Chapter 5

Data security

5.1 Introduction

5.1.1 G **Who should read this chapter?** This chapter applies to **all firms** subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R and to **e-money institutions** and **payment institutions** within our supervisory scope.

5.1.2 G Customers routinely entrust firms with important personal data; if this falls into criminal hands, fraudsters can attempt to undertake transactions in the customer's name. Firms must take special care of their customers' personal data, and comply with the data protection principles set out in Schedule 1 to the Data Protection Act 1998. The Information Commissioner's Office provides guidance on the Data Protection Act and the responsibilities it imposes on data controllers and processors. See section 4 and schedule 1 Data Protection Act 1998.

5.2 Themes

Governance

5.2.1 G The guidance in ■ FCG 2.2.1G on governance in relation to financial crime also applies to data security.

Firms should be alert to the financial crime risks associated with holding customer data and have written data security policies and procedures which are proportionate, accurate, up to date and relevant to the day-to-day work of staff.

Self-assessment questions:

- How is **responsibility** for data security apportioned?
- Has the firm ever **lost customer data**? If so, what remedial actions did it take? Did it contact customers? Did it review its systems?
- How does the firm monitor that **suppliers of outsourced services** treat customer data appropriately?
- Are data security standards set in **outsourcing** agreements, with suppliers' performance subject to monitoring?

Examples of good practice	Examples of poor practice
• There is a clear **figurehead** championing the issue of data security.	• The firm does not **contact customers** after their data is lost or compromised.
• Work, including by internal audit and compliance, is **coordinated** across the firm, with compliance, audit, HR, security and IT all playing a role.	• Data security is treated as an **IT** or **privacy issue**, without also recognising the financial crime risk.
• A firm's **plans to respond to data loss incidents** are clear and include notifying customers affected by data loss and offering advice to those customers about protective measures.	• A '**blame culture**' discourages staff from reporting data losses.
• A firm **monitors accounts** following a data loss to spot unusual transactions.	• The firm is unsure how its **third parties**, such as suppliers, protect customer data.
• The firm looks at **outsourcers'** data security practices before doing	

Examples of good practice	Examples of poor practice
business, and monitors compliance.	

Five fallacies of data loss and identity fraud

5.2.2 G

1. **'The customer data we hold is too limited or too piecemeal to be of value to fraudsters.'** This is misconceived: skilled fraudsters can supplement a small core of data by accessing several different public sources and use impersonation to encourage victims to reveal more. Ultimately, they build up enough information to pose successfully as their victim.

2. **'Only individuals with a high net worth are attractive targets for identity fraudsters.'** In fact, people of all ages, in all occupations and in all income groups are vulnerable if their data is lost.

3. **'Only large firms with millions of customers are likely to be targeted.'** Wrong. Even a small firm's customer database might be sold and re-sold for a substantial sum.

4. **'The threat to data security is external.'** This is not always the case. Insiders have more opportunity to steal customer data and may do so either to commit fraud themselves, or to pass it on to organised criminals.

5. **'No customer has ever notified us that their identity has been stolen, so our firm must be impervious to data breaches.'** The truth may be closer to the opposite: firms that successfully detect data loss do so because they have effective risk-management systems. Firms with weak controls or monitoring are likely to be oblivious to any loss. Furthermore, when fraud does occur, a victim rarely has the means to identify where their data was lost because data is held in so many places.

Controls

5.2.3 G

We expect firms to put in place systems and controls to minimise the risk that their operation and information assets might be exploited by thieves and fraudsters. Internal procedures such as IT controls and physical security measures should be designed to protect against **unauthorised access** to customer data.

Firms should note that we support the Information Commissioner's position that it is not appropriate for customer data to be taken off-site on laptops or other portable devices which are not encrypted.

Self-assessment questions:

- Is your firm's customer data taken **off-site**, whether by staff (sales people, those working from home) or third parties (suppliers, consultants, IT contractors etc)?

