Data Protection Act 1998

Monetary Penalty Notice

Dated: 20 February 2015

Name: Staysure.co.uk Limited

Address: McGowan House, Waterside Way, The Lakes, Northampton, NN4 7XD

Statutory framework

---

1. Staysure.co.uk Limited is a data controller, as defined in section 1(1) of the Data Protection Act 1998 (the "Act") in respect of the processing of personal data and is referred to in this notice as "the data controller". Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

2. The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act"). By virtue of section 6(1) of the Act, the office of the Data Protection Registrar originally established by section 3(1)(a) of the 1984 Act became known as the Data Protection Commissioner. From 30 January 2001, by virtue of section 18(1) of the Freedom of Information Act 2000 the Data Protection Commissioner became known instead as the Information Commissioner (the "Commissioner").

3. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice on a data controller requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice but not exceeding £500,000. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. It should be read in conjunction with the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

Power of Commissioner to impose a monetary penalty

(1) Under section 55A of the Act the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the Act by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

Background

4. The data controller is a specialist online travel insurer offering multiple insurance products such as travel, health, life, holiday, home and car insurance to the general public.

5. Between 14 and 28 October 2013 the data controller's website was subject to an attack by someone exploiting a vulnerability in the JBoss Application Server on which its website server was based.

6. The attacker used this vulnerability to inject a malicious javascript webpage called "JspSpy" into the data controller's website. This created a backdoor to the web server allowing the attacker to remotely

view and modify website source code and query the website's backend database where customer data was being stored. It also enabled the attackers to open a command shell allowing them to remotely execute privileged operating system commands.

7. The vulnerability in the JBoss Application Server, and a software update to fix the issue, had been first published in 2010. A similar vulnerability and software update was subsequently published in 2013. However, the data controller did not have a formal process for reviewing and applying software updates and did not apply the available updates.

8. At the time of the attack, the data controller's database contained approximately three million customer records. Those records included customer name, date of birth, email address, postal address, phone number, payment card number, card expiry, card CVV, travel dates and destination(s) and medical screening responses data. Whilst all of this information was potentially at risk, the evidence suggests that only payment card data was targeted and downloaded.

9. Prior to June 2008 payment card numbers were held in a plain text format and unencrypted within the data controller's database along with the customer name, expiry dates and CVV number.

10. From June 2008 payment card numbers, but not CVV numbers, were encrypted. However, having gained access to the data controller's entire system, the attackers were able to identify the keys used in encrypting the data and then use these to decrypt the payment card numbers.

11. The data controller stored CVV numbers to assist with renewals of policies. In 2012 the data controller identified that CVV numbers should not have been stored and a decision was taken to delete them. However, as a result of human error the work to delete and cease storage of the CVV numbers was not completed.

12. Since 16 May 2012, 95% of all customer transactions were processed via a new separate and external system which removed the need to store card data on the web server. However, CVV data continued to be stored in relation to the remaining 5% of transactions until the breach was discovered.

13. At the time of the attack, a total of 110,096 live card details, relating to a total of 93,389 customers, stored on the old system were at risk of being accessed and used in fraudulent transactions.

14. The attack was discovered after the data controller was notified by its card acquirer of suspicious activity on customer accounts.

15. Multiple IP addresses are known to have accessed and downloaded customer data from the data controller's web server. There is evidence that attackers downloaded payment card data and used this information to carry out fraudulent transactions.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

16. The relevant provision of the Act is the Seventh Data Protection Principle which provides, at Part I of Schedule 1 to the Act, that:

    "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".

17. Paragraph 9 at Part II of Schedule 1 to the Act provides that:

    "Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to –

    (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

    (b) the nature of the data to be protected".

18. In deciding to issue this Notice of Intent, the Commissioner has considered the facts of the case and the deliberations of those within his office who have recommended this course of action. In particular, he has considered whether the criteria for the imposition of a monetary penalty have been met; whether, given the particular circumstances of this case and the underlying objective in imposing a monetary penalty, the imposition of such a penalty is justified; and whether the amount of the proposed penalty is proportionate.

Serious (S55A (1)(a))

19. The Commissioner is satisfied that there has been a serious contravention of the Seventh Data Protection Principle.

20. In particular, the data controller failed to take appropriate technical measures against the unauthorised or unlawful processing, or accidental loss, of personal data by:

    - Failing to have adequate policies and systems in place for checking, reviewing and applying available software security updates.

    - Storing payment card CVV numbers on its database in breach of the Payment Card Industry Data Security Standard.

