

An organisation's commitment to open and effective whistleblowing is embodied by its formal policy, which should embed the guiding principles of the regime. For this to happen, a number of key decisions must be made:

What is the purpose of the whistleblowing arrangements?

At the outset, the whistleblowing policy must determine whether the arrangements are intended to be an individual's first port of call or his or her last resort. The policy should steer the development of the regime and state a clear purpose that can be consistently interpreted during the design and implementation phase.

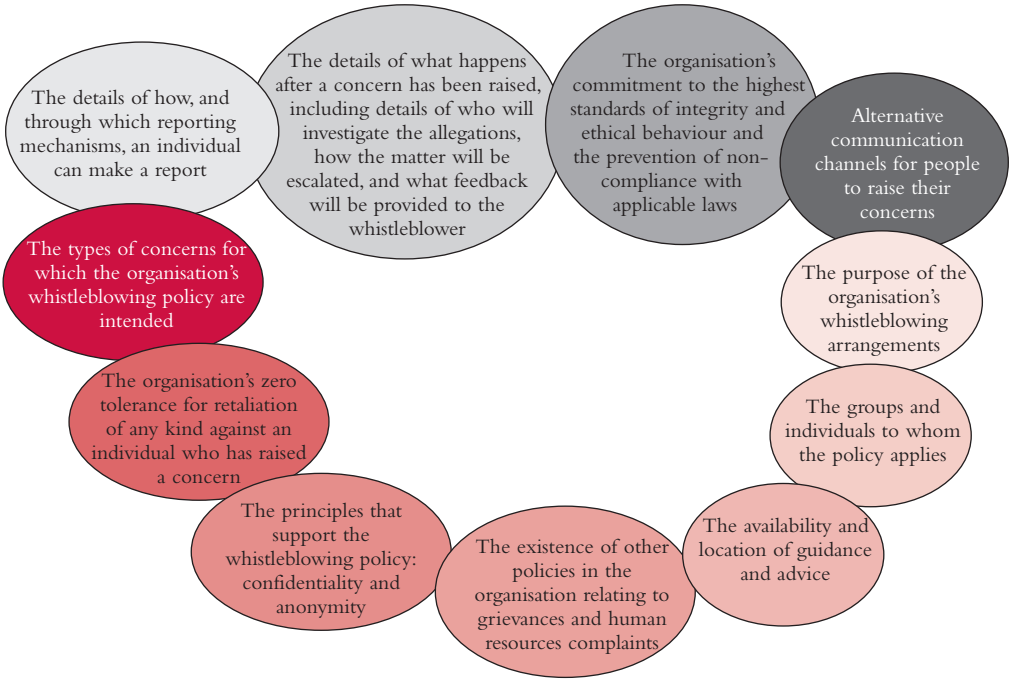
What risks are the whistleblowing arrangements designed to mitigate?

The arrangements must cater for the reporting of a number of different risks, including:

- malpractice, fraud or corruption, or any other illegal acts
- environmental damage
- health and safety risks
- concealment of information relating to any of the above.

It must be communicated to stakeholders what risks are to be reported through which of the designated whistleblowing arrangements. Different risks may require different reporting channels, so stakeholders should be clear as to where their particular concern will be raised.

Figure 2: what a whistleblowing policy should contain



Who are the intended users?

Traditionally, whistleblowers have been an organisation's employees. Increasingly, though, businesses are opening up their whistleblowing arrangements to third parties and those among the public who are well placed to raise concerns. This not only reflects a commitment on the part of the company to high standards of ethical practice, but also recognises that external sources of information are vital in combating inappropriate practices.

With the introduction of the UK Bribery Act, the regulator's field of vision has expanded to include the activities of 'associated persons'. As a result, there is value in operating a whistleblowing regime that covers this area.

What should the policy contain?

Primarily, an organisation's policy should set out the key principles that underpin a commitment to whistleblowing. To that extent, the points in Figure 2 should be included.

Step 4: designing intake mechanisms

Intake or reporting mechanisms are the channels through which organisations are notified of their people's concerns. As such, they act as a risk-management safety net. We have defined three levels of reporting mechanism, each of which is an integral part of an organisation's 'speak up' framework.

As Table 2 (over page) explains, the specific circumstances relevant to each issue will determine which mechanisms are employed; in some instances, an individual may want to report a matter directly to their line manager, whereas in more sensitive matters, only confidential reporting to a designated whistleblowing intake mechanism will suffice.

Table 2: the three levels of a reporting mechanism

Level	Overview	Explanation
1	Individual reports to line manager	When an individual wishes to raise a concern, it is important that they have the option of making a face-to-face report to their immediate manager. This is the preferred option from the business's perspective, as it allows for a swift and effective response, which is to everyone's benefit.
2	Individual reports to internally nominated party	It may not always be appropriate or possible for an employee to raise a concern directly with a line manager, particularly where that individual may be involved. So organisations should also consider designating another trusted individual – perhaps from divisional management, a union or a professional body – as a second point of contact.
3	Individual reports to dedicated intake mechanism	All organisations, regardless of size, should consider providing additional whistleblowing facilities and reporting mechanisms as this increases the likelihood that employees will feel comfortable in taking up at least one of the available options. The different mechanisms will also address different user preferences and cultural profiles, and options include a designated address, fax number, phone line, email address or web-based system.

Step 5: embedding the regime, cultivating the mindset

Even the best-designed whistleblowing arrangements will not be effective unless they are allowed to take root. That means the organisation's people must be aware of what the arrangements are and how they work, and be confident enough to confide in the regime. To meet this end, organisations need to provide potential users with clear and consistent guidance, training and communication. They must also stay true to their word by investigating all concerns in full, providing feedback to whistleblowers where appropriate.

Guidance and advice

Guidance may come in many forms – direct and indirect, personal and impersonal, written and oral. However it is rolled out, the provision of relevant and constructive advice will result in an increased awareness among staff. Many larger organisations, for example, choose to provide a helpline that allows individuals to discuss their concerns before making a formal report. A helpline can provide explanations on:

- the reporting process
- the investigation and feedback process
- the controls in place to maintain the individual's confidentiality.

Training and communication

For reporting mechanisms to be effective, it is important that individuals are aware of how to raise a concern. It is also just as critical that the people in receipt of a report know what their responsibilities are.

In this regard, training is key. The embedding of a strong whistleblowing culture relies as much on the handler knowing how to behave as it does on the informant knowing how to blow the whistle. Consequently, the whistleblowing regime should be built into regular compliance training sessions.

Employees should also receive regular communications on compliance issues, including matters relating to the whistleblowing arrangements. The communications should be delivered by senior management and other relevant parties (such as an external service

provider) so that the messages become engrained in the organisation's psyche.

Furthermore, there are benefits to be gained from publishing the outcomes of past investigations into whistleblowing allegations. Although there may be constraints – in respect of confidentiality, for example – whistleblowing will be kept at the front of people's minds and the organisation will also be seen to be making good on its promise to address all the concerns that it receives.

Case management and feedback

Actions speak louder than words, which is why management must ensure that their good intentions are put into practice when it comes to dealing with individual case reports. This is a key element in the embedding process. If users ever catch wind of poor examples of case management, all confidence in the regime will be eroded. End-to-end case management systems can be used to great effect to record and monitor the status of all whistleblower concerns, from the time they are notified until the time they are resolved.

Organisations must also commit to providing whistleblowers with feedback on the outcome of their case (within certain constraints such as employment and human rights). This commitment should be pledged in the whistleblowing policy and demonstrated in practice. It will not always be appropriate to set feedback deadlines in stone, but the simple practice of maintaining contact with whistleblowers has the effect of reassuring employees that the programme actually works. At the same time, it helps mitigate the risk that they report their concerns elsewhere – in other words, externally – because of real or perceived inaction.

Step 6: reporting, monitoring and evaluation

Organisations devote considerable time and resources to the evaluation of their internal control frameworks. This is because strong controls are effective in mitigating risk and helping to protect the bottom line. An organisation's whistleblowing arrangements should be monitored and retrospectively reviewed for the very same reasons.

Reporting and monitoring of designated intake mechanisms

The body or function charged with governance of the whistleblowing arrangements should receive regular reports on the level of activity experienced by the intake mechanisms. They should include details of the types of concerns that are being raised, the level of investigation being undertaken and the remedial actions proposed as a result of an issue being identified.

It is important that organisations evaluate the volume and substance of the whistleblowing reports. It is not possible or appropriate to make such evaluations against a set of defined parameters, but there is value in monitoring trends over time as this can identify areas of imbalance in an organisation's whistleblowing arrangements, so opening the way for remediation.

Organisations that use an end-to-end case management system will be at an advantage in this regard; these systems can be configured to generate regular reports, greatly enhancing the oversight of a company's whistleblowing arrangements.

Evaluation

From time to time, the body or function charged with governance should ensure that the organisation's arrangements are subjected to retrospective review so assurance is gained on the effectiveness of the design and implementation. This process also offers an opportunity to reflect on the lessons learnt to date and how to improve the regime as a result.

The scope and regularity of retrospective reviews will depend on the size and resources of an organisation, but there are several key questions that should be asked as part of a thorough evaluation:

- do the organisation's policy and arrangements reflect current thinking on good practice?

- how many concerns has the organisation received through its reporting mechanisms, and have they been well founded?
- what evidence is there that employees and others are both aware of reporting mechanisms and willing to use them?
- has the organisation appropriately and consistently addressed the concerns it has received?
- is the organisation aware of any illegal or unethical behaviour that has not been raised through its reporting mechanisms?
- what is the impact on the bottom line of the whistleblowing arrangements?

Conclusion

Organisations have long recognised whistleblowing as a mechanism for capturing malpractice. However, they have all too often failed to harness its full potential for good. In today's world, an effective, robust and confidential whistleblowing regime is an invaluable tool for managing risks. Without one, organisations expose themselves unnecessarily to potential financial, legal, regulatory and reputational damage.

Embedding a confidential whistleblowing regime is as much about fostering a culture and mindset of openness and transparency as it is about designing and implementing policies and procedures. Naturally, significant challenges will need to be overcome as the regime takes root and matures. However, the cost and effort involved should not dissuade businesses from investing in such a valuable long-term asset.

Notes and references

Serious Economic Crime: Notes and references

Chapter 2. The FSA's role in prosecuting market abuse and insider dealing

(1) The government has introduced a Bill that proposes to split the FSA's current responsibilities into two new regulatory authorities. The government has made clear its intention that most of the FSA's financial crime related activities will pass to the new FCA.

(2) Section 52 makes it an offence for a person who has information as an insider to deal in price-affected securities, or to encourage another to deal in those securities or to improperly disclose the information, subject to a number of caveats and pre-conditions set out in the succeeding sections.

(3) 'Market abuse' is defined in Section 118 of the FSMA, which sets out seven types of behaviour that are described as being abusive. The first three can be loosely categorised as market abuse through the improper use of information – to trade or to pass on to another. In addition, there are four forms of manipulation of the market itself, essentially involving misleading the market through trading strategies or devices or through disseminating false information.

(4) The FSA's decisions can be referred to the independent upper tribunal for a de novo hearing.

(5) See, for example, *R v Rollins* (2010).

Chapter 5. Fraud prevention by the European Commission: how the lessons from OLAF's administrative investigations are used to stop irregularities and fraud.

(1) Commission Decision of April 28, 1999 establishing the European Anti-Fraud Office.

(2) Regulation 1073/99 of the European Parliament and European Council of May 25, 1999 concerning investigations conducted by the European Anti-Fraud Office.

(3) Article 1(2) of Regulation 1073/99.

Chapter 8. Co-ordinating the fight against fraud and corruption: agreement on cross-debarment among multilateral development banks

(1) The African Development Bank Group consists of the African Development Bank, the African Development Fund and the Nigeria Trust Fund.

