



Financial Services Authority

Data Security in Financial Services

***Firms' controls to prevent data loss by their
employees and third-party suppliers***

Financial Crime and Intelligence Division

Foreword by the Information Commissioner

April
2008



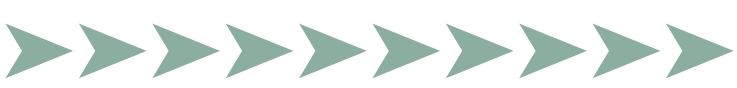


Foreword by Richard Thomas, the Information Commissioner

I welcome this report on the protection of customer data within the financial services industry. It includes examples of good practice by some financial institutions which others could usefully learn from. However, I am disappointed – but not altogether surprised – that the FSA has found that financial services firms, in general, could significantly improve their controls to prevent data loss or theft.

The blunt truth is that all organisations need to take the protection of customer data with the utmost seriousness. I have made clear publicly on several occasions over the past year that organisations holding individuals' data must in particular take steps to ensure that it is adequately protected from loss or theft. There have been several high-profile incidents of data loss in public and private sectors during that time which have highlighted that some organisations could do much better. The coverage of these incidents has also raised public awareness of how lost or stolen data can be used for crimes like identity fraud. Getting data protection wrong can bring commercial, reputational, regulatory and legal penalties. Getting it right brings rewards in terms of customer trust and confidence.

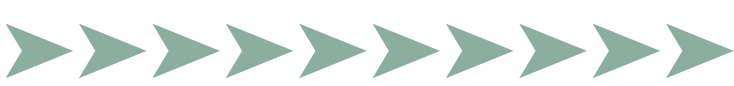
The financial services industry needs to pay close attention to what its regulator is saying here. But this report is also relevant to organisations outside the financial services industry which hold data about private individuals. All organisations handling individuals' data, in both the public and private sectors, could benefit from the good practice advice it contains.



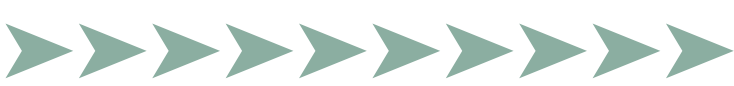


Contents

1. Executive summary	6
1.1 Introduction	6
1.2 Findings	7
1.3 Conclusions	9
2. Introduction	11
2.1 Objectives	11
2.2 Background	12
2.3 Methodology	13
2.4 How data loss occurs	14
2.5 How lost data is used for identity fraud	15
2.6 Firms' responsibilities	17
2.6.1 Legal requirements	17
2.7 Attitudes to data security and identity fraud	18
2.7.1 Five fallacies	18
2.7.2 Changing attitudes	20
2.7.3 Changing behaviour	21
3. Findings	22
3.1 Governance – managing systems and controls	22
3.1.1 Policies and procedures	23
3.1.2 Benchmarking	24
3.1.3 Risk assessment	24
3.1.4 Organisation, monitoring performance and communication	25
3.1.5 External liaison	26



3.1.6	Data loss reporting and response	27
3.1.7	Notifying customers of data loss	27
3.2	Training and awareness	30
3.2.1	Poor assumptions about risk awareness	31
3.2.2	Advantages of written guidelines	31
3.2.3	Effective training and awareness mechanisms	31
3.3	Staff recruitment and vetting	34
3.3.1	Initial Recruitment Process	35
3.3.2	Temporary staff	38
3.3.3	Ongoing vetting of staff	39
3.4	Controls	40
3.4.1	Controls in offshore operations	41
3.4.2	Access rights	42
3.4.3	Passwords and user accounts	47
3.4.4	Monitoring access to customer data	49
3.4.5	Authentication	51
3.4.6	Data back-up	53
3.4.7	Access to the internet and email	56
3.4.8	Key-logging devices	59
3.4.9	Laptops	60
3.4.10	Portable media including USB devices and CDs	63
3.5	Physical security	65
3.5.1	Access to firms' premises	66
3.5.2	Clear-desk policy	68
3.5.3	Storage of paper customer files	68
3.6	Disposing of customer data	70
3.6.1	Procedures for disposing of confidential paper	70



