PROMONTORY

Washington, DC Atlanta Dubai London Milan New York Paris San Francisco Singapore Sydney Tokyo Toronto

Mandatory Breach Notification in the Financial Services Sector- The UK Perspective

Melanie Shillito
Director
Promontory
mshillito@promontory.com
24 January 2011

Mandatory Breach Notification – UK Financial Services Sector

- There has been a number of high profile data security breaches in the financial services sector in the UK resulting in large fines being levied – but by the Financial Services Authority (FSA), not the UK Information Commissioner.
- Would mandatory breach notification to the UK Information Commissioner and to individuals have prevented the breaches or made a difference to the individuals affected? Would they have been better protected?

Mandatory Breach Notification – UK Financial Services Sector

- UK financial institutions do not notify affected clients if there is a data breach because of the existence of the Data Protection Directive (the Directive) and implementing legislation – they would notify where appropriate in the absence of the Directive.
- Protecting *all* client data is at the core of the banking relationship, the banking relationship is built on trust and there certainly is no wish on the part of member banks to do anything that prejudices the rights and freedoms of individuals with respect to the processing of their personal data.

Mandatory Breach Notification – UK Financial Services Sector

Key existing obligations for financial institutions:

- Duty of confidentiality/secrecy
- Financial regulations
- Contractual obligations
- UK Data Protection Act 1998

PROMONTORY

FSA Requirements

- The FSA requires firms to have adequate systems and controls in place to protect customer confidential data.
- Since publishing its report 'Data Security in Financial Services ' in 2008, the FSA has left firms in no doubt what is expected of them in relation to the protection of customer data, not only in respect of the technical and organisational steps that should be taken to safeguard the data but also what individuals should be told in the event of a data breach, namely:
  - exactly what data has been lost,
  - an assessment of the risk and
  - advice and assistance to consumers at a heightened risk of identity fraud

"Even if there is no evidence of theft or fraud, it is good practice for firms to inform affected customers of a data loss in writing, unless the data is encrypted or there is law enforcement or regulatory advice to the contrary."

PROMONTORY

Concerns with a Personal Data Breach Notification Regime

- What is the evidence that a personal data breach notification regime for the financial services sector will better protect individuals?
- Do regulators want statutory breach notification or greater fining powers? Is it really just another financial threat? The UK financial services sector has that threat today.
- The interaction between data protection and financial regulators will need to be defined.
- The triggers for notification are difficult to define.
- Regulatory guidance and Codes of Practice may be a more appropriate solution?

PROMONTORY