(2) The Inter-American Development Bank Group consists of the Inter-American Development Bank, the Inter-American Investment Corporation and the Multilateral Investment Fund.

(3) In this article, we use the term 'World Bank Group' to mean, collectively, the International Bank for Research and Development (IBRD), the International Development Association (IDA), the International Finance Corporation (IFC) and the Multilateral Investment Guarantee Agency (MIGA). The term 'World Bank' refers to the IBRD and IDA alone.

(4) The Articles of Agreement of the IBRD, for example, contain a provision stating that "the Bank and its officers shall not interfere in the political affairs of any member; nor shall they be influenced in their decisions by the political character of the member or members concerned".

(5) See Ibrahim Shihata, 'Corruption – A General Review with an Emphasis on the Role of the World Bank'. Paper based on a keynote address delivered at the International Symposium on

International Crime, Cambridge, 1996. See also Claes Sandgren, 'Combating Corruption: The Misunderstood Role of Law', International Lawyer, American Bar Association, 2005.

(6) See Ibrahim Shihata, *The World Bank Legal Papers*, Kluwer Law International, 2000.

(7) The Articles of Agreement of the IBRD, for example, state that: "The Bank shall make arrangements to ensure that the proceeds of any loan are used only for the purposes for which the loan was granted, with due attention to considerations of economy and efficiency."

(8) The World Bank, for example, defines debarment as a declaration that the firm or individual is "ineligible, either indefinitely or for a stated period of time, to be awarded a contract … for any Bank project" … or "to receive the proceeds of any loan made by the Bank".

(9) IFI Task Force, 'Uniform Framework for Preventing and Combating Fraud and Corruption' (2006).

(10) The World Bank Group, 'Mutual Enforcement of Debarment Decisions among Multilateral Development Banks' (2010).

(11) The WBG subsequently adopted a fifth definition for 'obstructive practices', as did the IDB and AsDB. Some MDBs have also targeted other practices. The AsDB, for example, may apply sanctions, among other things, over conflicts of interest and retaliation against whistleblowers.

(12) The International Investigators Conference is an annual gathering of the investigative offices from more than 35 international organisations to discuss issues of common interest, explore opportunities for harmonisation, and identify best practice in the detection, investigation and punishing of misconduct in the execution of development projects.

(13) The WBG has a two-tiered sanctions process. The first tier consists of a review of the case by an evaluation and suspension officer (EO), who reviews the evidence in a case and recommends a sanction, if any, to be imposed. If the respondent does not wish to accept the EO's determination, it may refer the case to the WBG Sanctions Board, an autonomous body consisting of seven members, four of whom are external to the Bank, for de novo consideration.

(14) There was also a belief that a joint sanctions process might have a negative impact on the privileges and immunities of individual MDBs. In reality, the opposite was probably true. In deciding whether to uphold the immunities of individual organisations, national courts (particularly in Europe) often look to whether alternative forms of redress that conform with fundamental notions of due process are available. One key feature of these notions of due process is independent decision making.

(15) In the end, the EIB did not join the Agreement. Its sanction system is still in the development stage and, when the EIB does impose sanctions, its debarment decisions will be subject to review by courts and institutional bodies within the European Union. The EIB is continuing to participate in the discussions among the MDBs on sanctions harmonisation and is reviewing how it might join the Agreement at a later time.

(16) In February 2007, the first instance of cross-debarment occurred when the EBRD debarred Lahmeyer International following debarment by the World Bank as a result of its involvement in the Lesotho Highland Waters Project. See Transparency International, 'Transparency Watch' (April 2007).

(17) The term 'open procurement' refers to the fact that the MDBs' borrowers, not MDBs, carry out the procurement of goods, works and services financed by the banks. To ensure an open and

competitive process, borrowers are only allowed to exclude bidders based on specific criteria for ineligibility – one of which is debarment by the MDB. Without cross-debarment, there was no legal basis for firms not debarred by the financing MDBs to be excluded simply because another MDB had debarred them.

(18) Knowledge that a firm or individual has been debarred by another MDB for fraud and corruption could be used as a basis for further due diligence. However, as explained above, unless the due diligence finds independent reasons not to do business with the debarred party, an MDB is obliged to finance contracts with that party under open procurement principles.

(19) Several other regional MDBs have expressed an interest in joining a regime for the mutual recognition of debarment.

(20) The AsDB only discloses debarments in two cases: (a) violation by a debarred firm of the terms of its debarment by bidding on AsDB-financed contracts; or (b) repeat offences.

(21) On the other hand, AsDB non-public debarments rely on voluntary restraint by the debarred party.

(22) Under the VDP, a firm is required to disclose misconduct on WBG-supported projects. If sanctions have been imposed on that firm by another MDB for misconduct unrelated to a WBG-supported project, it would still be protected by the VDP vis-à-vis the WBG.

(23) See Jeffrey L Friesen, 'The Distribution of Treaty-Implementing Powers in Constitutional Federations' (1994). It is noted that: "The opt-out provisions provide some safeguard for the autonomy of the nation that has the option to exercise it, while the agreement or standard is otherwise presumptively in force. The burden to opt out is on the nation seeking to exercise the option, and it will presumably do so only when it perceives a genuine threat to its interests."

(24) 'Guidelines: Procurement under IBRD Loans and IDA Credits'; 'Guidelines: Selection and Employment of Consultants under IBRD Loans and IDA Credits and Grants by World Bank Borrowers'; 'Guidelines on Preventing and Combating Fraud and Corruption in Projects Financed by IBRD Loans and IDA Credits and Grants'; 'General Conditions for Loans'.

(25) The Bank is planning to undertake a review of its sanctions regime. One of the issues that it will attempt to address is the deterrent effect of the system. Recognising that any direct or precise measurements are virtually impossible, it is hoped it will be possible to find 'proxies' that provide a rough appraisal of the regime's effectiveness.

(26) The World Bank recently adopted comprehensive guidance for dealing with corporate groups, which, among other things, allows for the derivative sanctioning of affiliated parties of a sanctioned party under certain circumstances. As a general matter, subsidiaries controlled by the sanctioned parties will also be sanctioned to avoid their use as a vehicle for circumvention, while parent companies are sanctioned only if they were involved in the misconduct or bear some responsibility for allowing it to happen.

(27) The High Level Committee on Management adopted recommendations on vendor sanctions for consideration by the organisations of the UN System, including agencies, funds and programmes.

Chapter 10. The Bribery Act 2010: implications for global businesses and individual directors

(1) British citizenship is typically acquired by birth in the UK to a parent who is a British citizen, whereas British nationality can be conferred in a

variety of circumstances and is generally held by persons connected with former British colonies. Individuals from the following overseas territories who rightly can be categorised as British nationals will be subject to the Bribery Act: Anguilla, Bermuda, British Antarctic Territory, British Indian Ocean Territory, Cayman Islands, Falkland Islands and dependencies, Gibraltar, Montserrat, Pitcairn, Henderson, Ducie and Oeno Islands, St Helena and dependencies, Hong Kong, Turks and Caicos Islands, and St Christopher and Nevis.

(2) The UK includes England, Wales, Scotland and Northern Ireland. It does not include Jersey, Guernsey or the Isle of Man. It also does not include the British overseas territories.

(3) The guidance sets out the Ministry of Justice's interpretation of various provisions of the Bribery Act. However, that interpretation is not binding on either the Serious Fraud Office or the courts.

(4) For example, the Director of the SFO has stated that the SFO will not be impressed with "overly technical interpretations" of the Bribery Act that have been crafted to evade the UK's jurisdiction. *The Daily Telegraph*, "SFO takes tough line on bribery by foreign companies", published March 31, 2011.

(5) Under Section 6, 'foreign public official' means: (a) an official who holds a legislative, administrative or judicial position of any kind, whether appointed or elected, of a country or territory outside the UK; (b) an official who exercises a public function for or on behalf of a country, territory or public agency/enterprise outside the UK (for example, professionals working for public health agencies or officers exercising public functions in state-owned enterprises); or (c) an official or agent of a public international organisation (such as the United Nations or the World Bank).

(6) Written law encompasses: (a) UK law if the official is subject to UK law; (b) the written constitution, legislation or case law of the official's country or territory; or (c) in the case of an official of a public international organisation, the organisation's written rules.

(7) When considering the activities of a company that continues to make small facilitation payments, the SFO has said that it will be looking to see whether: (a) the company has a clear issued policy regarding such payments; (b) written guidance is available to relevant employees as to the procedure they should follow when asked to make such payments; (c) such procedures are being followed by employees; (d) there is evidence that all such payments are being recorded by the company; (e) there is evidence that proper action (collective or otherwise) is being taken to inform the appropriate authorities in the countries concerned that such payments are being demanded; and (f) the company is taking what practical steps it can to curtail the making of such payments.

(8) On February 10, 2011, a jury at Southwark Crown Court found two former directors and a sales manager of Mabey & Johnson guilty of inflating the contract price for 13 steel modular bridges to provide over £360,000 in bribes to the Iraqi government of Saddam Hussein. Mabey & Johnson had pleaded guilty to breaching UN sanctions – along with separate corruption offences in Jamaica and Ghana – and was sentenced in September 2009.

Chapter 12. Cartels: competing within the rules, understanding the boundaries of fair competition

(1) *Norris v Government of the United States of America and others* (2008).

(2) Under the Enterprise Act, the Lord Advocate will prosecute the cartel offence in Scotland.

(3) See *Norris v Government of the United States of America and others*.

(4) *R v Whittle and others* (2008).

(5) *R v George, Crawley and others* (2009).

(6) In relation to Scotland, while guarantees of immunity from prosecution cannot be given, co-operation by an individual will be reported to the Lord Advocate, who will take such co-operation into account.

(7) See *R v Whittle and others*.

Chapter 15. The Proceeds of Crime Act 2002 and the prosecution of economic crime

(1) John Denham, Minister for Police, Courts and Drugs, introducing the second reading of the Proceeds of Crime Bill in the House of Commons, October 30, 2001.

(2) An SFO guide, 'The Serious Fraud Office's approach to dealing with overseas corruption', states: "We have encouraged business and professional advisers to self-report cases of overseas corruption to us … The benefit to the corporate will be the prospect (in appropriate cases) of a civil rather than a criminal outcome as well as the opportunity to manage, with us, the issues and any publicity proactively."

(3) 'Bribery Act 2010: a new beginning' – speech by Richard Alderman, Director of the Serious Fraud Office, October 13, 2010.

(4) Attorney General's Office – 'Guidance to prosecuting bodies on their asset recovery powers under the Proceeds of Crime Act 2002'.

(5) In short, a person will commit a criminal offence if he or she conceals, disguises, converts or transfers criminal property, or removes criminal property from the UK (Section 327); enters into or becomes concerned in an arrangement which he or she knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person (Section 328); or acquires, uses or has possession of criminal property (Section 329). Under Section 340 of POCA, property is 'criminal property' if it constitutes a person's benefit from criminal conduct or represents such a benefit (in whole or part, and whether directly or indirectly) and the alleged offender knows or suspects that it constitutes or represents such a benefit. The term 'criminal conduct' is broadly defined in Section 340 to include conduct that constitutes an offence in the UK or would constitute an offence in the UK if it occurred there.

(6) Further defences are provided (a) when a person intended to make an authorised disclosure but had a reasonable excuse for not doing so and (b) when a person's act was committed in carrying out a function relating to the enforcement of POCA or any other legislation relating to criminal conduct or the benefit from criminal conduct. In respect of the offence of acquiring, using or having possession of criminal property, no offence will have been committed if a person can establish that he or she acquired, used or had possession of criminal property for adequate consideration (Section 329). Consideration will be inadequate if its value is significantly less than the value of the property or the value of the use or possession of the property. The provision of goods or services that may help another to conduct criminal conduct is not regarded as adequate consideration.