3.6.2	Procedures for disposing of obsolete computers and other electronic equipment	72
3.7	Managing third-party suppliers	75
3.7.1	Why do third parties matter?	75
3.7.2	Firms' management of third-party suppliers	76
3.7.3	Issues for firms to consider when using third-party suppliers	77
3.8	Internal audit and compliance monitoring	80
3.8.1	Internal audit	80
3.8.2	Compliance monitoring	81
4.	Consolidated examples of good and poor practice	83
5.	Glossary	96
6.	References and useful links	99



1. Executive Summary

1.1 Introduction

1. This report describes how financial services firms in the UK are addressing the risk that their customer data may be lost or stolen and then used to commit fraud or other financial crime. It sets out the findings of our recent review of industry practice and standards in managing the risk of data loss or theft by employees and third-party suppliers.
2. We did not examine the threat of data theft by criminals seeking to infiltrate firms' systems by hi-tech means such as 'hacking' into computer systems.
3. Firms' responsibilities in this area are defined in our 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'.
4. 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. Rule 3.2.6R in our Senior Management Arrangements, Systems and Controls sourcebook (SYSC) requires firms to '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'. This is the minimum standard to meet the requirements of the regulatory system.
5. This report does not constitute formal guidance from the FSA. However, we expect firms to use our findings, to translate them into a more effective assessment of this risk, and to install more effective controls as a result. Small firms should consider the specific data security factsheets that we will make available to them on our website and monthly 'regulation round up' email. As in any other area of their business, firms should take a proportionate, risk-based approach to data security, taking into account their customer base, business and risk profile. Failure to do so may result in us taking enforcement action.
6. Firms should note that we support 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.¹ We may take enforcement action against firms that fail to encrypt customer data offsite.

1 www.ico.gov.uk/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx



7. This report is based on a systematic review by our Financial Crime and Intelligence Division (FCID) to find out how firms are responding to this risk. We visited 39 firms, including retail and wholesale banks, investment firms, insurance companies, financial advisers and credit unions. Half of our sample was firms supervised by our Small Firms Division. We consulted other stakeholders including the Information Commissioner's Office, law enforcement, trade associations, forensic accountants and compliance consultants regarding industry practice and the risk to consumers arising from poor data security. We also spoke to CIFAS – the UK's fraud prevention agency – who have conducted significant research on the impact of identity fraud on consumers.² In addition, we took into account our experience of data loss incidents dealt with by our Financial Crime Operations Team. During 2007, the team dealt with 56 cases of lost or stolen customer data from financial services firms. Of course, these were only the losses which were reported to us by firms or identified by the team. We judge it to be highly likely that many data loss incidents go unreported.
8. The main purpose of the review was to gather information on current data security standards, identify good practice to share with the industry and highlight areas where improvement is required. The proactive identification of potential enforcement cases was not an objective of our review, but we have referred one firm to our Enforcement division as a result of our findings. However, we will be issuing guidance to supervisors to ensure data security is reviewed as part of normal supervision. If firms fail to take account of this report and continue to demonstrate poor data security practice, we may refer them to Enforcement. In addition, we are likely to repeat this project to see if standards have improved.
9. We would like to thank the firms that participated in the review for the information they supplied before and during our visits, and for meeting us.
10. A glossary of terms used in this report can be found in Section 5.

1.2 Findings

11. Many firms are failing to identify all aspects of the data security risk they face, for three main reasons. First, some do not appreciate the gravity of this risk; second, some do not have the expertise to make a reasonable assessment of key risk factors and devise ways of mitigating them; and third, many fail to devote or coordinate adequate resources to address this risk.
12. Large and medium-sized firms generally devote adequate resources to data security risk management but there is a lack of coordination among relevant business areas such as information technology, information security, human resources, financial crime, and

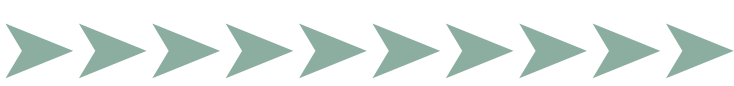
² See: www.cifas.org.uk/default.asp?edit_id=577-73



physical security. There is too much focus on IT controls and too little on office procedures, monitoring and due diligence. This scattered approach, further weakened when firms do not allocate ultimate accountability for data security to a single senior manager, results in significant weaknesses in otherwise well-controlled firms.

