Chapter 6

Data security in Financial Services (2008)

6.3 Consolidated examples of good and poor practice

6.3.1 Governance

Examples of good practice	Examples of poor practice
• Identification of data security as a key specific risk, subject to its own governance, policies and procedures and risk assessment.	• Treating data security as an IT issue and failing to involve other key staff from across the business in the risk assessment process.
• A senior manager with overall responsibility for data security, specifically mandated to manage data security risk assessment and communication between the key stakeholders within the firm such as: senior management, information security, Human Resources, financial crime, security, IT, compliance and internal audit.	• No written policies and procedures on data security.
• A specific committee with representation from relevant business areas to assess, monitor and control data security risk, which reports to the firm's Board. As well as ensuring coordinated risk management, this structure sends a clear message to all staff about the importance of data security.	• Firms do not understand the need for knowledge-sharing on data security.
• Written data security policies and procedures that are proportionate, accurate and relevant to staff's day-to-day work.	• Failing to take opportunities to share information with, and learn from, peers and others about data security risk and not recognising the need to do so.
• An open and honest culture of communication with predetermined reporting mechanisms that make it easy for all staff and third parties to report data security concerns and data loss without fear of blame or recrimination.	• A 'blame culture' that discourages staff from reporting data security concerns and data losses.

• Firms seeking external assistance if they feel they do not have the necessary expertise to complete a data security risk assessment themselves. • Firms liaising with peers and others to increase their awareness of data security risk and the implementation of good systems and controls. • Detailed plans for reacting to a data loss including when and how to communicate with affected customers. • Firms writing to affected customers promptly after a data loss, telling them what has been lost and how it was lost. • Firms offering advice on protective measures against identity fraud to consumers affected by data loss and, where appropriate, paying for such services to be put in place.	• Failure to notify customers affected by data loss in case the details are picked up by the media

6.3.2 Training and awareness

Examples of good practice	Examples of poor practice
• Innovative training and awareness campaigns that focus on the financial crime risks arising from poor data security, as well as the legal and regulatory requirements to protect customer data.	• No training to communicate policies and procedures.
• Clear understanding among staff about why data security is relevant to their work and what they must do to comply with relevant policies and procedures.	• Managers assuming that employees understand data security risk without any training.
• Simple, memorable and easily digestible guidance for staff on good data security practice.	• Data security policies which are very lengthy, complicated and difficult to read.
• Testing of staff understanding of data security policies on induction and once a year after that.	• Reliance on staff signing an annual declaration stating that they have read policy documents without any further testing.
• Competitions, posters, screensavers and group discussion to raise interest in the subject.	• Staff being given no incentive to learn about data security.

6.3.3 Staff recruitment and vetting

Examples of good practice	Examples of poor practice
• Vetting staff on a risk-based approach, taking into account data security and other fraud risk.	• Allowing new recruits to access customer data before vetting has been completed.
• Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists and the CIFAS Staff Fraud Database – for staff in roles with access to large amounts of customer data.	• Temporary staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.
• Liaison between HR and Financial Crime to ensure that financial crime risk indicators are considered during the vetting process.	• Failing to consider continually whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.
• A good understanding of vetting conducted by employment agencies for temporary and contract staff.	
• Formalised procedures to assess regularly whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.	

6.3.4 Controls – Access rights

Examples of good practice	Examples of poor practice
• Specific IT access profiles for each role in the firm, which set out exactly what level of IT access is required for an individual to do their job.	• Staff having access to customer data that they do not require to do their job.
• If a staff member changes roles or responsibilities, all IT access rights are deleted from the system and the user is set up using the same process as if they were a new joiner at the firm. The complexity of this process is significantly reduced if role-based IT access profiles are in place – the old one can simply be replaced with the new.	• User access rights set up on a case-by-case basis with no independent check that they are appropriate.
• A clearly-defined process to notify IT of forthcoming staff departures in order	• Failing to consider continually whether staff in higher-risk positions are becoming

that IT accesses can be permanently disabled or deleted on a timely and accurate basis.	vulnerable to committing fraud or being coerced by criminals.
• Regular reviews of staff IT access rights to ensure that there are no anomalies.	• User accounts being left 'live' or only suspended (i.e. not permanently disabled) when a staff member leaves.
• Least privilege' access to call recordings and copies of scanned documents obtained for 'know your customer' purposes.	• A lack of independent check of changes effected at any stage in the joiners, movers and leavers process.
• Authentication of customers' identities using, for example, touch-tone telephone before a conversation with a call centre adviser takes place. This limits the amount of personal information and/or passwords contained in call recordings.	
• Masking credit card, bank account details and other sensitive data like customer passwords where this would not affect employees' ability to do their job.	