(7) According to its website: "The Joint Money Laundering Steering Group is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance."

Chapter 17. Serious financial crime in the financial services sector

(1) Edward Garnier QC MP, June 18, 2011.
(2) In *R v Powell and Hinkson* (2009), the appellants were convicted of offences contrary to Section 21 of the 2000 Act. On appeal, their sentences of 15 months' imprisonment were upheld. Although there was no finding of dishonesty, the sentences were held to be justified. Likewise in *R v Epton* (2009), a sentence of 15 months' imprisonment after a guilty plea was upheld.

(3) *FSA v Fradley,* The Times, December 1, 2005.

(4) Archbold 2011, 30-212.

(5) See *FSA v Fradley*.

(6) In *R v Greaves (Claude Clifford)*, *R v Jenkins (Fraser)*, *R v Botcher (Henrik)* (2010), a judge had been entitled to order that sentences imposed on three offenders for money laundering contrary to the Proceeds of Crime Act 2002 Section 328 be served consecutive to sentences imposed for conspiracy to contravene the Financial Services and Markets Act 2000 Sections 19 and 21, as the conduct involved in the money laundering offences had added to the culpability of the conduct involved in the conspiracy offences.

(7) In *FSA v Fradley*, W had been a director of a company (R), which had sent unsolicited mail to individuals inviting them to become participants in the scheme.

(8) Archbold 2011, 3-215a.

Chapter 20. Voluntary disclosure and the problems of plea bargaining

(1) The exception to that general rule is when a company's directors have personally engaged in corrupt activities, particularly if they have obtained a personal benefit from their actions. In those circumstances, the SFO would probably commence its own criminal investigation, although it would look to the company to co-operate.

(2) 'Approach of the Serious Fraud Office to Dealing with Overseas Corruption' at paragraphs 11 and 14. Following the case of Innospec and the comments of Lord Justice Thomas, the SFO has stepped back from issuing 'joint' agreed press releases with companies, but has issued its own press releases based on the agreed facts. Examples of that practice can be seen in the press releases issued following the recent civil recovery orders in the MW Kellogg and DePuy International cases.

(3) See *SEC v Bank of America* (2010).

(4) The Attorney General's guidelines do not, and do not purport to, introduce a plea-bargaining regime. Rather, they state that the purpose of plea discussions is merely to narrow the issues in a case with a view to reaching a just outcome at the earliest possible opportunity, which may involve reaching an agreement about acceptable pleas of guilty and preparing a joint submission as to the sentence. Any such decisions are not, however, binding on the courts.

(5) See *R v Innospec Ltd* – sentencing remarks of Lord Justice Thomas, March 26, 2010.

(6) 'Approach of the Serious Fraud Office to Dealing with Overseas Corruption' at paragraph 24.

Chapter 25. Internal corporate investigations: avoiding the pitfalls

(1) See *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v European Commission* (European Court of Justice, 2010).

(2) See *Upjohn Co v United States* (1981).

Chapter 26. E-discovery and serious economic crime: a European approach to the e-discovery model

(1) A 'litigation hold' is a process used by an organisation to preserve all forms of relevant information when litigation is reasonably anticipated. The litigation hold is initiated by a notice or communication from the lawyer, at which point the organisation suspends the normal processing of records, such as back-up tape recycling, archived media and other forms of document management and storage. A litigation hold will be issued as a result, for example, of current or anticipated litigation, an audit or a government investigation, in order to avoid evidence spoliation.

(2) Data protection is not confined to EU states; there is legislation pending in many countries, including Brazil and Argentina.

(3) Bank secrecy is a legal principle in jurisdictions such as Switzerland, Singapore, Lebanon and Luxembourg. In 2009, the US government caught UBS encouraging tax evasion by sending undercover bankers with encrypted computers to the US. UBS paid a US$780 million fine and handed over hundreds of client files to US authorities. A subsequent agreement was reached between the US and Swiss governments to allow UBS to transmit to the US information about 4,450 American UBS clients suspected of tax evasion.

(4) For example, in order to protect commercial secrets, Swiss law prohibits the search for manufacturing or trade secrets in order to make them available to a foreign court or governmental agency, a foreign organisation, a private enterprise, or their agents. Therefore, anyone submitting documents to an American court or a party involved in judicial proceedings in the US may be liable to prosecution in Switzerland if such documents contain a manufacturing or trade secret. This prohibition may be in conflict with a party's duty under US procedural law to produce documents. Also, the definition of a Swiss commercial secret is quite broad: any fact relating to a Swiss-based business, or even employee, that is commercially significant and not publicly known outside Switzerland, such as a contract or an employee's salary, may fall under the umbrella of 'commercial secret'.

In France, a 'shielding' law defends French economic interests and protects the strategic data of companies against abusive actions undertaken by foreign authorities to collect economic information. This law provides that "subject to treaties or international agreements and applicable laws and regulations, it is prohibited for any party to request, seek or disclose, in writing, orally, or otherwise, economic, commercial, industrial, financial or technical documents or information leading to the constitution of evidence with a view to foreign judicial or administrative proceedings". Failure to observe this provision carries a penalty of six months' imprisonment and/or a fine of €18,000.

(5) The French Blocking Statute 80-538 of July 16, 1980 was enacted in response to perceived abuses in the extra-territorial application of US laws. Violation of the French Blocking Statute can result in criminal sanctions of six months in jail and/or a fine of €18,000.

(6) A mutual legal assistance treaty (MLAT) is an agreement between two countries for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal laws. The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters authorises obtaining evidence from other countries that are members of the convention. The Hague Convention was intended to streamline the process of obtaining discovery located abroad by bypassing the traditional consular process. Rather than route requests through diplomatic offices, letters of requests for documents are sent directly through a central authority in each of the two countries involved.

(7) The location of the servers may be influenced by how privilege attaches in different jurisdictions. If the company fears a raid, for example in France, it might be advisable to locate the servers within a French solicitor's offices. In Switzerland, as long as the e-discovery adviser is engaged by the lawyer, the data is secure.

(8) It may be the case that work product and/or analysis can be transmitted outside the jurisdiction for presentation to the investigative body or regulator. This has been a solution that we have employed when addressing Swiss Bank-related documentation and data where the underlying source data and documentation was processed in Switzerland, but the results of that analysis were delivered in a report format to US bodies in consultation with the Swiss Federal Banking Commission and SECO.

Chapter 28. Forensic accounting and serious economic crime — 'follow the money'

(1) We recognise that accounting principles and standards deal with how individual transactions are aggregated, and how transactions that are not yet completed are valued. While there are seemingly irreconcilable differences between the differing standards in different jurisdictions, at their heart individual transactions are all accounted for in similar ways. Moreover, many countries use or are converging on the International Financial Reporting Standards (IFRS), established and maintained by the International Accounting Standards Board. In some countries, local accounting principles are applied for regular companies, but listed or large companies must conform to IFRS. As a result, statutory reporting is increasingly comparable across jurisdictions.

(2) In the context of serious economic crime, the forensic accountant's work will involve pre-emptive, as well as reactive applications – good housekeeping, as well as pre- and post-acquisition due diligence work. Prevention or early identification can prove especially valuable if the potential for successor or vicarious liability exists.

(3) A CRO is a civil remedy and is therefore subject to the civil standard of proof. It can therefore be used in situations where the subject cannot be brought to trial, or has been acquitted, or there is insufficient evidence to obtain a criminal conviction. As such, the CRO can be used as a means of settling bribery charges without the need for a criminal trial. For a civil recovery order to be made, the claimant agency (in this case the SFO) needs only to establish (a) that criminal activity has taken place; and (b) that the funds which it seeks to recover represent the proceeds of such crime.

(4) The SFO first used its new asset-seizing powers on October 6, 2008, when construction group Balfour Beatty agreed to pay £2.25 million under a CRO agreed with the SFO over 'payment irregularities' in a joint venture in Egypt.

(5) The problem is that the starting point for confiscation is benefit, which is not profit but revenue. At least that is the case law to date. In the UK Court of Appeal case *R v Del Basso* in 2010, Luigi Del Basso and a colleague ran a lucrative long-term car park service at London's Stansted airport on land owned by Bishop's Stortford Football Club. Unfortunately, they operated without planning consent for several years, and failed to comply with a series of enforcement notices. The parking scheme was eventually closed down; the defendants pleaded guilty and were fined.

Confiscation proceedings under POCA began, and the main issue became how the business's operating costs should be treated for the purpose of calculating 'benefit'. The revenue received from the illegal parking was £1.88 million. The defendants, however, spent significant money operating the scheme, including paying rent and taxes. Deducting these costs brought the net profit to just £180,000.

The Court of Appeal rejected arguments that

confiscation should be based on what the defendants actually made net of all expenses. Rather, it relied on the wording of the statute that deals with the total value of the property or advantage obtained, and made a confiscation order for the full £1.88 million.

(6) Lord Justice Thomas at Southwark Crown Court also indicated that criminal cases involving corporate defendants should be resolved by criminal proceedings, not civil recovery proceedings, and that the level of fines should be much higher than those currently handed out.

(7) The fine concluded an inquiry into payments of £8 million to businessman Shailesh Vithlani in the run-up to a £28 million military radar contract for Tanzania. It was to be paid out of the £30 million compensation fund for the Tanzanian people, agreed as part of a US-style plea bargain between BAE Systems and the SFO.

Contributor profiles

This page intentionally left blank

Serious Economic Crime: Contributor profiles

Allen & Overy LLP
One Bishops Square, London E1 6AD
Tel +44 20 3088 3768
Web www.allenovery.com

Jonathan Hitchin
Partner
Email jonathan.hitchin@allenovery.com
Partner Jonathan Hitchin has over 20 years' experience and particular expertise in advising corporates on multi-jurisdictional cases and criminal investigations. He has spent much of the past ten years advising on corruption defence matters, and regularly briefs corporates on anti-corruption compliance issues, particularly relating to the new English legislation.

Arnondo Chakrabarti
Partner
Email arnondo.chakrabarti@allenovery.com
Partner Arnondo Chakrabarti has significant experience of advising on regulatory, criminal and internal investigations. In particular, he has extensive experience of liaising with the UK SFO on overseas corruption cases and has conducted internal investigations in collaboration with the SFO and negotiated settlements.

Davina Given
Senior Associate
Email davina.given@allenovery.com
Senior Associate Davina Given acts for major corporates on both domestic and cross-border contentious matters. She is a specialist in regulatory, internal and criminal investigations and has a wealth of experience in this area.

She has advised major UK companies on both SFO investigations and on making self-disclosures to the SFO following the publication of its guidelines on reporting overseas corruption.

About the Allen & Overy team
Jonathan, Arnondo and Davina – together with contributors Michelle de Kluyver, Oliver Rule, David Pygott, Laesha Smith and Trevor Withane – are part of the wider global anti-corruption team at Allen & Overy, which includes former US prosecutors in New York and experienced defence investigation lawyers in Europe and Asia.

Ranked in Tier 1 in the UK Legal 500's Corporate Crime section, the group spans Allen & Overy's offices in 26 countries. It regularly represents large multinational corporations on the full range of corruption issues, ranging from handling global investigations and defence, to risk management and assisting with policies and procedures. In 2010 the team handled separate investigations into allegations of bribery/corruption for four FTSE 350 companies, all of which involved more than one jurisdiction.

BCL Burton Copeland
51 Lincoln's Inn Fields, London WC2A 3LZ
Tel +44 20 7430 2277
Web www.bcl.com

Harry Travers
Partner
Email htravers@bcl.com
Partner Harry Travers is the consulting editor of *Serious Economic Crime*.

He specialises in all aspects of business crime and regulation, both criminal and civil, giving advice to corporates and individuals subject to investigation by the UK's leading enforcers such as the SFO, the FSA, the Office of Fair Trading, and HM Revenue and Customs.