13. Firms' risk assessment of their exposure to data loss incidents is often weak. Some make no risk assessment at all and only a few continuously monitor the effectiveness of their data security controls. In some medium-sized and small firms, there is a lack of awareness that customer data is a valuable commodity for criminals. As a consequence, systems and controls are often weak and sometimes absent. 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. It is good practice for firms to conduct a risk assessment of their data security environment and implement adequate mitigating controls. If firms consider that their in-house resources or expertise are inadequate to perform a coherent risk assessment, they should consider seeking external guidance.
14. Our experience of dealing with data loss incidents shows that firms often fail to consider the wider risks of identity fraud arising from significant cases of data loss. Many firms appear more concerned about adverse media coverage than in being open and transparent with their customers about the risks they face and how they can protect themselves. However, some firms which suffer data loss are beginning to take a more responsible approach by writing to their customers to explain the circumstances, give advice and, in some cases, pay for precautions such as credit checking and CIFAS Protective Registration.³
15. Firms' vetting of staff is variable. In most firms, more-stringent vetting is applied to staff in senior positions – there is little consideration of the risk that junior staff with access to large volumes of customer data may facilitate financial crime. Consequently, very few firms conduct criminal record checks on junior staff. In addition, few firms repeat vetting to identify changes in an individual's circumstances which might make them more susceptible to financial crime.
16. Data security policies in medium-sized and larger firms are generally adequate but implementation is often patchy, with staff awareness of data security risk a key concern. Training for front-line staff (e.g. in call centres), who often have access to large volumes of customer data, is rarely relevant to their day-to-day duties and focuses more on legislation and regulation than the risk of financial crime. This means staff are often unaware of how to comply with policies and do not know that data security procedures are an important tool for reducing financial crime. In addition, many firms do not test that their staff understand their policies.

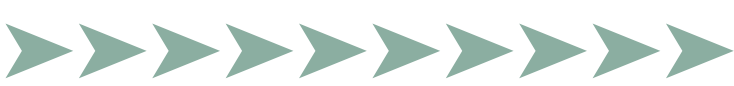
3 CIFAS offers a service called Protective Registration which requires anyone applying for credit in that person's name to undergo additional checks. The product, supplied by the Equifax credit bureau, costs £12 plus VAT. CIFAS have recently launched a 'bulk' Protective Registration facility for firms to use in cases of mass data loss.



17. Access to customer data via computer systems and databases is generally well controlled in large and medium-sized firms, with a general aim of only allowing staff to access information that they specifically require to do their job. In small firms, it is not unusual for all staff to have access to all customer data.
18. Firms' dealings with third-party suppliers are a major concern. Many firms, small and large, use third parties for IT maintenance, as well as the backing up of electronic files and archiving of paper documents. Firms generally rely too much on assumptions that contractual terms are being met, with very few firms proactively checking how third parties vet their employees or the security arrangements in place to protect customer data. In addition, some firms do not consider the risk associated with granting third-party suppliers such as cleaners and security staff access to their premises.
19. Large and medium-sized firms tend to transfer data to and from third parties using secure internet links but there are still occasions where data is transferred on CDs or mainframe cartridges. We observed that these items are not always encrypted. On rare occasions, firms are sending unencrypted customer data by unregistered post.
20. Large and medium-sized firms usually recognise the risks of data loss via laptops, USB devices and the internet. But few firms completely mitigate data security risks by locking down USB ports and CD writers, encrypting laptops and USB devices and blocking web-based communication facilities such as Hotmail and instant messaging. Small firms are very weak in this area, with few of them identifying or mitigating risks.
21. Disposal of confidential paper is generally very good, with most firms shredding sensitive documents either onsite or via a suitably-accredited supplier. This is likely to be the result of significant media attention on this subject (e.g. BBC Watchdog) as well as, in March 2007, the Information Commissioner's Office's public censure of firms disposing of customer data carelessly.
22. Compliance and Internal Audit of data security in large and medium-sized firms is variable. Some firms' compliance and audit staff lack the necessary understanding of the subject or technical expertise. As with firms' governance of data security in general, compliance and internal audit functions often lack coordination, do not examine data security holistically and do not pay adequate attention to the non-IT aspects of data security. Small firms are often wholly reliant on compliance consultants who we found do very little – if any – work on data security. So the standard of small firms' compliance checking – and their overall performance on data security – is very weak indeed.

1.3 Conclusions

23. This review and the incidents we have dealt with since the formation of our Financial Crime & Intelligence Division (FCID) at the beginning of 2007 has led us to conclude that poor data security is currently a serious, widespread and high-impact risk to our objective to reduce financial crime.



