

## Keeping the cat in the bag: FSA regulation of data security

July 2009

A forgotten briefcase, a stolen laptop, a discarded CD, a disgruntled employee, a slapdash sub-contractor, or an internet-based attack by an organised crime gang. All can, and have, resulted in serious breaches of customer data security. And such a breach can never be more serious for a business than when it provides financial services or products under the glare of the FSA.

Given the number of high profile cases involving the loss of personal (often customer) data, this article seeks to set out: (1) the FSA's concerns on customer data security practice; (2) a summary of the relevant rules; (3) examples of the FSA's enforcement activity in the area; and (4) practical guidance to firms on how to minimise the risk of a data security breach.

### The FSA's concerns

The FSA first voiced its concerns over firms' data security measures in 2004 with the publication of its Financial Sector Crime Report entitled "*Countering Financial Crime Risks in Information Security*".<sup>1</sup> In that report, the FSA made it clear that firm's could not simply react to data security breaches as and when they arose; proactive steps were required to deal with the risks. Some of the key proactive steps that a firm might take are set out below.

The FSA once again put this issue of data security in the headlines in April 2008, with the publication of its report entitled: "*Data Security in Financial Services: Firms' controls to prevent data loss by their employees and third-party suppliers*".<sup>2</sup> The report followed a comprehensive review of a range of firms' policies and procedures for managing customer data. The FSA's overall conclusion was that: "*poor data security is a serious and widespread problem in the financial services industry.*"

In its report, the FSA identified in particular the following three main problems with firms:

- Failure to appreciate the gravity of the risk.
- Lack of expertise to make a reasonable assessment of key risk factors and devise ways of meeting them.
- Failure to devote or co-ordinate adequate resources to address the risk.<sup>3</sup>

### The FSA's rules

Such failures are very likely to constitute breaches of FSA rules and guidance. The rules to be borne in mind when deciding how to deal with customer data security are relatively high level, providing firms with flexibility in ensuring compliance. The most important of these are, first, the following Principles for Business:

- **Principle 2** - A firm must conduct its business with due skill, care and integrity.
- **Principle 3** - A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
- **Principle 6** - A firm must pay due regard to the interests of its customers and treat them fairly.<sup>4</sup>

Second, the recently revised Senior Management Arrangements, Systems and Controls impose on the vast majority of firms more specific requirements relating to data security:

- **SYSC 6.1.1R** provides that a firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.

<sup>1</sup> [http://www.fsa.gov.uk/pubs/other/fcrime\\_sector.pdf](http://www.fsa.gov.uk/pubs/other/fcrime_sector.pdf)

<sup>2</sup> [http://www.fsa.gov.uk/pubs/other/data\\_security.pdf](http://www.fsa.gov.uk/pubs/other/data_security.pdf)

<sup>3</sup> [http://www.fsa.gov.uk/pubs/other/data\\_security.pdf](http://www.fsa.gov.uk/pubs/other/data_security.pdf)

<sup>4</sup> <http://fsahandbook.info/FSA/html/handbook/PRIN/2/1>

- **SYSC 6.3.1R** provides that a firm must ensure the policies and procedures established under SYSC 6.1.1R include systems and controls that: (1) enable it to identify, assess, monitor and manage money laundering risk; and (2) are comprehensive and proportionate to the nature, scale and complexity of its activities.
- **SYSC 6.3.3R** provides that a firm must carry out a regular assessment of the adequacy of these systems and controls to ensure that they continue to comply with SYSC 6.3.1 R.<sup>5</sup>

Different but similar systems and controls requirements are imposed on insurers, managing agents, and Lloyds.

### The FSA's enforcement action

The FSA has meted out a series of fines to firms that have failed to properly secure customer data, in breach of the obligations referred to above:

- **Norwich Union Life Assurance** – Fined £1.26 million when its defective customer data security systems and controls allowed fraudsters to use publicly available information to impersonate Norwich Union customers, and instruct Norwich Union staff at call centres to surrender the proceeds to bank accounts controlled by the fraudsters. Of 632 cases, there were 74 fraudulent surrenders amounting to approximately £3.3 million in total. To compound matters, confidential customer information regarding the policy was disclosed to the fraudsters in almost all of those 632 cases. Finally, on discovering the frauds in July 2006, Norwich Union took specific action to identify, inform and protect all current and former directors of Norwich Union and the wider Aviva Group directors who were policyholders. It did not, however, take equivalent action at that time to inform and protect the policyholders who were not connected with the business.<sup>6</sup>
- **Merchant Securities Group** – Fined GBP 77,000 for operating defective client identification procedures. In particular, advisers, each of whom had approximately 150 customers, relied on recognising customers' voices to identify their clients and by talking with them informally about personal matters such as holidays or hobbies. Additionally, the firm included customers' account numbers in letters it sent to them.<sup>7</sup>
- **HSBC** - Three HSBC entities (HSBC Life (UK) Ltd,<sup>8</sup> HSBC Actuaries and Consultants Ltd,<sup>9</sup> and HSBC Insurance Brokers Ltd<sup>10</sup>) were collectively fined £3.2 million for defective

customer data security systems and controls. Specifically, the firms allowed large quantities of unencrypted customer data to be sent to third parties via post or local courier services. Additionally the firms allowed customer data to be kept on open shelves or in cabinets which were unable to be locked.