- If so, what **levels of security** exist? (For example, does the firm require automatic encryption of laptops that leave the premises, or measures to ensure no sensitive data is taken off-site? If customer

data is transferred electronically, does the firm use secure internet links?)

•How does the firm **keep track** of its digital assets?

•How does it **dispose** of documents, computers, and imaging equipment such as photocopiers that retain records of copies? Are accredited suppliers used to, for example, destroy documents and hard disks? How does the firm satisfy itself that data is disposed of competently?

•How are **access** to the premises and sensitive areas of the business **controlled**?

•When are **staff access rights** reviewed? (It is good practice to review them at least on recruitment, when staff change roles, and when they leave the firm.)

•Is there enhanced **vetting** of staff with access to lots of data?

•How are staff made aware of **data security risks**?

Examples of good practice	Examples of poor practice
• **Access** to sensitive areas (call centres, server rooms, filing rooms) is restricted.	• Staff and third party suppliers can access **data they do not need** for their role.
• The firm has **individual user accounts** for all systems containing customer data.	• Files are not **locked away**.
• The firm conducts risk-based, **proactive monitoring** to ensure employees' access to customer data is for a genuine business reason.	• Password standards are not robust and individuals **share passwords**.
• IT equipment is disposed of responsibly, e.g. by using a contractor **accredited** by the British Security Industry Association.	• The firm **fails to monitor** superusers or other staff with access to large amounts of customer data.
• Customer data in electronic form (e.g. on USB sticks, CDs, hard disks etc) is always **encrypted** when taken off-site.	• Computers are disposed of or transferred to new users without data being **wiped**.
• The firm understands what checks are done by **employment agencies** it uses.	• Staff working **remotely** do not dispose of customer data securely.
	• Staff handling large volumes of data also have access to **internet email**.
	• Managers assume staff understand data security risks and **provide no training**.
	• **Unencrypted** electronic data is distributed by post or courier.

Effective cyber practices

5.2.3A G Self-assessment questions:

•Are critical systems and data backed up, and do you test backup recovery processes regularly?

•Are you able to restore services in the event of an incident?

•Are network and computer security systems, software and applications kept up to date and regularly patched? Do you make sure your computer network and information systems are configured to prevent unauthorised access?

•How do you manage user and device credentials? Do you ensure that staff use strong passwords when logging on to hardware and software? Are the default administrator credentials for all devices changed?

•Is two-factor authentication used where the confidentiality of the data is most crucial?

•How do you protect sensitive data that is stored or in transit? Do you use encryption software to protect your critical information from unauthorised access?

Examples of good practice	Examples of good practice
	• Using weak or easy to guess passwords or creating passwords from familiar details.
• The firm carries out regular vulnerability assessments and patching.	• Poor physical management and/or control of devices.
• The firm carries out regular security testing.	• Not setting out appropriate user privileges on access to resources on the firm's network, data storages or applications.
• An application programming interface (API) allows different software to communicate with each other and has security measures in place.	• Not encrypting data at storage or between networks.
	• Not updating devices, software and operating systems with the latest security patches.
	• Not properly vetting third-party systems and vendors.

Examples of good practice	Examples of good practice
	• Not employing multi-factor authentication for devices, systems and services. • Insufficient staff training around social engineering and vishing and phishing campaigns.
• The firm is able to restore systems following an incident and restorations are done in a timely manner.	
	• Inadequate controls to revoke access for staff that leave the firm, the role or the department.

Case study – protecting customers' accounts from criminals

5.2.4 G In December 2007, the *FSA* fined Norwich Union Life £1.26m for failings in its anti-fraud systems and controls.

Firms should note that we support the Information Commissioner's position that it is not appropriate for customer data to be taken off-site on laptops or other portable devices which are not encrypted.

•Callers to Norwich Union Life call centres were able to satisfy the firm's caller identification procedures by providing public information to impersonate customers.