24. Recent incidents of data loss have brought many firms to consider data security for the first time. Some progress has been made: firms in general are beginning to understand more about this risk and are becoming more assertive in their efforts to contain it. However, there exists a very wide variation between the good practice demonstrated by firms committed to ensuring data security, and the weaknesses seen in firms that are not taking adequate steps to treat fairly the customers whose data they hold.
25. Overall, data security in financial services firms needs to be improved significantly. Many firms, particularly small firms, still need to make substantial progress to protect their customers from the risk of identity fraud and other financial crime.

This review was conducted by Robert Gruppetta, Stephen Oakes, Laura Covill and Emma Richardson.

This report is published for information; however, your comments are welcomed.
Please contact:

Financial Crime Operations Team
Financial Services Authority
25 The North Colonnade
London
E14 5HS

Email: rob.gruppetta@fsa.gov.uk or stephen.oakes@fsa.gov.uk

Telephone: 020 7066 0140 or 020 7066 5530



2. Introduction

2.1 Objectives

26. This report is the result of a significant effort during 2007 to examine how firms safeguard customer data. We investigated how financial services firms assess and manage their data security risks, how these risks are changing, and how they impact on our statutory objectives.
27. Our four statutory objectives are:
- *market confidence*: maintaining confidence in the financial system;
 - *public awareness*: promoting public understanding of the financial system;
 - *consumer protection*: securing the appropriate degree of protection for consumers; and
 - *the reduction of financial crime*: reducing the extent to which it is possible for a business to be used for a purpose connected with financial crime.
28. Financial crime includes money laundering, market abuse and fraud or other dishonest practices. The risk of data loss and subsequent fraud is relevant to all four of our objectives for the following reasons:
- *the reduction of financial crime* because poor controls over customer data present opportunities for thieves and fraudsters to steal data and commit identity fraud and other financial crime;
 - *consumer protection* because data loss, especially on a large scale, could cause significant detriment to individuals;
 - *market confidence* could be affected by large data loss which causes consumers to question the integrity or safety of the financial sector or service delivery channels, such as online banking; and
 - *consumer awareness* is also relevant, because people should take responsibility for keeping their own personal data safe.
29. We have highlighted data security as a significant issue in our Financial Risk Outlook in 2008 and the four previous years.⁴

‘Personal data remains a high-value commodity for criminals, with both the market in consumer details and the technology used by criminals continuing to evolve.’

FSA Financial Risk Outlook 2008

⁴ www.fsa.gov.uk/Pages/Library/corporate/Outlook/index.shtml



2.2 Background

30. In January 2007, we created a new Financial Crime and Intelligence Division (FCID). The division brings together financial crime experts that were previously spread throughout the organisation. It is equipped to address financial crime issues more intensively, in particular by checking firms' systems and controls for assessing and mitigating risk. The new centre of excellence provides advice and intelligence to the rest of the FSA, particularly firms' supervisors. FCID also undertakes thematic and case work on financial crime issues.
31. In 2007, FCID's Operations Team dealt with 56 cases of data loss by financial services firms. This accounted for just under a third of all financial crime cases dealt with by the team. In fact, data security was the most common type of financial crime incident dealt with during the year. These cases have revealed some serious weaknesses in firms' data security.
32. As a result of this developing trend, FCID reviewed data security in financial services firms, visiting 39 of them to find out how well they are identifying and tackling the risks of data loss. We examined how customer data is stored in electronic databases, paper files and with third-party suppliers; the controls in place to restrict access to customer data and prevent it from being lost or stolen; and how redundant customer data is disposed of securely.
33. We looked at some technical aspects such as passwords and encryption of laptops and other portable devices. However, we did not examine the threat of data theft by criminals seeking to infiltrate firms' systems by hi-tech means such as 'hacking' into computer systems.
34. This report describes the findings of the review and sets out examples of good and poor practice observed. It also describes some of the general trends we saw in the financial services industry, as well as risks that were specific to particular segments of it.
35. We discussed our intention to carry out this project when we gave evidence to the House of Lords Select Committee on Science and Technology in December 2006 and our Executive Committee approved the project on 2 March 2007.
36. We last published a detailed review of firms' information security controls in November 2004. It concluded that firms could be more active in managing relevant risks rather than being reactive to events and could protect better their own assets and those of their customers from the risk of fraudulent activity.⁵
37. We expect firms to use our findings, to translate them into a more effective assessment of this risk, and to install more-effective controls as a result. As in all areas of their business, firms should take a proportionate, risk-based approach to data security taking into account their customer base, business and risk profile. If firms fail to do this, we may take enforcement action.

