

DATA LOSS AND FINES BY THE FSA AND THE ICO

Last month the FSA published a large report into data security in financial services. The conclusion of the report is that poor data security is currently a serious, widespread and high-impact risk to the FSA's objective to reduce financial crime. This month Parliament has given the Information Commission new powers to impose substantial fines on firms that deliberately or recklessly commit serious breaches of the Data Protection Act.

The FSA's Report on Data Security and Financial Services

The FSA found that many firms still need to make substantial progress to protect their customers from the risk of identity fraud and other financial crime. The financial services industry in the UK has come to recognise the risk of damage to reputation that can result from loss of personal data of their customers. The FSA now wants companies to step up their protection of their customers' personal data to reduce the risk of identity theft and to be open and transparent with their customers when data loss occurs.

Loss of personal data is seldom out of the news and firms, including insurers, have found themselves in the firing line for failing to adequately protect personal data. With this report the FSA has made it very clear that they expect the firms that they regulate to be more stringent in their vetting of staff with access to large volumes of customer data. They also threaten to take enforcement action against any firm that fails to encrypt customer data taken off-site in a laptop or other device.

In conformity with its new principle-based approach to regulation, the FSA defines the responsibility of firms to protect data by reference to two of their Principles for Business:

- Principle 2 - a firm must conduct its business with due skill, care and diligence;
- Principle 3 - a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

The FSA also considers that the secure handling of customer data is part of the 'Treating Customers Fairly' standard that they require all firms adhere to.

The investigation by the FSA found that in large and medium-sized firms there is a lack of coordination among business areas and too much focus on IT controls, and too little on office procedures, monitoring and due diligence. The FSA found that some firms make no risk assessment of their exposure to data loss and few continuously monitor the effectiveness of their data security controls. In smaller firms the FSA found a lack of awareness that customer data is a valuable commodity for criminals and as a result controls are often weak and sometimes absent.

The FSA note that few firms carry out criminal record checks on junior staff even where they have access to large volumes of customer data. They also criticise the training given to such staff and this results

in poor implementation of data security policies.

A major concern for the FSA is the access firms give third party suppliers to their customers' data. They found that very few firms check how their third party suppliers vet their staff or the security policies they have in place to protect personal data. Somewhat surprisingly after the high-profile instances of data loss, they found some examples of firms sending unencrypted customer data by unregistered post. Few firms have completely blocked their staff from copying data by locking USB ports and CD writers and blocking web-based email and instant messaging sites.

This report demonstrates that the FSA is going to be active in increasing the compliance of firms with data security and taking enforcement action where necessary.

The Information Commissioner's new powers

The Criminal Justice and Immigration Act 2008 which received Royal Assent on 8 May 2008, gives the Information Commissioner the power to impose substantial fines on firms that deliberately or recklessly commit serious breaches of the Data Protection Act 1988.

Under this new provision the Information Commissioner has to be satisfied that there has been a serious breach of the data protection principles that was likely to cause substantial damage or distress. He also has to be satisfied that the breach was deliberate or that the data controller knew, or ought to have known, that there was a risk of such a breach and he failed to take reasonable steps to prevent the breach. It is expected that the ICO will publish guidance on what would amount to a serious breach but allowing employees to take unencrypted personal data out of the office would probably be viewed as such a breach.

Comment

With the ICO's powers increased and the FSA taking an active role, it is a good time for firms to carry out a risk assessment of their exposure to incidents of loss of personal data. The risk assessment should cover:

- Restriction of access to premises
- The adequacy of written data security policies and procedures
- Credit checks and criminal record checks on staff with access to large volumes of customer data
- The adequacy of training given to staff about the importance of data security
- Systems and controls to minimise the risk of data loss or theft
- Encrypting of customer data taken offsite
- Disabling USB and CD writers
- The adequacy of security of backing up data
- The risks of staff using web-based email, social networking and instant messaging sites
- The secure disposal of data
- Conducting due diligence on the data security of third party suppliers.

If you would like any further information, please contact either of the following:

Robert Viney
DDI: 020 7293 4106
E: rviney@dac.co.uk

Graham Ludlam
DDI: 020 7293 4462
E: gludlam@dac.co.uk

This publication is not a substitute for detailed advice on specific transactions and problems and should not be taken as providing legal advice on any of the topics discussed.

LONDON

6-8 Bouverie Street
 London EC4Y 8DD

T +44 (0)20 7936 2222
 F +44 (0)20 7936 2020
 DX 172
 E daclon@dac.co.uk

LONDON MARKET

85 Gracechurch Street
 London EC3V 0AA

T +44 (0)20 7936 2222
 F +44 (0)20 7293 4888
 E daclon@dac.co.uk

MADRID

Paseo de la Castellana, 20
 2ª Planta
 28046 Madrid

T +34 91 781 6300
 F +34 91 576 8669
 E dacmadrid@dacspsain.com

MANCHESTER

60 Fountain Street
 Manchester M2 2FE

T +44 (0)161 839 8396
 F +44 (0)161 839 8309
 DX 14363 Manchester
 E dacman@dac.co.uk

MEXICO CITY

Av. Insurgentes 950-9
 Colonia del Valle
 Delegación Benito Juárez.
 Código Postal 03100
 México D.F.

T +52 551 107 6056
 F +52 555 687 6849
 E dacmexico@dacmexico.com

ST ALBANS

60 Victoria Street
 St Albans
 Herts AL1 3XH

T +44 (0)1727 893 200
 F +44 (0)1727 797 720
 E dacstalbens@dac.co.uk