www.pdpjournal.com

ISSN 1473-3498

Privacy & Data Protection

Volume 7, Issue 4

March 2007

Headlines:

- Report on UK surveillance, p.14
- Bank sues retailer over data loss, p.15
- Complaint upheld over opt-out in text message, p.15
- Elle Macpherson privacy breach, p.15

Inside this issue:

Bank fined £1m for data security breach

The UK financial services regulator, the Financial Services Authority, has fined the country's largest building society £980,000 following the theft of an employee's laptop. The laptop contained customer data relating to some of its 11 million account holders.

The FSA has criticised the Nationwide Building Society for failing adequately to address the risk that customer data might be lost or stolen. The laptop was stolen from the home of a Nationwide employee who reported the theft but not the fact that the laptop contained such a significant amount of customer data. The employee then went on holiday for three weeks. During this period nothing was done to investigate what data the stolen laptop contained.

The FSA indicated that the Nationwide's risk assessment and security procedures were inadequate. The regulator specifically pointed to the fact that staff did not know what steps they were supposed to take in the event of such a breach. Policies were apparently inaccessible and staff were not adequately trained. The fact that no action was taken in the first three weeks after the breach increased the opportunity for the information to be misused (although there is no evidence of misuse).

The FSA particularly noted that the failures occurred in an environment of heightened awareness of information security issues.

"Nationwide is the UK's largest building society and holds confidential information for over 11 million customers," said Margaret Cole, director of enforcement at the FSA. "Nationwide's customers were entitled to rely upon it to take reasonable steps to make sure their personal information was secure," she added.

Businesses regulated by the FSA, whose remit includes the supervision of systems and controls of the businesses it regulates, will need urgently to reassess their data protection and data security risks.

(Continued on page 14)

Electronic health data—new regulation

The European Union's Article 29 Data Protection Working Party has adopted a working document on the processing of personal data relating to health in electronic health records ('EHR').

The document provides guidance on the interpretation of the applicable data protection legal framework for EHR systems and the data protection requirements for setting up EHR systems.

The paper includes recommendations for special safeguards within EHR systems which the Working Party regards as necessary to guarantee the data protection rights of patients and individuals.

In the UK, the working document will be received with some interest, as Tony Blair's government has been pressing ahead with a national IT system for the whole of the country's nationalised health service.

The Working Party provides recommendations on eleven topics where special safeguards within EHR systems are "particularly necessary" in order to guarantee the data protection rights of patients and individuals. These include:

- Respecting self determination
- Use of EHR for other purposes
- Organisational structure of an EHR system

(Continued on page 14)