⁵ See www.fsa.gov.uk/pubs/other/fcrime_sector.pdf



2.3 Methodology

38. We began the fieldwork for our review in April 2007 and continued it until December 2007. From April until June, we sought the views of 12 important stakeholders, including the Information Commissioner's Office, trade associations, law enforcement, forensic accountants and compliance consultants used by small firms. Overall, these meetings suggested that, while some firms were taking data security seriously and had good systems and controls in place, there was the need for significant improvement across the financial services industry.

'Firms do not understand the value to criminals of customer data.'

'Generally, firms are only concerned about data security risk if there is some risk to their own business – they are not concerned about protecting their customers from wider identity theft.'

'I have never seen a risk assessment which cuts across all aspects I would expect to be covered.'

A 'big four' forensic accountant.

39. We visited 39 firms, including retail and wholesale banks, investment firms, insurance companies, financial advisers and credit unions. Half our sample comprised firms supervised by our Small Firms Division. We selected 20 small firms for visits by sending a simple questionnaire to 110 small firms and analysing the quality of their responses. We ensured that our review included firms that had given both good and poor responses to our questionnaire, and that it was focused on firms spread across the UK.
40. We interviewed staff with key roles in each firm to get a balanced view of how data security is handled, and identify at what level in the management structure it was dealt with. Where dedicated roles existed, we usually met managers responsible for information security, fraud, staff vetting, IT operations, compliance and internal audit. Where separate roles did not exist, for example in smaller firms, we met the individual with general responsibility for data security. We also met front-line staff to assess their understanding of policies and procedures, the quality of the training they received, whether their access to customer data was appropriate, and to conduct some limited testing of controls.
41. We also assessed:
- firms' understanding of and attitude to data security risk and identity fraud (section 2.7);
 - the quality of risk assessment and related processes (section 3.1.3);
 - staff recruitment and vetting procedures (section 3.3);
 - IT controls, including those relating to laptops and other portable devices, and using the internet and email (section 3.4);

- staff access to electronic and paper-based customer data (section 3.4.2);
- physical security (section 3.5);
- disposing of paper records and redundant computers (section 3.6); and
- potential access to customer data by third-party suppliers of services such as IT consultancy, call centres and archiving firms (section 3.7.2).

Our sample

Type of firm	Total	FSA Supervisory Division			
		Major Retail Groups	Wholesale Firms	Retail Firms	Small Firms
Banks	6	2	3	1	
Building societies	2			2	
Credit unions	2				2
Insurance (Life and General)	7	1	1	4	1
Investment firms	22		1	4	17
Total	39	3	5	11	20

2.4 How data loss occurs

42. We have identified data security as a key risk because financial services firms, by the nature of their business, generally hold lots of data about their customers. Most firms hold an extensive stock of personal and financial data: names; addresses; dates of birth; contact details; national insurance numbers; passport numbers; bank account details; family circumstances; transaction records; passwords; PINs and so on.
43. There are many reasons for this. For example, the ‘know your customer’ (KYC) provisions of the anti-money laundering (AML) regime often require firms to gather documentary evidence of customers’ identity. Firms must also gather information about their customers’ personal circumstances to ensure they are offering appropriate products. Lenders ask their customers for details of employment, income and indebtedness, while life insurers require medical details.
44. Despite the Data Protection Act’s requirement for firms holding customer data to keep it secure, data is sometimes lost, either through error – such as when an employee loses a company laptop – or theft. Firms are vulnerable to both types of loss.



45. During 2007, FCID handled 187 financial crime cases and 56 of them involved data loss. This made data loss the most common type of financial crime incident reported to us last year. The most common reasons for the loss of data were the theft of a portable device such as a laptop or memory stick; data lost in the post and data lost by third-party suppliers. Only two cases reported to us involved malicious insiders. However, these were only the data losses reported to us by firms or identified by the team. We judge it to be highly likely that many data losses either are not identified or go unreported.
46. We have found that, in cases of data theft, firms often assume the thief was focused on the value of the equipment rather than the data on it. Although this may often be the case, there is a risk that criminals will use data for criminal purposes or sell the data on through criminal networks to specialist identity fraudsters.