21. The contravention is serious because these failings enabled an attacker to enter the data controller's systems and access unencrypted card data which is known to have been fraudulently used. The measures taken by the data controller did not ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or data loss, and the volume and nature of the data to be protected.

Likely to cause substantial damage or substantial distress (S55A (1) (b))

22. The Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress.

23. Active payment card data was obtained and there is evidence of fraud having taken place. Following the breach, over 5000 payment card details were reported to have been used in fraudulent transactions. However, losses arising were reimbursed by the banks. Therefore, not only was the contravention of a kind likely to cause substantial damage or distress, but there is evidence to suggest that it may in fact have caused distress.

24. The data subjects would also be likely to suffer from substantial distress on being informed that their personal data had been accessed

by an unauthorised third party and could have been further disclosed. The knowledge of this access alone is likely to cause substantial distress.

Knew or ought to have known that there was a risk that the contravention would occur and that it would be of a kind likely to cause substantial damage or distress (S55A (3)(a)(i) and (ii)).

---

25. The Commissioner is satisfied that section 55A(3) of the Act applies in that the data controller knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

26. The data controller should have been aware of the risks associated with any compromise of payment card and cardholder data due to the nature of the data being collected. The data controller was also aware of the Payment Card Industry Data Security Standard covering security related issues, and that there was a particular risk in storing CVV numbers.

27. Information about the security vulnerability in the JBoss Application Server, and the appropriate update to fix that vulnerability, was first published in the Common Vulnerabilities and Exposures List in 2010. Information about a similar vulnerability was published in 2013. The update was also made available via the software repositories of the Linux distribution in use by the data controller, namely Red Hat.

28. In the circumstances, the data controller knew or ought to have known that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as those outlined above.

29. Further, it should have been obvious to the data controller who was aware of the nature and amount of the personal data processed stored on the system, that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the data subjects.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

---

30. *Effect of the contravention*

- There is evidence that some of the personal data was used for fraudulent transactions.

31. *Behavioural issues*

- The data controller should have been aware of the vulnerability in 2010.

32. *Impact on the data controller*

- The data controller is a limited company so liability to pay a monetary penalty will not fall on any individual.

- The data controller has access to sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship.

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

---

33. *Nature of the contravention*

- The data controller's systems were subjected to a criminal attack.
- The data controller has not experienced any previous data or similar security breach that the Commissioner is aware of.

34. *Behavioural issues*

- The data controller was in the process of upgrading its IT infrastructure at the time of the breach.
- Voluntarily reported to the Information Commissioner's Office.
- The data controller has been co-operative with the Information Commissioner's Office.
- The data controller took remedial action to remove all payment card data from its systems.
- The data controller subsequently notified the data subjects of the security breach and provided a dedicated response team to assist customers together with a free Experian Data Patrol subscription for a period of six months.

Other considerations

35. The Fifth Data Protection Principle at Part I of Schedule 1 to the Act was also contravened in that payment card CVV numbers were stored on the data controller's systems for longer than was necessary.

36. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data stored on their information technology systems.

Notice of Intent

37. A notice of intent dated 18 December 2014 was served on the data controller. The Commissioner received written representations from the data controller in response to the notice of intent dated 27 January 2015. The Commissioner has considered those representations when deciding whether to serve a monetary penalty notice. In particular, the Commissioner has taken the following steps:

- reconsidered the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective which the Commissioner seeks to achieve by this imposition;
- ensured that the monetary penalty is within the prescribed limit of £500,000; and
- ensured that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory or public law duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible data controller.

Amount of the monetary penalty

38. The Commissioner considers that the contravention of the Seventh Data Protection Principle is very serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in

the sum of **£175,000 (one hundred and seventy five thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

39. In reaching this decision, the Commissioner considered other cases of a similar nature in which a monetary penalty had been imposed, and the facts and aggravating and mitigating features referred to above.

Payment

40. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 25 March 2015 at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

Early payment discount

41. If the Commissioner receives full payment of the monetary penalty by 24 March 2015 the Commissioner will reduce the monetary penalty by 20% to **£140,000 (one hundred and forty thousand pounds)**. However, you should be aware that the early payment discount is not available if you decided to exercise your right of appeal.

Right of Appeal

42. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

    a) the imposition of the monetary penalty and/or;

    b) the amount of the penalty specified in the monetary penalty notice.

43. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

44. Information about appeals is set out in Annex 1.

Enforcement

---

45. The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified within the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;

- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and

- the period for appealing against the monetary penalty and any variation of it has expired.

46. In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the 20th day of February 2015

Signed ……..

David Smith
Deputy Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (the "Tribunal") against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

d) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

e) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).