Described by *Chambers UK* as "intense, tenacious and thoroughly committed to both clients and cases", he has had an involvement in numerous high-profile business crime cases brought

by the SFO over the past 20 years, from Maxwell and BCCI in the Nineties to, more recently, BAE, Innospec, Torex and GP Noble.

He is a member of *The Times* Law Panel, an advisory body of 100 of the country's most prominent lawyers, and is ranked by *Chambers UK* in Band 1 for both Fraud and Contentious Tax Fraud. He is also ranked as a market leader in both Civil Fraud and Health and Safety (an area where criminal sanctions are an increasing concern for corporates and their directors and employees), and named as a leading individual for Fraud by the UK Legal 500.

He joined BCL Burton Copeland in1991, and has been a partner since 1995. He was previously an employed barrister in the tax and trusts department of Berwin Leighton, specialising in anti-avoidance litigation and trusts.

He was educated at St Edmund Hall, Oxford (BCL, MA) and Manchester Grammar School.

Guy Bastable
Partner
Email gbastable@bcl.com
Partner Guy Bastable is a recognised leading expert in the UK in relation to corporate manslaughter, health and safety, criminal fraud and business crime (*Chambers UK*; the Legal 500). He has particular expertise in corporate manslaughter, health and safety, inquests, all types of fraud, financial regulation, corruption, cartel defence and money laundering. As such, he regularly advises corporates in relation to disaster management and the conduct of internal investigations.

Following an MA (Hons) at the University of Edinburgh, Mr Bastable graduated from the College of Law and the Inns of Court School of Law before qualifying as a barrister. He has enhanced full rights of audience such that he can appear as an advocate in any court, and is a co-author of Oxford University Press's *Money Laundering Law and Regulation: a Practical Guide*.

Shaul Brazil
Barrister
Email sbrazil@bcl.com
Employed Barrister Shaul Brazil specialises in business crime and regulation. He has particular experience in serious fraud, corruption (particularly overseas corruption) and contentious financial services regulation. His practice also encompasses cartel defence, extradition and mutual legal assistance, money laundering and all matters relating to the proceeds of crime.

Mr Brazil has acted in many high-profile investigations and prosecutions/proceedings brought by agencies including the SFO, the FSA, Revenue and Customs, the Serious Organised Crime Agency, the US DOJ and the Society of Lloyd's.

Recent cases include acting for a former director of a large engineering company in relation to an overseas corruption and breach of sanctions against Iraq investigation by the SFO, acting for a director of a fund of funds in relation to investigations arising from the collapse of Bernard L Madoff Investment Securities LLC, and acting for a former senior manager in a price-fixing prosecution by the US Department of Justice

Mr Brazil regularly speaks at conferences, and has authored published papers on subjects including the civil recovery of the proceeds of crime, and the effect of the new Bribery Act 2010. He is a contributing author to Oxford University Press's *Money Laundering Law and Regulation: a Practical Guide*.

Mr Brazil studied business administration at the University of Bath. He was called to the bar in 2003, and completed pupillage at a leading set of chambers specialising in fraud and regulatory law.

Robert Lawrie
Barrister
Email rlawrie@bcl.com
Employed Barrister Robert Lawrie specialises in commercial litigation and civil fraud, with a particular emphasis on actions against directors, insolvency and tax fraud matters.

Mr Lawrie advises and represents claimant and defendant clients in multi-million-pound commercial litigation, frequently in tandem with the firm's business crime and regulation department. Recent instructions include involvement in the ongoing UK litigation brought by the liquidators of Bernard Madoff's US and UK companies.

Before joining BCL Burton Copeland, Mr Lawrie practised as a self-employed barrister in employment and commercial litigation. He was educated at Edinburgh University, MA (Hons), and Eton College.

About the BCL Burton Copeland team

Harry Travers, Guy Bastable and Shaul Brazil, together with contributor Kitty St Aubyn, are all members of the business crime and regulation department of BCL Burton Copeland. Robert Lawrie is a member of the firm's dispute resolution department.

BCL is a London based law firm which is pre-eminent in the areas of business crime and regulatory enforcement, providing advice nationwide and internationally. The firm is top-ranked by *Chambers UK* for both Fraud: Criminal Corporate and Fraud: Criminal, and has seven partners ranked individually in that combined practice area.

The firm is also ranked as a leading firm in the related areas of White Collar Crime Cartel Defence, Tax: Contentious: Fraud, and Health and Safety, and is a ranked as a first-tier firm for Fraud: White Collar Crime by the UK Legal 500.

City of London Police

37 Wood Street, London EC2P 2NQ
Tel +44 20 7601 2004
Web www.cityoflondon.police.uk

Adrian Leppard
Commissioner
Email PostMaster@cityoflondon.police.uk

Adrian Leppard took up his post as Commissioner of the City of London Police in January 2011, heading the country's lead force in economic crime.

Commissioner Leppard was born, grew up and educated in Surrey, where he continues to live today. He joined Surrey Police in 1984 and has enjoyed a varied career. He has spent the majority of his service as a Detective, investigating a broad range of criminality through the ranks of Detective Sergeant to Detective Superintendent, with specialist expertise in hostage negotiation, intelligence and covert operations.

He completed an MBA with City University in 2000.

From 2003 to 2005, Commissioner Leppard served as BCU Commander in north-west Surrey, responsible for managing performance and partnerships while policing a diverse population. He transferred to Kent Police on promotion in January 2005, where he took up the role of Assistant Chief Constable for Specialist Operations with responsibility for major and organised crime, Special Branch, counter-terrorism and frontier operations, intelligence and covert operations, firearms and civil contingencies. He was appointed as Deputy Chief Constable for Kent Police in December 2007.

Jonathan Cohen

Littleton Chambers, 3 King's Bench Walk North, London EC4Y 7HR
Tel +44 20 7797 8600
Web www.littletonchambers.com
Email jcohen@littletonchambers.co.uk

Jonathan Cohen has a mixed commercial litigation and employment law practice. He has a particular expertise and interest in civil frauds and applications for all forms of interim and injunctive relief, including freezing and search-and-seizure orders. He was educated at Manchester Grammar School and Oxford University. He joined Littleton Chambers in 2007.

Mr Cohen is recommended as a leading junior in both *Chambers* and the Legal 500. He has been identified in those directories as "a fearless and

analytical advocate, loved by clients", as "a tough advocate" and described by his opponents as "knowing the law" and "extremely persuasive".

He has most recently been involved in two major pieces of commercial litigation. In *Tullett Prebon PLV v BGC Brokers LP & Ors* (2010), he represented the defendant, BGC (formerly Cantor Fitzgerald), in a high-profile claim between these city heavyweights. In *JSC BTA Bank v Ablyazov*, Mr Cohen is instructed for defendants in this significant Kazakhstan banking fraud. The litigation is ongoing. He was counsel for the defendants in the Court of Appeal in the important decision extending the abrogation of the privilege against self-incrimination.

Covington & Burling LLP
265 Strand, London WC2R 1BH
Tel +44 20 7067 2000
Web www.cov.com

Robert Amaee
Counsel
Email ramaee@cov.com

Robert Amaee, a lawyer in Covington & Burling's London office, advises companies and individuals on issues arising under the UK Bribery Act, the US Foreign Corrupt Practices Act and various country-specific anti-corruption laws. This work includes conducting risk assessments, helping design and strengthen compliance programmes, developing and delivering tailored training programmes, leading internal investigations and, when necessary, interacting with enforcement authorities.

Dr Amaee is the former Head of Anti-Corruption and Head of Proceeds of Crime at the UK Serious Fraud Office. He was responsible for the operational delivery of the SFO's anti-corruption cases, from investigation and prosecution to confiscation of criminal assets, and had strategic oversight of and involvement in negotiations that led to civil settlements in the cases of Johnson & Johnson/De Puy, MW Kellogg/KBR and Macmillan Publishers.

Dr Amaee represented the SFO on the Attorney General's Working Group on the Prosecutors' guidance to the Bribery Act and the OECD Prosecutors' Forum, and served as the SFO's Head of International Assistance.

Prior to joining the SFO, he practised as a criminal barrister and holds a PhD in medical research.

Alexandra Melia
Associate
Email amelia@cov.com

Alexandra Melia is an Associate in the London office of Covington & Burling. Ms Melia's practice encompasses a wide range of contentious and quasi-contentious matters, including internal corporate investigations, litigation before the English courts and arbitral proceedings. She also advises clients on the design, implementation and evaluation of global compliance programmes.

Ian Redfearn
Associate
Email iredfearn@cov.com

Ian Redfearn is an Associate in the dispute resolution group of the firm's London office. Mr Redfearn's practice encompasses a wide range of contentious and quasi-contentious matters, including litigation before the English courts, arbitral proceedings and internal corporate investigations.

John P Rupp
Partner
Email jrupp@cov.com

During his nearly 40 years at the firm, John Rupp has advised on compliance matters, including assisting companies in revising their compliance policies and procedures, and structuring and undertaking internal investigations involving trade control issues, bribery, money laundering and accounting irregularities.

Mr Rupp routinely interacts with senior enforcement officials in multiple jurisdictions on anti-bribery and money laundering matters. He also has written extensively on such issues. Earlier in his career, Mr Rupp spent several years at the US DOJ.

More recently, he has chaired several international anti-bribery conferences, has presented extensively at such conferences and has taught courses on anti-bribery and money laundering issues.

Dewey & LeBoeuf
No 1 Minster Court, Mincing Lane, London EC3R 7YL
Tel + 44 20 7459 5000
Web www.deweyleboeuf.com

Peter Crowther
Partner
Email pcrowther@dl.com

Peter Crowther co-ordinates the competition/EU practice, working out of the firm's London and Brussels offices.

A significant part of Mr Crowther's practice involves defending companies in a wide range of national and international government and regulatory enforcement proceedings, often simultaneously across a range of jurisdictions. He also devises and implements compliance programmes covering areas such as competition, trade/sanctions, and bribery and corruption.

Mr Crowther is a former law lecturer and former holder of a Jean Monnet Professorship in European Law. He was named one of *The Lawyer*'s 'Hot 100' for 2011.

Financial Services Authority
5 The North Colonnade, Canary Wharf, London E14 5HS
Tel +44 20 7066 1000
Web www.fsa.gov.uk

Tracey McDermott
Acting Director of Enforcement and Financial Crime

Tracey McDermott graduated in law from Queen Mary and Westfield College, University of London, and subsequently qualified as a solicitor in 1995 specialising in commercial litigation.

She joined the Enforcement Division of the FSA in 2001. Since then she has been responsible for a large number of regulatory, civil and criminal investigations across the spectrum of the FSA's regulatory responsibilities. She is currently Acting Director of the FSA's Enforcement and Financial Crime Division.

Forensic Risk Alliance
170 Westminster St, Suite 200, Providence, Rhode Island 02903
Tel: +1 401 289 0866
Web www.forensicrisk.com

Greg Mason
Partner
Email gmason@forensicrisk.com

Greg Mason is one of the co-founding partners of FRA. His expertise lies in database architecture, database programming and software design, mass data analysis and data mining for the purposes of investigations, disputes and litigation. He has been retained as an expert to provide evidence on e-discovery and electronic evidence methodology and practice, and database name matching. He has expertise in many database tools and programming languages as well as in complex financial and transactional analysis.

Mr Mason has worked on a high-profile FCPA matter where he analysed the internal financial database, comprising over 21 million transactions made in over 25 countries, for a global oil services company for presentation to SEC investigators.

He has also developed a tailored database and e-discovery review platform to review documents and capture electronic financial information for the forensic audit of monies related to over 500 bank accounts for investigation of bribery allegations in connection with a Central Asian government's privatisation of its national oil company.