2.5 How lost data is used for identity fraud

47. The implications of data loss are very serious. Criminals with access to lost or stolen data, particularly highly-confidential information such as national insurance numbers, payment card and banking information, can use it to commit identity and other frauds, according to the Serious Organised Crime Agency's (SOCA) Threat Assessment 2006/07. Firms have told us these frauds include false credit applications, fraudulent insurance claims, fraudulent transactions on a victim's account and even a complete account takeover.
48. These crimes are sometimes the work of opportunistic criminals but they are also carried out by organised criminal groups that possess expert knowledge of data technology. CIFAS has found that fraudsters often get help from insiders in financial services firms.
49. There is a mature and transparent international market for stolen customer data, including data belonging to UK citizens, according to PricewaterhouseCoopers, a consulting firm. Sets of data are bought and sold freely in social settings such as pubs and clubs and subsequently traded through criminal networks that often operate on the internet. Identity fraudsters use sophisticated technology to make full use of the stolen data, both by creating false documents and by making fraudulent transactions.
50. The proceeds of these crimes can be laundered within criminal networks and may be used to fund other criminal activities, including drug trafficking, human trafficking and terrorism. Indeed, identity fraud underpins a wide variety of serious organised criminal activities, according to the SOCA Threat Assessment 2006/07.
51. The impact on the consumer can be very serious, according to CIFAS. Victims of identity fraud suffer considerable inconvenience and possible financial detriment. They often need to spend substantial time and effort repairing their credit record, and repairing the damage done by fraudsters. In the meantime, their credit scores can be impaired, potentially affecting their ability to obtain a mortgage or find a new job. This stress and financial burden might continue for years, since identity fraudsters often strike



repeatedly. This is because customer data may be repackaged and re-sold many times over to criminals who are difficult to trace and prosecute, given the covert and often international nature of their activities.

One firm we visited described how some job applicants discovered they had become victims of identity fraud only when their credit history was examined during pre-employment checks.

52. There is also evidence that consumers' fears about data loss affect their willingness to use new delivery channels; almost one in three internet users say they do not bank online because of concerns about security.⁶

It can take between 3 and 48 hours of work for a typical victim of identity fraud to undo the damage done by fraudsters. In cases where a total identity hijack has occurred, perhaps involving 20 or 30 different firms, it may take the victim over 200 hours and cost them up to £8,000 before things are put right. They may suffer considerable (albeit temporary) damage to their credit status, which may then affect their ability to obtain finance, insurance or a mortgage.

Source: CIFAS

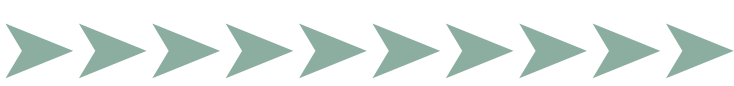
53. Consumers have become much more aware in recent months of the dangers of identity fraud. No one in the UK can be ignorant of the potential harm of data loss following several well-publicised incidents. These included two compact discs holding data on all recipients of child benefit lost in transit from HM Revenue & Customs, a laptop containing a large amount of customer data stolen from a member of Nationwide Building Society staff; and the Information Commissioner's Office's public censure of 12 firms found to be disposing of customer data carelessly.

We fined Nationwide Building Society £980,000 for failing to have effective systems and controls to manage its information security risks (see our Final Notice of 14 February 2007).⁷

54. These cases – and many campaigns to raise awareness of identity fraud – have encouraged consumers to keep their personal financial records safe, check their credit records for any unusual transactions, and exercise discretion in revealing any personal details to others. CIFAS, the UK Fraud Prevention Service, reports that, in 2006, 80,000 people applied for CIFAS Protective Registration – a protective measure to reduce the risk of identity fraud – compared with 24,000 people five years earlier.

⁶ Get Safe Online Report 2007, Get Safe Online

⁷ See www.fsa.gov.uk/pubs/final/nbs.pdf



2.6 Firms' responsibilities

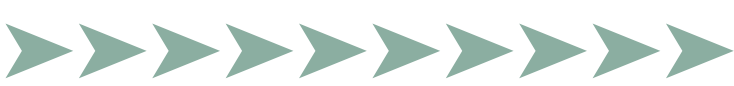
55. The safekeeping of customer data is a crucial responsibility for firms. We have emphasised the importance of data security for several years, and we currently regard poor data security controls as a serious, widespread and high-impact financial crime risk.
56. Firms' responsibilities in this area are defined in our 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'.
57. 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'.
58. So firms have a responsibility to assess the risks of data loss and take reasonable steps to prevent that risk occurring. SYSC 3.2.6A says firms' relevant systems and controls must be 'comprehensive and 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 and information assets be exploited by thieves and fraudsters. Consumers are entitled to rely on firms to ensure their personal information is secure.

