

# Firms' Responsibilities for Protecting Data



## 1. FSA Regulations

The safekeeping of customer data is a crucial responsibility for firms. The FSA have emphasised the importance of data security for several years, and regards poor data security controls as a serious, widespread and high-impact financial crime risk.

Firms' responsibilities in this area are defined in the FSA's Principles for Businesses....

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

Also relevant is FSA Rule [SYSC 3.2.6R](#), which states that 'a firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime'.

So firms have a responsibility to assess the risks of data loss and to take reasonable steps to prevent that risk occurring. [SYSC 3.2.6A](#) says firms' relevant systems & controls must be 'comprehensive & proportionate to the nature, scale and complexity of their operations'.

In essence, firms should put in place systems and controls to minimise the risk that their operations & information assets be exploited by thieves & fraudsters. Consumers are entitled to rely on firms to ensure their personal information is secure.

Firms should note that the FSA supports the Information Commissioner's position that it is not appropriate for customer data to be taken offsite on laptops or other portable devices which are not encrypted. The FSA may take enforcement action if firms fail to encrypt customer data taken offsite.

The secure handling of customer data is also part of the 'Treating Customers Fairly' standard.

### 1.1. What does this mean for regulated businesses?

FSA regulated firms are obliged to have systems and controls in place for data security that:

- ✓ Mitigate the risk of data loss and fraud to their businesses; and
- ✓ For countering the risk that the firm might be used to further financial crime.

**Put more simply....** financial services firms in the UK need to address the risk that their customer data may be lost or stolen and then used to commit fraud or other financial crime.

In line with these principles, firms' senior management are responsible for making an appropriate assessment of the financial crime risks associated with their customer data and to 'take reasonable care to counter any weaknesses'.

Now, with several well-publicised incidents of data loss during 2007, nobody in the UK can claim ignorance of the risk of customer data falling into the wrong hands.

### 1.2. What do the FSA recommend as best practice?

 *Data Security in Financial Service – FSA Review Apr 2008.....*

The Financial Services Authority (FSA) is urging firms to change their attitude to data security & do more to help prevent their customers falling victim to identity fraud and other types of financial crime. An FSA review of systems and controls for data security at 39 firms including banks, building societies, insurance companies and financial advisers listed examples of best practice as follows:

- ✓ Encrypting laptops and transferring data via secure internet links to third parties.

#### *Data Security in Financial Service – FSA Review Apr 2008.....*

The FSA have compiled good and poor practices in relation to financial crime.

Examples of good practice:

- ✓ Conducts a risk assessment of data security and thinks about the risk to the sensitive pieces of information they hold about their members;
- ✓ Has a formal policy and written procedures for the handling of sensitive data (both paper based and electronic), with staff being trained on these procedures;
- ✓ Computer records backed-up regularly, with the back-up held securely off site;
- ✓ Data that was sent electronically or taken to other locations was encrypted and / or password protected.

### 1.3. What is the cost of getting this wrong?

In the last four years, the FSA has fined:

- ▶ **HSBC** - £3,000,000 for not having adequate systems & controls in place to protect their customers' confidential details from being lost or stolen. These failings contributed to customer [data being lost in the post on two occasions](#).
- ▶ **Capita Financial Administrators** - £300,000 for poor anti-fraud controls over client identities and accounts. Names and addresses had been changed and client instructions accepted without [appropriate validation / authentication](#).
- ▶ **Norwich Union** - £1,260,000 for not having effective systems and controls in place to protect customers' confidential information and manage its financial crime risks. The weaknesses in systems and controls allowed fraudsters to use publicly available information impersonate customers. They were also, in some cases able to ask for confidential customer records such as addresses and bank account details to be altered.
- ▶ **Merchant Securities** - £77,000 for failings relating to data security lapses & fraud. Merchant Securities had inadequate procedures for verifying the identities of customers that contacted the firm by telephone. Personal account numbers which could be used, with a customer's name, to access account information were included in routine letters.

## 2. Legal Requirements under the Data Protection Act

The Data Protection Act 1998 (DPA) gives legal rights to individuals in respect of personal data processed about them by others. There are eight Principles in the DPA that apply to all data controllers who must comply with them, unless an exemption applies.

A data controller is any person who determines the purpose for which personal data is to be processed and may include financial services firms. There is also a requirement for a data controller to notify the Information Commissioner's Office (ICO) of their processing of personal data, so the ICO can maintain a public register. The ICO has certain powers & duties under the DPA to ensure that data controllers comply with this legislation. So it is important that firms are aware of their obligations under the DPA.

The seventh DPA principle says that a data controller must take appropriate security measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data. The DPA gives some further guidance on matters that should be taken into account in deciding whether security measures are 'appropriate'.

Many firms also pass on a customer's personal data to third-party suppliers. They do so usually because the firm has specific expertise, for example in sending bulk mailings to a large number of customers, or providing other services such as IT or archiving facilities. However, this does not absolve firms of responsibility for data security who, as the data controller, will still need to comply with the seventh principle.

The DPA also introduces express obligations on data controllers when a data processor processes personal data on behalf of the data controller. In these circumstances, a data controller must choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures they take.

The data controller must also take reasonable steps to ensure compliance with those measures, and ensure the data processor carried out the processing under a contract containing certain terms & conditions. In addition, it is in the firm's own interest to comply with this legislation and protect their reputation, given increasing awareness of data loss & identity fraud in the media and among consumers.

## The Net is Tightening - Tougher Penalties for Breach of UK Data Protection Laws

The Information Commissioner's Office (ICO) — the United Kingdom's data regulator — announced on the 12th January 2010 that new powers designed to fine organizations responsible for security breaches are likely to come into effect on 6 April 2010.

From that date forward, fines of up to £500,000 can be imposed on organisations for what are considered serious breaches of the [UK's Data Protection Act 1998](#).

For the fine to be levied, "the Information Commissioner must be satisfied that there has been a serious breach that was likely to cause damage or distress and it was either deliberate or negligent and the organisation failed to take reasonable steps to prevent it."

The ICO provided examples of when the new powers will be used, such as when customers face identity theft following a data breach or when an organisation collects data for a competition but then uses the entrant's details for other purposes. The legislation states that an enforcement notice can be issued at the same time as a fine.

In the past, enforcement notices that were served required a corporation to encrypt laptops after a breach, change its marketing practices or take other compliance measures.

However, high UK fines after data breaches are not new. The Financial Services Authority (FSA) has already fined financial services organisations double the new ICO maximum after a data breach. It is likely that the ICO and FSA will continue to cooperate on investigations that involve a financial services organization or an organization that would be required to mitigate the risk of identity theft, such as Accountants sending personal tax returns to their clients.