Mr Mason has provided investigative and forensic accounting consulting, complex financial analysis, e-discovery processing and transactional data reconstruction, and reconciliation in response to a UN oil-for-food investigation. He went on to

perform analysis of the oil-for-food management database, which triggered payments under the programme. He carried out an audit and asset-tracing exercise of all the accounts of an employee of a high-profile client in its response to the UN and US congressional oil-for-food investigations.

After graduating from Radford University, Virginia, with a degree in statistics and mathematics, Mr Mason spent three years performing statistical testing and analysis for the US Department of Defense, evaluating the performance of sophisticated defence systems. He then moved to the disputes and investigations group at PricewaterhouseCoopers, before co-founding FRA in 1999.

Frances McLeod
Partner
Email fmcleod@forensicrisk.com

Frances McLeod is one of the co-founders of FRA and the Managing Partner. She advises diverse clients on anti-corruption (FCPA/OECD/Bribery Act) issues in terms of response to internal and external investigations, in a compliance context, and in related civil and criminal litigation in a variety of jurisdictions. Having lived and worked in the developing world, the US and Europe, she has first-hand experience in balancing regulatory demands with the working practices of G7/G20 and emerging markets.

In addition, she advises a number of European clients on data protection, privacy and related matters in the context of US-driven discovery requests, with an emphasis on providing practical solutions that balance potential conflicts of law.

Ms McLeod was responsible for the design and implementation of the claim-evaluation and administration systems of the US$1.3 billion Swiss Bank and US$2.5 billion German Slave Labor Holocaust settlements advised on by FRA. In order to develop appropriate systems for such complex and challenging claims, she drew on her experience in banking, evaluating long tail liabilities, corporate and banking/insurance archaeology, forensic accounting and asset tracing.

She has been involved in advising all of FRA's clients responding to the oil-for-food investigations in respect of their investigative and forensic accounting needs – from contributing to the formulation of strategy, presenting complex financial analysis and data, electronic and other discovery, to conducting an evaluation of the database system that underpinned the whole oil-for-food programme, and preparing witnesses for interview. Drawing on experience gained in the Swiss Bank investigations, Ms McLeod was instrumental in finding solutions for a number of clients to allow for the presentation of analysis in a manner that was not in breach of Swiss banking secrecy and/or the Swiss Criminal Code.

After graduating from Oxford University with a Masters degree, she spent six years in investment banking working in the M&A divisions of Lazards and Schroders in London and of HSBC in Indonesia.

Forensic Risk Alliance
Third Floor, Audrey House, 16-20 Ely Place, London EC1N 6SN
Tel +44 20 7831 9110
Web www.forensicrisk.com

Toby Duthie
Partner
Email tduthie@forensicrisk.com

Toby Duthie is one of co-founders of FRA and heads its London office. With experience in cases involving government enforcement in both the UK and the US, his expertise lies in internal and regulatory investigations, data protection and complex financial modelling, with particular experience in global, multi-jurisdictional cases.

Mr Duthie was instrumental in the development of FRA's service in the anti-corruption and white-collar defence arena across Europe. He spent more than five years in the US gaining extensive experience advising on damages amounts in a number of complex civil and criminal litigations and in connection with a number of

high-profile FCPA enforcement actions (relating to, for example, Panalpina, Bonny Island LNG and oil-for-food). He has also worked on matters involving the UK, Swiss and French regulators.

His experience spans a number of areas. He has worked on pre- and post-acquisition due diligence for a number of multinational corporations. He has provided damages modelling and prepared expert reports relating to a dispute involving the acquisition of a major financial institution. He has advised on trust fund and restitution work for the International Criminal Court, involving all aspects of document and evidence management, reparation processes, asset identification and seizure.

After graduating from University College London, Mr Duthie worked for two years as a steel trader in Hong Kong and China. He then moved to the investment banking division of Deutsche Bank/Morgan Grenfell, where he focused on infrastructure finance and structured trade finance.

Fulbright & Jaworski LLP
85 Fleet Street, London EC4Y 1AE
Tel +44 20 7832 3600
Web www.fulbright.com

Lista M Cannon
Partner
Email lcannon@fulbright.com

Lista Cannon is a Partner in the global disputes and investigations practice and based in Fulbright's London office. She is Co-Chair of the firm's international investigations group, and Co-Chair of Fulbright's international trade and sanctions group. She is also the Managing Partner of Fulbright's London office.

Ms Cannon, who in 2006 was listed by the *Financial Times* as "one of the 16 most innovative lawyers in the UK who has made a significant contribution to international regulatory investigations", is dually qualified to practice in England & Wales and New York. In 2011, from a nominees list of leading UK litigation practitioners, she won the 'Best in Litigation' award at the inaugural *International Financial Law Review* (IFLR) Women in Business Awards.

Ms Cannon has extensive experience of representing multinational corporations, governments and financial institutions in a range of commercial disputes and transnational regulatory investigations, in the context of which she has gained significant expertise in handling bribery and corruption issues and related litigation.

Ms Cannon has advised international corporations in complex multi-jurisdictional investigations involving a range of regulators, including the US DOJ, the UK SFO, HM Revenue and Customs, and the FSA.

She was seconded to the Securities Investment Board (now FSA) as acting head of enforcement during its transition to the FSA. Ms Cannon has advised clients in arbitration and ADR proceedings, and represents major law and accountancy firms in civil and regulatory proceedings.

Fulbright & Jaworski LLP
Market Square, 801 Pennsylvania Avenue, NW
Washington DC 20004-2623
Tel +1 202 662 0200

Richard C Smith
Partner
Email rcsmith@fulbright.com

Richard Smith is a Partner in Fulbright's Washington DC office. He is Co-Chair of Fulbright's international investigations group and Chair of the firm's global white-collar crime and government investigations group.

Mr Smith advises multinational corporations, governments and financial institutions in a range of transnational regulatory investigations and related litigation. He is a leading practitioner in Foreign Corrupt Practices Act matters. He was the former Acting Chief and Principal Deputy Chief for Litigation in the Fraud Section of the US DOJ, Criminal Division. Here, he supervised the

litigation activities of all trial attorneys in the investigation, indictment and trial of criminal matters involving FCPA violations, money laundering, conspiracy, obstruction of justice, false books and records, and more.

He has over 20 years' trial experience, handling more than 100 criminal cases in state and federal courts throughout the US. While at the DOJ, Mr Smith tried the first cases prosecuted under the Sarbanes-Oxley statute and was instrumental in executing a new strategy to quickly investigate and prosecute corporate fraud matters.

A graduate of the University of Florida, he is admitted to practise law in the District of Columbia, Florida, Maryland and before the US Court of Appeals for the Fifth Circuit and the District of Columbia Court of Appeals.

Kingsley Napley LLP
Knights Quarter, 14 St John's Lane, London EC1M 4AJ
Tel +44 20 7814 1200
Web www.kingsleynapley.co.uk

Stephen Gentle
Partner
Email SGentle@kingsleynapley.co.uk

Stephen Gentle specialises in assisting corporate and individual clients in complex fraud and financial regulatory matters, frequently with multi-jurisdictional aspects. He has expertise in corruption and bribery matters (generally with an overseas focus) and FSA investigations and proceedings (with a particular emphasis on insider dealing, market misconduct matters and international regulatory issues).

He is experienced in Office of Fair Trading investigations, and money laundering prevention, investigations and prosecutions (he is a member of the Law Society Money Laundering Task Force).

His international criminal practice covers extradition proceedings, sanctions breaches and mutual legal assistance requests where he acts for individuals, corporations and governments.

Alongside his fraud practice, Mr Gentle maintains a general crime practice and he is also one of four lawyers in the firm who represent members of the Chief Police Officers' Staff Association facing internal disciplinary inquiries. In common with other members of the team, he is frequently involved in advising members of government agencies in sensitive inquiries where independent expertise in criminal law is required.

In addition to advising in criminal and financial services cases, Mr Gentle has experience of public and administrative law in cases such as the judicial review of decisions leading to deaths in custody, extradition and mutual legal assistance matters.

Elly Proudlock
Solicitor
Email eproudlock@kingsleynapley.co.uk

Elly Proudlock is a solicitor at Kingsley Napley, where she qualified in 2008. She specialises in general and business crime and has a particular interest in cartels, having been part of the team that successfully defended the first contested OFT prosecution under the Enterprise Act 2002.

Ms Proudlock acts for both suspects and witnesses in SFO and FSA investigations. She undertakes regulatory work in addition to her criminal practice, prosecuting cases on behalf of the Security Industry Authority and representing members of the Chief Police Officers' Staff Association in disciplinary matters.

Kirkland & Ellis International LLP
30 St Mary Axe, London EC3A 8AF
Tel +44 20 7469 2000
Web www.kirkland.com

Chris Colbridge
Partner, London
Email chris.colbridge@kirkland.com

Christopher Colbridge is a Partner in, and heads, the firm's international litigation and arbitration group in London. Prior to joining Kirkland &

Ellis, he was a partner in, and head of, the international arbitration and litigation group at Shearman & Sterling LLP in London.

He has particular experience in conducting cross-border white-collar crime investigations. In this regard, he has extensive experience in advising multinational corporations and dealing with prosecuting authorities around the world in the context of complex cross-border white-collar crime investigations.

In addition, Mr Colbridge has represented multinational corporations, governments and government-owned entities in international arbitration and litigation cases around the world.

A graduate of King's College London and the Sorbonne in Paris, he is both a solicitor and admitted to the Paris bar.

Mr Colbridge has been cited as a leading white-collar crime lawyer in the Legal 500. His team has been described as having "impressive depth of experience in corporate crime matters".

Harkiran Hothi
Partner, London
Email harkiran.hothi@kirkland.com
Harkiran Hothi is a Partner in the firm's international litigation and arbitration group in London, where she practises in white-collar crime, international arbitration and litigation.

Ms Hothi has extensive experience in both conducting and advising multinational clients on all aspects arising from complex cross-border white-collar crime investigations. In addition, she has represented clients in both institutional and ad hoc arbitrations around the world. She is a graduate of University College London.

Chiraag Shah
Partner, London
Email chiraag.shah@kirkland.com
Chiraag Shah is a Partner in the firm's international litigation and arbitration group in London. He has represented clients in both institutional and ad hoc arbitrations around the world. He is dual qualified (in Kenya and England and Wales) and has advised clients on fraud and corruption-related matters and investigations both in the UK and Kenya. He is a graduate of the London School of Economics.

Kobre & Kim LLP

60 Gresham Street, London EC2V 7BB
Tel +44 20 3301 5704
Web www.kobrekim.com

Robert W Henoch
Partner
Email robert.henoch@kobrekim.com
Robert Henoch is a Partner at Kobre & Kim, a litigation specialist firm with more than 70 professionals, including 13 former US government lawyers. Kobre & Kim has offices in London, New York, Hong Kong, Washington DC and Miami. Mr Henoch is based in the firm's London office.

Mr Henoch focuses his practice on the representation of European-based clients in US government and regulatory investigations. He is often retained to conduct confidential internal investigations on behalf of executive boards and committees of international public and private companies as a result of allegations concerning accounting fraud, securities, money laundering and various other laws with international applications.

Mr Henoch also has extensive experience advising and representing clients in investigations and prosecutions conducted by the US DOJ, the SEC, the Commodity Futures Trading Commission and various state Attorney General offices.

Prior to joining Kobre & Kim, he served for over five years as an Assistant US Attorney and supervisor in the Criminal Division of the US Attorney's Office for the Eastern District of New York, as well as an Assistant District Attorney in the New York County District Attorney's Office for over nine years. Mr Henoch also served in the US Army and US Army Reserves for over 23 years, and left the service as a Lieutenant Colonel.

Mr Henoch received a JD from George Washington University and a BA from the Honors College at the University of Michigan.