6.3.5 Controls – passwords and user accounts

Examples of good practice	Examples of poor practice
• Individual user accounts – requiring passwords – in place for all systems containing customer data.	• The same user account and password used by multiple users to access particular systems.
• Password standards at least equivalent to those recommended by Get Safe Online – a government-backed campaign group. In July 2011, their recommended standard for passwords was a combination of letters, numbers and keyboard symbols at least eight characters in length and changed regularly.	• Names and dictionary words used as passwords.
• Measures to ensure passwords are robust. These might include controls to ensure that passwords can only be set in accordance with policy and the use of	• Systems that allow passwords to be set which do not comply with password policy.

password-cracking software on a risk-based approach.	
• 'Straight-through processing', but only if complemented by accurate role-based access profiles and strong passwords.	• Individuals share passwords.

6.3.6 Controls – monitoring access to customer data

Examples of good practice	Examples of poor practice
• Risk-based, proactive monitoring of staff's access to customer data to ensure it is being accessed and/or updated for a genuine business reason.	• Assuming that vetted staff with appropriate access rights will always act appropriately. Staff can breach procedures, for example by looking at account information relating to celebrities, be tempted to commit fraud themselves or be bribed or threatened to give customer data to criminals.
• The use of software designed to spot suspicious activity by employees with access to customer data. Such software may not be useful in its 'off- the-shelf' format so it is good practice for firms to ensure that it is tailored to their business profile.	• Names and dictionary words used as passwords.
• Strict controls over superusers' access to customer data and independent checks of their work to ensure they have not accessed, manipulated or extracted data that was not required for a particular task.	• Failing to monitor superusers or other employees with access to large amounts of customer data.

6.3.7 Controls – data back-up

Examples of good practice	Examples of poor practice
• Firms conducting a proper risk assessment of threats to data security arising from the data back-up process – from the point that back-up tapes are produced, through the transit process to the ultimate place of storage.	• Firms failing to consider data security risk arising from the backing up of customer data.

• Firms encrypting backed-up data that is held off-site, including while in transit.	• A lack of clear and consistent procedures for backing up data, resulting in data being backed up in several different ways at different times. This makes it difficult for firms to keep track of copies of their data.
• Regular reviews of the level of encryption to ensure it remains appropriate to the current risk environment.	• Unrestricted access to back-up tapes for large numbers of staff at third party firms.
• Back-up data being transferred by secure Internet links.	• Back-up tapes being held insecurely by firm's employees; for example, being left in their cars or at home on the kitchen table.
• Due diligence on third parties that handle backed-up customer data so the firm has a good understanding of how it is secured, exactly who has access to it and how staff with access to it are vetted.	
• Staff with responsibility for holding backed-up data off-site being given assistance to do so securely. For example, firms could offer to pay for a safe to be installed at the staff member's home.	
• Firms conducting spot checks to ensure that data held off-site is held in accordance with accepted policies and procedures.	

6.3.8 Controls – access to the internet and email

Examples of good practice	Examples of poor practice
• Giving internet and email access only to staff with a genuine business need.	• Allowing staff who handle customer data to have access to the internet and email if there is no business reason for this.
• Considering the risk of data compromise when monitoring external email traffic, for example by	• Allowing access to web-based communication Internet sites. This content includes web-based email,

	looking for strings of numbers that might be credit card details.	messaging facilities on social networking sites, external instant messaging and 'peer-to- peer' file-sharing software.
	• Where proportionate, using specialist IT software to detect data leakage via email.	
	• Completely blocking access to all internet content which allows web-based communication. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and 'peer-to-peer' file-sharing software.	
	• Firms that provide cyber-cafes for staff to use during breaks ensuring that web-based communications are blocked or that data cannot be transferred into the cyber-cafe, either in electronic or paper format.	

6

6.3.9 Controls – key-logging devices

Examples of good practice	
• Regular sweeping for key-logging devices in parts of the firm where employees have access to large amounts of, or sensitive, customer data. (Firms will also wish to conduct sweeps in other sensitive areas. For example, where money can be transferred.)	
• Use of software to determine whether unusual or prohibited types of hardware have been attached to employees' computers.	
• Raising awareness of the risk of key-logging devices. The vigilance of staff is a useful method of defence.	
• Anti-spyware software and firewalls etc in place and kept up to date.	

6.3.10 Controls – laptop

Examples of good practice	Examples of poor practice
• The encryption of laptops and other portable devices containing customer data.	• Unencrypted customer data on laptops.
• Controls that mitigate the risk of employees failing to follow policies and procedures. The *FSA* has dealt with several cases of lost or stolen laptops that arose from firms' staff not doing what they should.	• A poor understanding of which employees have been issued or are using laptops to hold customer data.
• Maintaining an accurate register of laptops issued to staff.	• Shared laptops used by staff without being signed out or wiped between uses.
• Regular audits of the contents of laptops to ensure that only staff who are authorised to hold customer data on their laptops are doing so and that this is for genuine business reasons.	
• The wiping of shared laptops' hard drives between uses.	