Firms should note that we support 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. We may take enforcement action if firms fail to encrypt customer data taken offsite.

59. The secure handling of customer data is also part of the 'Treating Customers Fairly' standard that all firms must adhere to. Financial services firms, particularly banks, are often the first to be told when a customer becomes the victim of fraud. Indeed, the principal response to financial fraud in the UK is action by firms, mainly through anti-fraud systems and controls that must constantly evolve to counter the threat. So it is good practice for firms to have procedures in place to investigate fraud and help the customer where appropriate. For example, firms can place blocks or anti-fraud flags on an account, change details and passwords and provide advice to the consumer on how they can protect themselves from further fraud.

2.6.1 Legal requirements

60. 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 are to be processed and may include financial services firms. There is also a requirement for



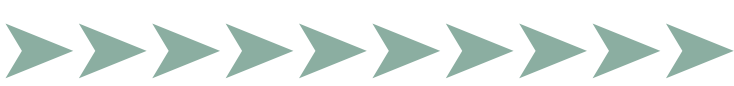
a data controller to notify the Information Commissioner’s Office (ICO) of their processing of personal data, so the ICO can maintain a public register. The ICO has certain powers and duties under the DPA to ensure that data controllers comply with this legislation. So it is important that firms are 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’.

61. 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 and 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 and identity fraud in the media and among consumers.

2.7 Attitudes to data security and identity fraud

2.7.1 Five fallacies

62. This review – and the continuing series of data losses reported to us – has revealed misconceptions among many firms about the risk of data loss and identity fraud.
 - i. The management of some firms believed the customer data they held was 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 – telephone directories, the electoral roll and other public records, many of which are available on the internet. They also use impersonation, for instance during phone calls or in emails, to encourage the victim to reveal more. Ultimately, they build up enough information to pose as their victim and obtain credit and other advantages in the victim’s name. In this way, a firm’s customer data might complete a set of data extensive enough to commit fraud.



- ii. There is a perception that 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. Recent data published by CIFAS⁸ shows the top ten postal districts affected by identity fraud are not all in affluent areas.
 - iii. A third fallacy is that only large firms with millions of customers are likely to be targeted. Even a small firm's customer database might be sold and re-sold for a substantial sum.
 - iv. Firms often assume the threat to data security is external – from burglars or computer hackers, for example. However, insiders have more opportunity to steal customer data and there are many examples of staff stealing customer data either to commit fraud themselves, or to pass it on to organised criminals.
 - v. Finally, some firms' believe that their firm is impervious to data breaches, because no customer has ever alerted them to identity fraud. The truth may be closer to the opposite: firms which 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, the source of data loss is often impossible to trace. Data is held in so many places: by government, retailers, employers and many others besides financial services firms. A victim of identity fraud rarely has the means to identify where their data was lost.
63. These common misconceptions mean some firms are failing to recognise that data security is their responsibility. The result is that they often have weak systems and controls to prevent data loss or theft. Other firms recognise the risk, but rate it so low that it never attracts the attention of senior management, nor is it allocated adequate financial or human resources.
64. Some firms regard data security as the sole responsibility of IT staff, whose responsibilities include creating technical systems and controls to prevent data loss. In fact, many of the good practices highlighted in this report are simply common sense which require input from many areas of a firm's business.
65. Some firms which lose data recognise the risks to their own reputation and business but overlook the wider risks to their customers. Data stolen from a financial services firm might not be used to compromise accounts at that firm, but could, for instance, be abused to create a false passport. The personal risk to customers arising from data loss is very broad and is certainly not limited to their dealings with the firm which lost the data.