Kobre & Kim LLP
1919 M Street, NW Washington DC 20036
Tel +1 202 664 1936
Web www.kobrekim.com

Brad H Samuels
Associate
Email brad.samuels@kobrekim.com

Brad Samuels is an Associate with Kobre & Kim, focusing on government enforcement and internal investigations, with a specific emphasis on the financial services industry. He is often retained by multinational companies and executives in investigations involving accounting fraud, money laundering, corruption, bid rigging and anti-competitive conduct, among other issues.

Prior to joining Kobre & Kim, Mr Samuels practised at McKenna Long & Aldridge LLP, where he represented clients in a wide range of complex civil and commercial litigation, government litigation, anti-trust litigation and white-collar litigation matters.

Mr Samuels received his JD from Georgetown University Law Center and a BA from American University.

Linklaters LLP
One Silk Street, London EC2Y 8HQ
Tel +44 20 7456 2000
Web www.linklaters.com

Nicole Kar
Partner
Email nicole.kar@linklaters.com

Nicole Kar is a specialist in EC and UK cartel enforcement. She advised the immunity applicant in the global marine hoses cartel, which resulted in the Office of Fair Trading's first criminal cartel prosecution and which involved unprecedented co-operation between the OFT and the US Department of Justice.

She has also advised clients in relation to the OFT's investigation into alleged collusion between suppliers and retailers of groceries (closed without a finding of infringement), and the OFT investigation into dairy retail price initiatives – as well as groundbreaking UK Court of Appeal litigation in relation to the copper fittings cartel.

Ms Kar has written extensively on competition law and in particular cartel enforcement. She is co-author of the UK chapter of Kluwer Law International's *European Cartel Digest*. Her other recent publications include 'Criminal Cartel Enforcement – More Turbulence ahead? The Implications of the BA/Virgin Case', *Competition Law Journal* (Issue 3, 2010), and 'Competition Disqualification Orders', Practical Law Company (August 2010, Volume XXI, Number 7).

Kirsten Donnelly
Associate
Email kirsten.donnelly@linklaters.com

Kirsten Donnelly is a competition law specialist who advises on all aspects of UK and EU competition law. She has advised clients in relation to: the OFT's investigation into bid-rigging in the construction industry, including successful appeals to the Competition Appeal Tribunal, which resulted in substantial fine reductions; as well as investigations into alleged collusion between suppliers and retailers of groceries, and potential anti-competitive agreements in relation to certain generic medicines.

Ms Donnelly also advised a major international airline in respect of the investigation into the alleged price-fixing cartel in the provision of air freight services. This was an alleged multi-jurisdictional cartel and was being investigated by a number of competition authorities around the world, including the EC.

Satindar Dogra
Partner
Email satindar.dogra@Linklaters.com
Satindar Dogra specialises in fraud investigations and is at the forefront of the firm's bribery and corruption work. He was part of the CBI and International Criminal Court (ICC) working groups commenting on the Bribery Act 2010 and related Ministry of Justice guidance.

Mr Dogra is currently advising a number of clients on their policies and procedures in light of the Bribery Act and has defended clients in a number of high-profile SFO and DOJ investigations.

Jane Larner
Managing Associate
Email jane.larner@linklaters.com
Jane Larner is an experienced professional support lawyer in the firm's litigation practice, with a particular interest in bribery, corruption and white-collar crime. She took part in the CBI working group commenting on the Bribery Act 2010 and MoJ guidance.

Ms Larner has also presented seminars to both lawyers and City organisations on the effect and implications of the Bribery Act.

Christopher Kerrigan
Associate
Email christopher.kerrigan@linklaters.com
Christopher Kerrigan is an Associate in the firm's litigation practice. He has advised a number of clients on the effect and implications of the Bribery Act 2010, with a particular focus on its extra-territorial scope.

Miller & Chevalier, Chartered

655 15th St, NW, Suite 900, Washington DC 20005
Tel +1 202 626 5800
Web www.millerchevalier.com

Matthew Reinhard
Member
Email mreinhard@milchev.com
Matthew Reinhard is a Member of Miller & Chevalier, where he practises in the firm's litigation department, with an emphasis on white-collar criminal defence. Mr Reinhard specialises in conducting internal investigations and representing corporate and individual clients before federal law enforcement agencies.

Mr Reinhard's practice includes conducting international internal investigations relating to potential violations under the US Foreign Corrupt Practices Act, and conducting compliance-related due diligence of targets in mergers, acquisitions, joint ventures and other business partnerships. He has conducted a number of internal investigations for corporations in potentially sensitive areas, including employee harassment, internal fraud, and breach of fiduciary duty by corporate officers.

Mr Reinhard is a graduate of the University of Iowa College of Law. Following graduation, he was a law clerk to Carolyn Dineen-King, Chief Judge of the United States Court of Appeals for the Fifth Circuit.

Morrison & Foerster (UK) LLP

CityPoint, One Ropemaker Street, London EC2Y 9AW
Tel+44 20 7920 4000
Web www.mofo.com

Kevin Roberts
Partner
Email kroberts@mofo.com
Kevin Roberts is a Litigation Partner in the London office of Morrison & Foerster, specialising

in regulatory compliance and investigations, and white-collar crime. He advises corporations and individuals on money laundering investigations and compliance, corruption, tax investigations, fraud and FSA investigations and enforcement. He assists companies in respect of internal investigations, asset recovery, and corporate governance and compliance with regulation and legislation.

Mr Roberts is noted in the UK Legal 500 for his work on the generic drugs cartel prosecution, the largest prosecution ever brought by the SFO in the UK, with further comments that: "His conduct and advice are of the highest quality" and "his preparation and mastery of complex issues in a case are second to none, as are his judgement and tactical ability".

Mr Roberts is a frequent speaker on money laundering, confiscation and asset recovery and is a contributing author to the leading texts, 'Smith, Owen and Bodnar on Asset Recovery' and 'International Asset Tracing in Insolvency'.

OECD

Centre for Tax Policy and Administration, OECD, 2 rue André Pascal – 75775 Paris Cedex 16
Tel + 33 1 45 24 88 48
Web www.oecd.org/ctp/taxcrimes

Brian McAuley
Policy Adviser, International Co-operation
Email brian.mcauley@oecd.org
Brian McAuley works in the OECD's International Co-operation and Administration Division at the OECD headquarters in Paris. His work includes promoting a 'whole of government' approach to tax crimes and other financial crime, including improving co-operation between tax administrations and other agencies such as anti-money laundering authorities and law enforcement. He also facilitates events on the effective exchange of information for tax purposes, and advises on the OECD's harmful tax practices project.

Mr McAuley previously worked for more than 30 years in the UK Inland Revenue and UK Treasury. His international tax policy work included negotiating tax treaties and tax information exchange agreements, but he also has worked on improving the efficiency and effectiveness of tax systems through organisation and process redesign, application of quality systems and use of information technology.

He has worked for the French government on quality improvement in tax and other areas.

OLAF– European Anti-Fraud Office

European Commission, B-1049 Brussels
Tel +32 2 299 5946
Web ec.europa.eu

Johan Khouw
Head of Unit Fraud Prevention and Intelligence
Email johan.khouw@ec.europa.eu
Johan Khouw has been Head of the Fraud Prevention and Intelligence Unit within OLAF since 2006. He is responsible for the financial and administrative follow-up of OLAF investigations (direct expenditure, external aid and structural actions), fraud proofing, strategic intelligence, analysis and management of irregularity notifications from EU member states.

Mr Khouw joined the European Commission in 2000 as a principal administrator for OLAF responsible for preparing legislative proposals and giving legal advice on the protection of the European Community's financial interests. He became head of unit in OLAF in 2002.

Before joining the Commission, Mr Khouw worked in various functions within the Dutch central public administration:

- Ministry of Justice as a senior policy adviser within the Directorate-General for International Affairs and Migration, and as a senior legal adviser within the Directorate-General for Police.
- Ministry of Agriculture, Nature Management and Fisheries, as a senior legal adviser.
- Ministry of Finance, Directorate-General for

Fiscal Affairs and the Customs Department, as an administrator and junior Customs inspector.

A Dutch national, Mr Khouw holds a degree in Dutch civil law and international law from the University of Leiden.

Winfried Kleinegris
Head of Sector Intelligence Direct Expenditures
Email winfried.kleinegris@ec.europa.eu
Winfried Kleinegris is Head of Sector Intelligence Direct Expenditures and Fraud Rates within OLAF. He is responsible for a small sector that carries out risk analyses on the European Union's direct expenditures in order to identify the threats and vulnerabilities to which the EU is exposed in relation to irregularities and fraud.

Mr Kleinegris joined the European Commission in 1995 and began by working for the Social Statistics Unit at the European Statistics Office (Eurostat) in Luxemburg. In 1996, he joined the Commission's service responsible for employment and social policies to work in the areas of social security systems for migrant workers and the evaluation of the EU's policies, in particular European Social Fund interventions.

From 2001 to 2007, Mr Kleinegris worked in the Rail Transport and Interoperability Unit of the Commission's Transport and Energy General Directorate, where he dealt with the monitoring of rail market developments and the opening of the market for international rail passenger services. He also drafted the proposal for rail passengers' rights, which was adopted in 2007. In April 2007, he joined OLAF as strategic intelligence analyst for direct expenditures.

Before joining the Commission, he worked for almost ten years in the private sector (food retail distribution, industry association) and the public sector (education, social security) in the Netherlands and France.

Mr Kleinegris holds a degree in European Community law from the University of Lyon and a degree in linguistics from the University of Tilburg (Netherlands).

O'Melveny & Myers LLP
1625 Eye Street, NW Washington DC 20006
Tel +1 202 383 5300
Web www.omm.com

Greta Lichtenbaum
Partner
Email GLichtenbaum@OMM.com
Greta Lichtenbaum is a Partner at O'Melveny & Myers in Washington DC. Her practice principally relates to regulations governing international business transactions and trade.

Ms Lichtenbaum represents and advises clients in matters related to US economic sanctions, export controls, anti-boycott, foreign investment, the Foreign Corrupt Practices Act, Customs, and trade laws and agreements.

In addition to advising clients on the application of these laws to ongoing business, she assists them in developing corporate compliance programmes, conducts internal investigations relating to potential violations, and represents companies before relevant agencies in connection with licence requests and enforcement proceedings.

Described as "a well-recognized export controls expert", Ms Lichtenbaum is ranked in Tier 1 by both *Chambers USA* and *Chambers Global*. She is a frequent speaker on legal issues at business groups and bar associations.

She received her law degree from Harvard University in 1990.

O'Melveny & Myers LLP
Warwick Court, 5 Paternoster Square, London EC4M 7DX
Tel +44 20 7088 0000
Web www.omm.com

James Barratt
Counsel
Email jbarratt@OMM.com
James Barratt is a Counsel in O'Melveny & Myers' London office. He advises clients on compliance with economic sanctions and export

controls regulations. In addition, Mr Barratt's practice covers international arbitration, white-collar defence, corporate investigations and complex litigation.

Mr Barratt has advised clients in the oil and gas and financial services industries on the scope of the European Union economic sanctions regarding Iran, Libya and Syria. He has also represented and advised clients on the impact of the UK Bribery Act 2010 and the disclosure obligations under the UK Proceeds of Crime Act 2002. In addition, Mr Barratt has conducted several internal investigations in relation to the Foreign Corrupt Practices Act.

Mr Barratt is a specialist international arbitration practitioner and has represented clients in numerous cases under all leading arbitral rules (including ICC and LCIA), as well as in ad hoc arbitrations at various seats (including London, Paris, Geneva, Vienna, Hong Kong and New York).

Prior to joining private practice, he was a barrister at a leading set of chambers specialising in criminal and civil fraud, asset tracing, confiscation and money laundering, and appeared as the sole or joint advocate in numerous trials.