6.3.11 Controls – portable media including USB devices and CDs

Examples of good practice	Examples of poor practice
• Ensuring that only staff with a genuine business need can download customer data to portable media such as USB devices and CDs.	• Allowing staff with access to bulk customer data – for example, superusers – to download to unencrypted portable media.
• Ensuring that staff authorised to hold customer data on portable media can only do so if it is encrypted.	• Failing to review regularly threats posed by increasingly sophisticated and quickly evolving personal technology such as mobile phones.
• Maintaining an accurate register of staff allowed to use USB devices and	

	staff who have been issued USB devices.
•	The use of software to prevent and/or detect individuals using personal USB devices.
•	Firms reviewing regularly and on a risk-based approach the copying of customer data to portable media to ensure there is a genuine business reason for it.
•	The automatic encryption of portable media attached to firms' computers.
•	Providing lockers for higher-risk staff such as call centre staff and superusers and restricting them from taking personal effects to their desks.

6.3.12 Controls – Physical security

Examples of good practice		Examples of poor practice	
•	Appropriately restricted access to areas where large amounts of customer data are accessible, such as server rooms, call centres and filing areas.	•	Allowing staff or other persons with no genuine business need to access areas where customer data is held.
•	Using robust intruder deterrents such as keypad entry doors, alarm systems, grilles or barred windows, and closed circuit television (CCTV).	•	Failure to check electronic records showing who has accessed sensitive areas of the office.
•	Robust procedures for logging visitors and ensuring adequate supervision of them while on-site.	•	Failure to lock away customer records and files when the office is left unattended.
•	Training and awareness programmes for staff to ensure they are fully aware of more basic risks to customer data arising from poor physical security.		
•	Employing security guards, cleaners etc directly to ensure an appropriate level of vetting and reduce risks that can arise		

through third party suppliers accessing customer data.	
• Using electronic swipe card records to spot unusual behaviour or access to high risk areas.	
• Keeping filing cabinets locked during the day and leaving the key with a trusted member of staff.	
• An enforced clear-desk policy.	

6.3.13 Controls – Disposal of customer data

Examples of good practice	Examples of poor practice
• Procedures that result in the production of as little paper-based customer data as possible.	• Poor awareness among staff about how to dispose of customer data securely.
• Treating all paper as 'confidential waste' to eliminate confusion among employees about which type of bin to use.	• Slack procedures that present opportunities for fraudsters, for instance when confidential waste is left unguarded on the premises before it is destroyed.
• All customer data disposed of by employees securely, for example by using shredders (preferably cross-cut rather than straight-line shredders) or confidential waste bins.	• Staff working remotely failing to dispose of customer data securely.
• Checking general waste bins for the accidental disposal of customer data.	• Firms failing to provide guidance or assistance to remote workers who need to dispose of an obsolete home computer.
• Using a third party supplier, preferably one with BSIA (British Security Industry Association) accreditation, which provides a certificate of secure destruction, to shred or incinerate paper-based customer data. It is important for firms to have a good understanding of the supplier's process for destroying customer data and their employee vetting standards.	• Firms stockpiling obsolete computers and other portable media for too long and in insecure environments.
• Providing guidance for travelling or home-based	• Firms relying on others to erase or destroy their hard

staff on the secure disposal of customer data.	drives and other portable media securely without evidence that this has been done competently.
• Computer hard drives and portable media being properly wiped (using specialist software) or destroyed as soon as they become obsolete.	

6.3.14 Managing third-party suppliers

Examples of good practice	Examples of poor practice
• Conducting due diligence of data security standards at third-party suppliers before contracts are agreed.	• Allowing third-party suppliers to access customer data when no due diligence of data security arrangements has been performed.
• Regular reviews of third-party suppliers' data security systems and controls, with the frequency of review dependent on data security risks identified.	• Firms not knowing exactly which third-party staff have access to their customer data.
• Ensuring third-party suppliers' vetting standards are adequate by testing the checks performed on a sample of staff with access to customer data.	• Firms not knowing how third-party suppliers' staff have been vetted.
• Only allowing third-party IT suppliers access to customer databases for specific tasks on a case- by-case basis.	• Allowing third-party staff unsupervised access to areas where customer data is held when they have not been vetted to the same standards as employees.
• Third-party suppliers being subject to procedures for reporting data security breaches within an agreed timeframe.	• Allowing IT suppliers unrestricted or unmonitored access to customer data.
• The use of secure internet links to transfer data to third parties.	• A lack of awareness of when/how third-party suppliers can access customer data and failure to monitor such access.
	• Unencrypted customer data being sent to third parties using unregistered post.

6.3.15 Internal audit and compliance monitoring

Examples of good practice	Examples of poor practice

• Firms seeking external assistance where they do not have the necessary in-house expertise or resources.	• Compliance focusing only on compliance with data protection legislation and failing to consider adherence to data security policies and procedures.
• Compliance and internal audit conducting specific reviews of data security which cover all relevant areas of the business including IT, security, HR, training and awareness, governance and third-party suppliers.	• Compliance consultants adopting a 'one size fits all' approach to different clients' businesses.
• Firms using expertise from across the business to help with the more technical aspects of data security audits and compliance monitoring.	