Given the FSA's commitment to "credible deterrence", we fully expect to see further high profile cases in which the FSA severely punishes firms that fail to establish and operate effective systems and controls in order to secure customer data.

### Practical steps for firms

Consequently, in order to assist firms to avoid being on the receiving end of the enforcement action referred to above, and the severe financial and reputation penalties that accompany that action, we set out below some practical preventative and remedial measures that firms should implement in a manner that is proportionate to the size of the firm and the risks it faces.

#### Preventative

- Consider the scope and location, physical and digital, of all live and back-up customer data, and its potential for transportability e.g. on firm laptops, CDs, and USB data sticks.
- Establish, monitor, and maintain a comprehensive security system, proportionate to the size of the firm and customer base, for the containment and management of physical and digital customer data. The system should include physically and digitally secure servers, internal IT user access restrictions, especially in relation to departed employees; robust username and password requirements; perimeter safeguards to prevent internet-based data security compromises; encryption of data held on laptops; procedures of signing laptops in and out so their location at any one time can be easily identified; properly enforced restrictions on access to premises; an enforced "clear desk" policy; and locking of filing cabinets and record rooms.
- Produce and distribute written policy for staff in order to assist in the implementation of the security system. The policy should: include rules and procedures for the management of customer data and data security risks by employees; make clear to employees the "do's and don'ts" when they are using digital and physical customer data, take it off-site, or dispose of it; and set out the steps to be taken if a breach is identified.

<sup>5</sup> <http://fsahandbook.info/FSA/html/handbook/SYSC/6>

<sup>6</sup> [http://www.fsa.gov.uk/pubs/final/Norwich\\_Union\\_Life.pdf](http://www.fsa.gov.uk/pubs/final/Norwich_Union_Life.pdf)

<sup>7</sup> [http://www.fsa.gov.uk/pubs/final/merchant\\_13jun08.pdf](http://www.fsa.gov.uk/pubs/final/merchant_13jun08.pdf)

<sup>8</sup> [http://www.fsa.gov.uk/pubs/final/hsbc\\_inuk0907.pdf](http://www.fsa.gov.uk/pubs/final/hsbc_inuk0907.pdf)

<sup>9</sup> [http://www.fsa.gov.uk/pubs/final/hsbc\\_actuaris0709.pdf](http://www.fsa.gov.uk/pubs/final/hsbc_actuaris0709.pdf)

<sup>10</sup> [http://www.fsa.gov.uk/pubs/final/hsbc\\_ins0709.pdf](http://www.fsa.gov.uk/pubs/final/hsbc_ins0709.pdf)

- Appoint one or more senior manager to be responsible for the system and policy.
- Vet employees (especially junior employees) who have access to customer data. Such vetting should be carried out on an initial and periodic basis.
- Regularly train staff on evolving data security risks and the policies in place to combat those risks. Implement simple staff awareness initiatives such as poster campaigns and quizzes or competitions.
- Vet and monitor parties to whom functions involving customer data are outsourced or sub-contracted, and encrypt all data communications with them.
- Notify the customers at risk of what has happened, the nature and level of the risk, and what is being done to remedy the situation. Offer advice on what steps the customer can take to safeguard their personal information.
- Consider the FSA notification obligations. If it is decided that the breach is sufficiently serious to notify the FSA, regularly update the FSA up with the progress of internal investigations and the remedial steps that are being taken.
- Promptly remediate any customers that have suffered any financial loss as a result of the breach.

We have advised several firms that have unfortunately allowed customer data security breaches to occur on both their legal and regulatory obligations, and the practical steps that they can take to remedy the situation. Please contact us if you would like to discuss any data security issues with us.

### Remedial

- If a breach is identified, act quickly to determine the cause, nature and scale of the breach, the customers or class of customers whose data may have been disclosed or at risk, and the financial and other risks caused to customers.

### If you require further information, please contact:



**Tim Pope**  
Senior Associate

Tel: +44(0)117 939 2230  
Mobile: +44(0)7968 225 096  
Email: [tim.pope@burges-salmon.com](mailto:tim.pope@burges-salmon.com)



**Thomas Webb**  
Associate

Tel: +44(0)117 307 6976  
Mobile: +44(0)7794 030 898  
Email: [thomas.webb@burges-salmon.com](mailto:thomas.webb@burges-salmon.com)

Disclaimer: This briefing gives general information only and is not intended to be an exhaustive statement of the law. Although we have taken care over the information, you should not rely on it as legal advice. We do not accept any liability to anyone who does rely on its content.

© Burges Salmon LLP 2009. All rights reserved. Extracts may be reproduced with our prior consent, provided that the source is acknowledged.

Data Protection: Your details are processed and kept securely in accordance with the Data Protection Act 1998. We may use your personal information to send information to you about our products and services, newsletters and legal updates; to invite you to our training seminars and other events; and for analysis including generation of marketing reports. To help us keep our database up to date, please let us know if your contact details change or if you do not want to receive any further marketing material by contacting [marketing@burges-salmon.com](mailto:marketing@burges-salmon.com).