•Callers obtained access to customer information, including policy numbers and bank details and, using this information, were able to request amendments to Norwich Union Life records, including changing the addresses and bank account details recorded for those customers.

•The frauds were committed through a series of calls, often carried out in quick succession.

•Callers subsequently requested the surrender of customers' policies

. •Over the course of 2006, 74 policies totalling £3.3m were fraudulently surrendered.

•The firm failed to address issues highlighted by the frauds in an appropriate and timely manner even after they were identified by its own compliance department.

•Norwich Union Life's procedures were insufficiently clear as to who was responsible for the management of its response to these actual and attempted frauds. As a result, the firm did not give appropriate

priority to the financial crime risks when considering those risks against competing priorities such as customer service.

For more, see the *FCA's* press release: www.fca.org.uk/news/press-releases/fsa-fines-norwich-union-life-%C2%A3126m-exposing-its-customers-risk-fraud

Case study – data security failings

5.2.5 G In August 2010, the *FSA* fined Zurich Insurance plc, UK branch £2,275,000 following the loss of 46,000 policyholders' personal details.

5

- The firm failed to take reasonable care to ensure that it had effective systems and controls to manage the risks relating to the security of confidential customer information arising out of its outsourcing arrangement with another Zurich company in South Africa.

- It failed to carry out adequate due diligence on the data security procedures used by the South African company and its subcontractors.

- It relied on group policies without considering whether this was sufficient and did not determine for itself whether appropriate data security policies had been adequately implemented by the South African company.

- The firm failed to put in place proper reporting lines. While various members of senior management had responsibility for data security issues, there was no single data security manager with overall responsibility.

- The firm did not discover that the South African entity had lost an unencrypted back-up tape until a year after it happened.

The *FCA's* press release has more details: www.fca.org.uk/news/press-releases/fsa-fines-zurich-insurance-%C2%A32275000-following-loss-46000-policy-holders-personal

5.3 Further guidance

5.3.1 G *FCTR* contains the following additional material on data security:

- FCTR 6 summarises the findings of the *FSA's* thematic review of Data security in Financial Services and includes guidance on:
  - Governance (FCTR 6.3.1G)
  - Training and awareness (FCTR 6.3.2G)
  - Staff recruitment and vetting (FCTR 6.3.3G)
  - Controls – access rights (FCTR 6.3.4G)
  - Controls – passwords and user accounts (FCTR 6.3.5G)
  - Controls – monitoring access to customer data (FCTR 6.3.6G)
  - Controls – data back-up (FCTR 6.3.7G)
  - Controls – access to the internet and email (FCTR 6.3.8G)
  - Controls – key-logging devices (FCTR 6.3.9G)
  - Controls – laptop (FCTR 6.3.10G)
  - Controls – portable media including USB devices and CDs (FCTR 6.3.11G)
  - Physical security (FCTR 6.3.12G)
  - Disposal of customer data (FCTR 6.3.13G)
  - Managing third party suppliers (FCTR 6.3.14G)
  - Internal audit and compliance monitoring (FCTR 6.3.15G)
- FCTR 10 summarises the findings of the Small Firms Financial Crime Review, and contains guidance directed at small firms on:
  - Records (FCTR 10.3.5G)
  - Responsibilities and risk assessments (FCTR 10.3.7G)
  - Access to systems (FCTR 10.3.8G)
  - Outsourcing (FCTR 10.3.9G)
  - Physical controls (FCTR 10.3.10G)
  - Data disposal (FCTR 10.3.11G)
  - Data compromise incidents (FCTR 10.3.12G)

5.4 Sources of further information

5

5.4.1 G To find out more, see

- the website of the Information Commissioner's Office: www.ico.org.uk.
- National Cyber Security Centre, 10 Steps to Cyber Security: www.ncsc.gov.uk/collection/10-steps/data-security.
- National Cyber Security Centre, Cyber Security Toolkit for Boards: www.ncsc.gov.uk/collection/board-toolkit/introduction-to-cyber-security-for-board-members.