Hayley Ichilcik
Associate
Email hichilcik@omm.com

Hayley Ichilcik is an Associate in O'Melveny & Myers' London office. She advises clients in matters related to UK and European regulatory regimes, including trade sanctions and anti-bribery laws. Ms Ichilcik has advised clients in the oil and gas and financial services industries on the scope of the European Union economic sanctions regarding Iran, Libya and Syria. She has also represented and advised clients on the impact of the UK Bribery Act 2010 and conducted internal investigations in relation to the Foreign Corrupt Practices Act.

In addition, her practice focuses on advising clients on cross-border dispute resolution by way of arbitration or High Court litigation. Ms Ichilcik has acted in arbitrations under the LCIA, ICC, VIAC and ICDR rules.

PricewaterhouseCoopers LLP
Plumtree Court, London, EC4A 4HT
Tel +44 20 7583 5000
Web www.pwc.co.uk

Tracey Groves
Partner
Email tracey.groves@uk.pwc.com

Tracey Groves has 20 years' consulting experience helping clients successfully implement strategic change in the areas of fraud, corruption and business ethics, regulatory compliance and behavioural risk. She is a specialist in improving organisational effectiveness in behavioural risk management across the area of economic crime. Her clients are made up of a portfolio from both the public and private sectors, including working with global clients in financial services, aerospace and defence, media and entertainment, automotive, manufacturing and soft drinks, among others.

Ms Groves is part of the PwC governance, risk and compliance leadership team leading the design, development and implementation of global fraud, corruption and business ethics remediation compliance frameworks for clients, and she sits on the PwC Ideas Engine on Trust for the UK firm. She led a PwC survey in 2010 on 'Tone from the Top' and published an external report that challenged whether leaders are just paying lip service to ethics.

Among her many client projects, Ms Groves has led business-conduct framework and remediation programmes for addressing bribery, corruption and behavioural risk management issues on FCPA matters and in preparation for the UK Bribery Act. She has deep experience in the behavioural and cultural challenges arising from implementation of global ethics and compliance remediation programmes, and knowledge of the underpinning tools and levers to drive tangible change.

Ms Groves is a qualified chartered accountant (Institute of Chartered Accountants in England and Wales, 1994) and she completed the organisation development certificate at the NTL

(National Training Laboratories) Institute for Applied Behavioural Science in 2008.

Harry Holdstock
Senior Associate
Email harry.g.holdstock@googlemail.com
Harry Holdstock has four years' experience of working for the PwC forensic services and assurance practices in London. He has specific expertise in a number of complex areas of financial services regulation, including anti-money laundering and market abuse. He is interested in all business ethics matters, including the practical implications of designing and embedding effective whistleblowing arrangements.

Mr Holdstock has also contributed to a number of fraud risk assessments, and anti-bribery and corruption and compliance transformation engagements for a variety of clients.

Andrew Gordon
Partner
Email andrew.gordon@uk.pwc.com
Andrew Gordon is Head of Investigations within the forensic services group of Pricewaterhouse-Coopers, based in London. He has over 18 years' experience as a forensic accountant and has been a partner for 12 years. His forensic team comprises over 150 dedicated partners and staff in the UK, supported by forensic technologists who provide data mining and electronic discovery services.

Mr Gordon has managed many complex and high-profile engagements, including: investigations on behalf of both the Volcker and Eagleburger Commissions into Holocaust victims' funds at, respectively, Swiss banks and European insurers; US SEC and/or DOJ investigations in the UK and Europe across a variety of industries and countries; and FSA, OFT and SFO investigations in the UK. He was recently engaged by the Mayor of London, Boris Johnson, as the independent forensic accounting adviser to the Mayor's Forensic Audit Panel.

Mr Gordon has experience across a number of industries, including financial services (both banking and insurance), retail, mining, oil and gas, transportation, utilities, industrial products, technology, property, telecoms and healthcare.

Andrew Clark
Partner
Email andrew.clark@uk.pwc.com
Andrew Clark leads the Financial Crime practice in the UK and is an expert in fraud, anti-money laundering, data compromise, corruption and market abuse. He has led many complex and international investigations involving a range of regulatory and investigative agencies. Mr Clark has been a certified fraud examiner since 1998.

He is a specialist in the investigation of fraud, financial crime and management impropriety, with extensive experience of investigations within the financial services sector, conducting investigations for regulators, criminal authorities and a range of authorised institutions.

Mr Clark spent two years in the Special Investigations Unit at the Bank of England, providing advice on appropriate courses of action to be taken regarding matters of fraud or dishonesty relating to authorised institutions.

He was seconded to the SFO as a forensic accountant and appointed as an investigator by the Department of Trade and Industry under Section 447 of the Companies Act 1985. He has also worked for a number of UK police fraud squads.

Tony Parton
Partner
Email tony.d.parton@uk.pwc.com
Tony Parton is a Partner in the UK forensic services group, specialising in corporate investigations. He has 30 years' experience of advising UK and overseas companies on fraud investigations, including financial statement fraud, extractive fraud, conflicts of interest and bribery and corruption cases. He has also worked for the firm in Africa and Asia and regularly investigates cases overseas. He has a particular focus on advising companies and private equity houses on M&A anti-bribery compliance due diligence.

Tracy Gill
Senior Manager
Email t.gill@uk.pwc.com
Tracy Gill is a Senior Manager in the firm's Manchester office, where she has gained forensic accounting experience over the past 12 years. She has gained that experience in a number of areas, including complex accounting investigations, shareholder transaction disputes, licensing management examinations and assisting on expert witness work for professional negligence and various contract-related disputes. In particular, she has been involved in a number of SEC investigations into alleged accounting irregularities, as well as in FCPA compliance reviews at international US-listed companies.

Ms Gill holds a BSc in mathematics from Lancaster University and is a member of the Institute of Chartered Accountants in England and Wales.

Robert Wilson
Senior Manager
Email robert.e.wilson@uk.pwc.com
Robert Wilson is a Senior Manager in the investigations team at PwC forensic services. He has over 17 years' experience in complex fraud investigations, business strategy and change management.

Mr Wilson rejoined PwC in May 2009, having spent the previous five years with the SFO, where he led multi-jurisdictional investigations into corporate fraud and corruption and was on secondment for six months at the Serious Organised Crime Agency.

The majority of Mr Wilson's work involves helping clients deal with criminal and other investigations. He is currently helping a major international client respond to police inquiries and another client deal with whistleblower allegations of corruption.

Other recent experience includes a regulatory inquiry for a general insurance company, investigations into fraud in the financial services sector, alleged malpractice by directors in breach of fiduciary duties, and a regulatory fraud investigation in the telecommunications sector.

Mr Wilson works closely with PwC's data analytic and information security experts to quickly get to grips with the situation, investigate the matter efficiently and take appropriate remedial action.

Marie-Alice Hofmaier
Manager
Email marie-alice.hofmaier@uk.pwc.com
Marie-Alice Hofmaier is a Manager in PwC's forensic services department who specialises in anti-money laundering (AML) solutions. She has wide experience of AML remediation projects, including training staff to perform 'know your customer' (KYC) reviews, delivering technical advice on KYC, politically exposed persons, sanctions and monitoring, and project managing teams. She led the review of the KYC documentation for over 1,500 clients at a large financial institution.

Ms Hofmaier also has extensive experience of regulatory investigations both in relation to AML and wider compliance issues, including investigations requested by the FSA. She has worked on a number of AML due diligence assignments, involving high-level reviews of client AML frameworks, detailed reviews of samples of customer files, and preparing reports for the central due diligence teams.

She has carried out financial crime investigations and regulatory investigations both for financial services clients and in other industries.

Mark Anderson
Director
Email mark.r.anderson@uk.pwc.com
Mark Anderson is a Director in forensic services who leads PwC's global corporate intelligence practice. He has over 12 years' experience of undertaking complex, multi-jurisdictional intelligence-gathering and investigations projects, much of these in emerging markets.

He has managed over 200 integrity and anti-

corruption due diligence projects for a wide range of clients, including financial institutions and private equity firms, examining issues such as reputation, corruption, and criminal and unethical behaviour in third-party relationships.

In addition, Mr Anderson has worked on the two largest-ever international commercial anti-corruption investigations and remediation programmes. He continues to work with a number of international private equity and other clients on the design and embedding of anti-bribery and corruption procedures, with a particular focus on third parties.

Reed Smith LLP

The Broadgate Tower, 20 Primrose Street, London EC2A 2RS
Tel +44 20 3116 3000
Web www.reedsmith.com

Charles M Hewetson
Partner
Email chewetson@reedsmith.com

Charles Hewetson is a former head of the commercial disputes group at Richards Butler and a former vice chair of Reed Smith's global litigation department. He specialises in regulatory investigations and is Head of Reed Smith's global regulatory enforcement team in London.

Mr Hewetson regularly advises clients in connection with complaints and proceedings brought by domestic and international regulators and prosecuting authorities, and in connection with internal investigations arising from the same.

He gives regular presentations and training on regulatory issues, including the Bribery Act 2010.

Tom Webley
Associate
Email twebley@reedsmith.com

Tom Webley is an Associate in Reed Smith's commercial disputes group and a member of Reed Smith's global regulatory enforcement team in London.

Mr Webley specialises in regulatory investigations and financial services disputes, as well as dealing with intellectual property and general commercial litigation. Much of his work involves multi-jurisdictional disputes and investigations, including working with colleagues in the US on investigations by the US authorities.

Reynolds Porter Chamberlain LLP

Tower Bridge House, St Katharine's Way, London E1W 1AA
Tel +44 20 3060 6000
Web www.rpc.co.uk

Steven Francis
Partner
Email steven.francis@rpc.co.uk

Steven Francis leads RPC's regulatory team. He advises on all aspects of contentious regulation, in particular as it affects insurance businesses, banks and broking and securities firms. Formerly a member of the management team of the FSA's Wholesale Enforcement Division, he managed large insider dealing and market abuse investigations and cases against a range of financial services institutions concerning breaches of the FSA's rules and principles.

On insider dealing investigations, Mr Francis has acted both for those defending and those prosecuting allegations, as well as for financial services firms conducting internal investigations into suspected leaks of price-sensitive information. He was the project manager on significant dawn raid operations conducted by the FSA and the City of London Police, and he has conducted numerous PACE and compulsion interviews for state agencies and prosecuting authorities. Mr Francis has also worked with overseas authorities, such as the US DOJ, on insider dealing investigations.

Mr Francis has also helped an energy and commodities trading firm to implement systems and controls to comply with FSA rules and other regulatory laws relating to bribery and

corruption, internal fraud and financial sanctions. He speaks regularly on financial regulation and business crime and has written widely on the subject for the general and specialist press.

Richard Burger
Partner
Email richard.burger@rpc.co.uk
Richard Burger is a Partner in RPC's regulatory team with substantial experience advising corporates and individuals across the spectrum of regulation. An experienced corporate crime lawyer, he has defended in serious business crime cases including insider dealing, bribery, conspiracy to defraud and US securities fraud with related US extradition proceedings, investigated/prosecuted by the SFO, the FSA, the Crown Prosecution Service and US law enforcement agencies.

Mr Burger was previously a lawyer in the Enforcement Division of the FSA, where he was involved in investigating market abuse/insider dealing and compliance system failures. He was the case lawyer in the FSA's first published case of market abuse.

Since returning to private practice, he has advised on contentious and non-contentious financial regulation and compliance, been seconded to a Lloyd's insurer as its head of compliance, undertaken numerous internal investigations, conducted private prosecutions on behalf of regulators, professional bodies and commercial organisations, and defended professional accountants in disciplinary proceedings.

Mr Burger is a chartered member of the Chartered Institute for Securities & Investment and sits on the CISI's Disciplinary Panel. He is also a member of the editorial board of the *Journal of Financial Regulation and Compliance*.

