Tougher enforcement for data breaches

Jun 30 2008 Bridget Treacy and Natalie Hunt

Bridget Treacy

Data breaches and data security concerns continue to hit the headlines, despite an increased awareness of security risks among companies that deal with personal data. The Financial Services Authority recently fined Merchant Securities Group Limited for poor data security practices. The company failed to adequately protect its customers from the risk of identity fraud. The FSA fined Merchant Securities £77,000 for having inadequate procedures for verifying the identities of customers who contacted the firm by telephone. Despite numerous headlines that relate to data security breaches and more active enforcement by regulators, it seems that firms remain slow to protect personal data.

Recent FSA enforcement action

In the last three years, the FSA has fined Norwich Union £1.26m, BNPP Private Bank £350,000, Nationwide £980,000 and Capita Financial Administrators £300,000 for security lapses which compromised customers' personal data and placed individuals at risk of identity theft. Despite the increased awareness of data security issues, and the FSA's own campaign to raise awareness of the risk of identity theft, some of the lapses in data security represent obvious oversights. It appears that Merchant Securities relied on inadequate, informal practices to verify the identity of customers who contacted the business by telephone. A member of staff was permitted to store unencrypted back-up tapes which contained customer data at their home.

Norwich Union was criticised for poor customer identification procedures while the regulator targeted BNPP and Capita for weaknesses in internal controls which were intended to prevent fraud. In each of these cases, the FSA sought to publicise its enforcement activity and, at least in the case of Nationwide, to emphasise that the level of fine it imposed was intended as a deterrent to others.

In April 2008, the FSA published its report, entitled "Data Security in Financial Services — Firms' controls to prevent data loss by their employees and third party suppliers" which urged regulated firms to change their attitude to data security. The report relates to financial services, although the recommendations and warnings are equally applicable to all organisations that handle personal data. Firms need to stop underestimating the risk of harm that data loss, weak data management and poor data handling pose to their businesses. The FSA made it clear in its final notice to Merchant Securities that it expects firms to be aware of its wider activities to combat the risks of financial crime.

Natalie Hunt

Information Commissioner's new power to fine for data breaches

Until now, firms that the FSA regulates have been, understandably, more concerned by the likelihood of the FSA, not the Information Commissioner, taking enforcement action. The Information Commissioner has responsibility for enforcing the data protection principles which include, as one of eight principles, a data security obligation. The ambit of the Data Protection Act 1998 is wider than the FSA's focus on system security, although the Information Commissioner's powers have been widely regarded as weak. This has resulted in some organisations taking a fairly broad brush approach to their data protection compliance obligations, secure in the knowledge that the regulator's enforcement powers have not included the power to fine.

That position has now changed. In early June 2008, primary legislation was passed which gave the Information Commissioner the power to fine organisations which "deliberately" or "recklessly" commit a serious breach of the Data Protection Act. Guidance is awaited which will set out how the fines will be imposed and what the likely level of fines will be. It is rumoured that these fines will be significant and will be used as a deterrent to others. Companies will need to think carefully about their internal procedures for collecting, storing and using customers' personal data, and ensure that their staff are trained in good data handling practices.

Wider concerns

Poor data security is not restricted to the financial services industry. Despite the now infamous HM Revenue & Customs data breach incident, there have been numerous other data breaches in recent months, many of which have involved the public sector. Most recently, a senior civil servant left top secret intelligence documents on a commuter train, treasury papers about plans to clamp down on terrorist funding were left on another train, and a leading government minister was in breach of data security rules by holding confidential information on a personal computer which was then stolen.

These incidents raise the question of why those in positions of responsibility are failing to ensure that personal information is adequately protected. Recent breaches, including many of the public sector breaches, suggest that organisations may well have adequate security and data protection policies in place, but that these are either ignored or poorly implemented.

With regard to this theme of poor implementation, the FSA security report highlights three specific failings among the firms it surveyed:

1. Failure to vet third-party suppliers, including employees of third-party suppliers, who will have access to systems and/or handle personal data.

2. Focusing too much on technical IT controls and failing to train staff.

3. Piecemeal use of third-party consultants.

In addition, the FSA security report highlights examples of good practice, including:

1. Laptop encryption and secure data transfer.

2. Ensuring that those staff who do not need access to personal data do not have such access.

3. Appointing a senior manager with responsibility for data security.

In addition to adopting good data security practices, firms would be wise, given the Information Commissioner's new powers, to broaden their focus to include data protection principles, as well as data security.

• ***Bridget Treacy*** *is a partner in the Hunton & Williams Global Sourcing and Privacy practices.* ***Natalie Hunt*** *is an associate. Her main areas of practice are global capital markets and mergers & acquisitions Tel: +44 (0)20 7220 5731*

This article first appeared on Complinet on www.complinet.com on June 30 2008. For a free trial of Complinet's services, please contact client support on client.support@complinet.com or +44 (0) 870 042 6400.