Saunders Law Ltd
Essex Hall, 1-6 Essex Street, London WC2R 3HY
Tel +44 20 7632 4300
Web www.saunders.co.uk

Stephen Gilchrist
Solicitor and Director
Email gilchrist@saunders.co.uk
Stephen Gilchrist is a Solicitor and Director of Saunders Law, practising in business crime and regulatory law.

Mr Gilchrist qualified in 1974 and has both defended and advised numerous individual and corporate clients in criminal proceedings and in civil proceedings instituted by various industry and professional regulatory bodies

Building on his criminal defence background, he now has a leading practice in fraud, financial services litigation, health and safety, and professional and sports regulation. He relishes the new challenges thrown up by a world seemingly obsessed with regulation.

Serious Fraud Office
Elm House, 10-16 Elm Street, London WC1X 0BJ
Tel +44 20 7239 7272
Web www.sfo.gov.uk

Richard Alderman
Director
Email richard.alderman@sfo.gsi.gov.uk
Richard Alderman is the Director of the Serious Fraud Office. Before joining the SFO, he held a number of senior roles in the Inland Revenue/HM Revenue and Customs. These roles gave him extensive experience of very complex financial investigations and criminal prosecution. As Director of the Special Compliance Office, for example, he was responsible for all of the Inland Revenue's criminal investigations.

Mr Alderman has also held other key roles within the government legal service. In 2002 he

was invited by the Attorney General and the Treasury Solicitor to work with the Home Office to set up the Assets Recovery Agency, subsequently becoming its first Legal Director. And he worked closely with the law officers when he was seconded to their Legal Secretariat between 1991 and 1993.

Mr Alderman is a barrister. He is a member of the Executive Committee of the International Association of Anti-Corruption Authorities, and the World Economic Forum's Global Agenda Council on Anti-Corruption. He frequently speaks at international conferences on issues such as the UK Bribery Act 2010 and economic crime.

Society of Corporate Compliance and Ethics
6500 Barrie Road, Suite 250, Minneapolis, MN 55435
Tel +1 952 933 4977
Web www.corporatecompliance.org

Roy Snell
Chief Executive
Email Roy.Snell@corporatecompliance.org

Roy Snell is the Chief Executive, Co-Founder and first President of the 9,000-member Society of Corporate Compliance and Ethics and Health Care Compliance Association. He has written over 100 articles, edited two manuals and three magazines, and published a book for compliance professionals. He is an outspoken advocate for compliance professionals and fierce promoter of compliance programmes.

Mr Snell is a frequent speaker in the US and has spoken in Brazil and for the United Nations in Warsaw. He has been interviewed or published by agencies and publications such as Reuters, *The Wall Street Journal, Forbes, BusinessWeek, EuropeanCEO*, *The European Business Review*, the *Financial Times* and *Ethical Corporation*.

He has worked with the enforcement community to encourage the recognition of businesses that implement compliance programmes, and has worked with compliance professionals from Russia, France, South Africa, Mexico and others to help promote compliance programmes internationally. He was named twice in Ethisphere's '100 Most Influential People in Business Ethics'.

Mr Snell is a former University of Wisconsin compliance officer, consultant for Deloitte and PricewaterhouseCoopers, and Mayo Clinic administrator. He is a certified Compliance and Ethics Fellow and has a Master's degree from St Mary's College in Minnesota.

Stroz Friedberg Ltd
Pinners Hall, 105-108 Old Broad Street, London EC2N 1AP
Tel +44 20 7448 0470
Web www.strozfriedberg.com

Vijay Rathour
Vice President, London
Email vrathour@strozfriedberg.com

As a Vice President at Stroz Friedberg's London office, Vijay Rathour supervises and works on an active caseload of digital forensic, cyber-crime response, and electronic disclosure assignments.

Prior to joining Stroz Friedberg, Mr Rathour practised law in the Enforcement and Financial Crime Division of the Financial Services Authority. In his role as a team lawyer, he provided legal analysis and strategic advice on the conduct of enforcement investigations into some of the highest-profile firms and individuals in the financial sector.

Mr Rathour has gained significant experience in managing the electronic disclosure process on a number of investigations and in drafting and responding to regulatory information requests, skilled persons reports and Data Protection Act and Freedom of Information Act requests. Previously he worked as a commercial litigator in private practice.

Mr Rathour received his LLB from Sheffield University and his LLM in international commercial law at the University of Nottingham

and the National University of Singapore. He was previously qualified as a barrister at the English bar.

Julian Parker
Managing Director, London
Email jparker@strozfriedberg.com
Julian Parker is a London-based Managing Director of Stroz Friedberg, where he oversees a significant caseload of assignments and develops strategic links to businesses and organisations in Europe, the US and around the world.

He has been instrumental in introducing the concept of digital forensics and e-disclosure to many UK law firms previously unfamiliar with the key issues at stake and the technology available to assist them. He has worked extensively not only with major UK law firms and other corporate entities, but also with investigation firms and regulatory agencies. He also manages a substantial number of due diligence investigations that span the globe.

His investigations experience was preceded by military service as an officer in the British Army. Mr Parker earned a BA in Arabic from the University of London's School of Oriental and African Studies.

He lectures internationally on computer forensics and digital evidence, and their importance in investigations and litigation.

Transparency International UK

CAN Mezzanine, 32-36 Loman Street, London SE1 0EH
Tel +44 20 7922 7906
Web www.transparency.org.uk

Chandrashekhar Krishnan
Executive Director
Email chandu.krishnan@transparency.org.uk
Chandrashekhar Krishnan joined Transparency International UK in September 2004. Prior to that, he was deputy director for strategic planning at the Commonwealth Secretariat. He co-ordinated the work of a Commonwealth Expert Group on Combating Corruption, which was endorsed by the 1999 Commonwealth Heads of Government meeting.

Mr Krishnan has expertise in international economic and sustainable development issues, including the challenges of good governance, combating corruption and poverty reduction. He has gained over 25 years' experience at Transparency International, the Commonwealth Secretariat and the United Nations.

He is a member of the Crown Agents Foundation Council and the expert Advisory Panel of the United Nations Association of the UK.

World Bank

1818 H Street, NW Washington DC 20433
Tel +1 202 473 1000
Web www.worldbank.org

Leonard Frank McCarthy
Vice President, Integrity
Email Lmcccarthy@worldbank.org
In June 2008, Leonard McCarthy was appointed by Robert B Zoellick, World Bank President, to serve as Vice President of the Integrity Vice Presidency (INT), whose mandate is to detect, deter and prevent fraud and corruption in Bank Group-supported activities. Under his leadership, INT focuses on promoting creative solutions in investigations, integrity due diligence, litigation, forensic audits and settlements, to solidify the lending environment and provide assurance to World Bank shareholders.

INT's newly created Preventive Services Unit analyses insights gained from investigations, and disseminates good practices to other Bank staff and governments in the form of structural precautions, fiduciary mechanisms and 'red flag' detection tools.

Prior to joining the World Bank Group, Mr McCarthy headed the Directorate of Special Operations (DSO) in South Africa, specialising in crime analysis, investigation, prosecution, forensic

accounting, asset forfeiture and civil litigation. During his tenure, the DSO successfully prosecuted many entities involved in financial crime, organised criminal enterprises, grand corruption, urban terror and money rackets. In addition, the DSO generated millions of rands destined for criminal restraint, and interdicted drugs and other contraband worth billions.

Previously, Mr McCarthy held the position of Director of Public Prosecutions in South Africa, to which he was appointed by the then president, Nelson Mandela.

He is a lawyer by profession and holds the following degrees: Baccalaureus Artium (BA), Bachelor of Law (B Juris), and LLB (Bachelor of Laws).

Stephen S Zimmermann
Director of Operations, Integrity Vice Presidency
Email Szimmermann@worldbank.org
Stephen Zimmermann is the Director of Operations for the World Bank's Integrity Vice Presidency. Mr Zimmermann directs a multi-disciplinary team of lawyers, investigators and analysts focusing on managing fraud and corruption in Bank-financed activities. He is also the World Bank Group focal point for the Agreement on Mutual Enforcement of Debarment Decisions among multilateral development banks.

Prior to joining the World Bank in 2009, Mr Zimmermann was chief of the Office of Institutional Integrity for the Inter-American Development Bank. He has also served as the interim chief of staff for the Independent Inquiry Committee into the United Nations oil-for-food programme.

From 1991 until 1999, Mr Zimmermann was an Assistant US Attorney in the District of Maryland. During his tenure as a federal prosecutor, he successfully prosecuted numerous complex cases involving corruption, financial fraud, tax evasion, healthcare fraud, securities fraud and money laundering. He has worked closely with federal law enforcement agencies including the FBI, the Internal Revenue Service, the US Customs Service, the Securities and Exchange Commission and the Food and Drug Administration.

He started his professional career as an attorney with Wilmer, Cutler & Pickering LLP. His practice involved matters including securities fraud, white-collar criminal work and a variety of commercial civil litigation.

Frank Anthony Fariello
Lead Counsel, Legal Vice Presidency
Email ffariello@worldbank.org
Frank Fariello, a graduate of Brown University and New York University School of Law, is currently Lead Counsel, Operations Policy, in the World Bank's Legal Vice Presidency (LEG). He is the LEG's primary focal point for the Bank's sanctions regime and governance and anti-corruption policies. In that capacity, he co-ordinated the recent comprehensive reforms of the Bank's sanctions process and advised the INT in connection with the Agreement on Mutual Enforcement of Debarment Decisions among multilateral development banks.

Prior to joining the Bank in 2005, Mr Fariello worked for nine years at the International Fund for Agricultural Development (IFAD) as senior counsel and subsequently as special adviser to the vice president. As a lawyer, he dealt with a broad variety of operational, administrative and policy matters including the legal aspects of IFAD's operations in Central America and South East Asia, as well as the simplification of its legal documentation (including the development of IFAD's 1998 General Conditions and new-model loan agreement).

Mr Fariello advised the vice president of IFAD on several policy initiatives including the development and adoption of a new grants policy, a performance-based allocation system and IFAD's anti-corruption policy, as well as corporate initiatives such as IFAD's Strategic Change Program. He was also a member ex officio of IFAD's Oversight Committee.

For the first ten years of his career, he practised corporate law, with an emphasis on international financial transactions, at a number of New York firms including Skadden, Arps, Slate, Meagher & Flom LLP.

Nicholas Yeo
Three Raymond Buildings, Gray's Inn, London WC1R 5BH
Tel +44 20 7400 6400
Web www.3raymondbuildings.com
Email Nicholas.Yeo@3raymondbuildings.com

Nicholas Yeo is a versatile advocate experienced in all aspects of criminal law and of civil litigation arising out of criminal law, particularly cases with a strong computer technology component.

He was instructed in the Court of Appeal and in the retrial in *Flook* (2010) (£113m drug importation), the leading case on third-party disclosure; and similarly in *Flynn* (2008) (armed robbery), the leading case on identification by voice; and again in the Court of Appeal in *Mintchev* (2011) (GBH) on the proper approach to the automatic deportation provisions in sentencing.

Mr Yeo is a specialist in the proceeds of crime, including civil forfeiture, money laundering and confiscation. He was instructed in the Court of Appeal in *Anwoir* (2009), a leading money laundering authority. He appeared for the appellant in *Perinpanathan* (CA) (2010) (costs in cash forfeiture proceedings), in which Lord Justice Goldring stated that he had argued the case with "conspicuous skill". He has dealt with numerous multi-million-pound confiscation cases, at hearing, certificate of inadequacy and enforcement stages.

Mr Yeo is experienced in fraud litigation in both criminal and civil matters. He is also knowledgeable in licensing, professional discipline, regulatory offending and extradition.