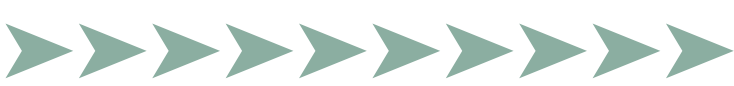
8 www.cifas.org.uk/default.asp?edit_id=789-57



2.7.2 Changing attitudes

66. These attitudes must change in the short term, for several reasons:
- i. Identity fraud is a growing financial cost for firms, because fraudsters make additional charges on credit cards, or debits on bank accounts. Credit card issuers and other lenders usually bear these costs. Loans and mortgages obtained fraudulently, using false identities, are rarely repaid in full.
 - ii. Data security is an essential aspect of Treating Customers Fairly (TCF), and in particular relevant to the first of the six TCF outcomes, that consumers can be confident that they are dealing with firms where the fair treatment of customers is central to the corporate culture. By the end of March 2008, firms were expected to have appropriate management information or measures in place to test whether they are treating their customers fairly.
 - iii. Firms suffer reputational damage if data entrusted to them is lost or stolen, particularly if they cannot demonstrate adequate preventative controls. We now regard it as good practice for firms to tell their customers of data loss, even if it is not demonstrably the firm's fault, unless there is law enforcement or regulatory advice to the contrary.
 - iv. A firm's operations will be undermined by any successful attempt to infiltrate them and steal data. The firm must bear the costs of the disruption and repairs to the systems. A study by the Ponemon Institute⁹ published in February 2008 found the average cost to UK firms of a data loss incident was £55 for each customer record.
 - v. We are increasingly concerned and vigilant about data security and there is now a pattern of enforcement action to raise standards. Although the proactive identification of potential enforcement referrals was not an objective of our review, one firm has been referred to enforcement based on our findings.
67. So it is in firms' interest to have a good awareness of data security and to establish effective controls to prevent their customer data from being used for financial crime. We expect this report will help firms understand better their responsibilities for securing customer data, enable them to undertake more accurate risk assessments, and take more effective action to prevent data loss.

⁹ www.symantec.com/about/news/release/article.jsp?prid=20080225_02



2.7.3 Changing behaviour

68. Our review found signs that firms are becoming more aware of the potential cost of losing customer data, both to themselves and their customers. But we found that firms could do much more to improve the systems and controls in place to protect customer data. Firms' internal controls are fundamental in ensuring customers' details remain as secure as they can be and, as technology evolves, firms should keep their systems and controls up to date to prevent lapses in security.
69. Despite the improvements, most firms still need more time and further public examples of good and poor practice to make improvements to their systems and controls to prevent data loss. This report provides many such examples – in Section 4, you will find consolidated examples of the good and poor practice we saw during our review.



3. Findings

3.1 Governance – managing systems and controls

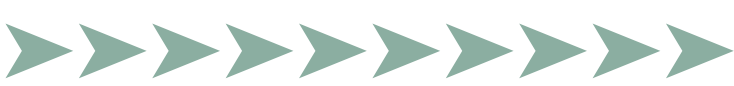
70. Governance can be defined as the way a firm runs its business. It includes aspects such as strategy, objective setting and deciding risk appetite. It also encompasses the culture and values driven through the business by senior management.
71. During our visits to firms, we discussed with senior management what their policies, procedures and risk appetite were in relation to data security, how they performed data security risk assessments and how they communicated and monitored performance against those assessments.
72. It was evident from our review that the level of awareness of data security risks varied considerably across the industry. Many firms had not yet considered data security as a specific risk, so had not conducted a data security risk assessment. In addition, there was a lack of awareness in some firms that data security is an important aspect of fighting identity fraud and other financial crime. Firms that did not recognise this often had serious weaknesses in their systems and controls and, in some cases, controls were completely absent.

A medium-sized insurance company, despite having a Fraud Committee, had never discussed data security at that committee. In addition, there was no IT representation on the committee – despite the fact that IT was the department with responsibility for data security.

73. This lack of awareness was sometimes demonstrated by poor pre-visit information provided by firms. Some firms, for example, did not suggest that we meet all staff with important roles to play in keeping customer data secure. Indeed, it appeared that some firms believed that only IT staff had a role to play in ensuring data security. In addition, a significant number of small firms did not consider the risk posed by insiders and focused their attention solely on external threats such as computer hackers.

A financial adviser told us the main threat to customer data would arise from a fire or flood at the office. They had not considered the risk of data loss or theft.

A medium-sized investment firm had not identified that high staff turnover and low staff morale might increase the risk of data loss or theft.



74. Data security is not simply an IT issue. The responsibility for ensuring data security should be coordinated across the business. Senior management, information security, human resources, financial crime, physical security, IT, compliance and internal audit are all examples of functions that have an important role to play in keeping customer data safe.
75. With several well-publicised incidents of data loss during 2007, nobody in the UK can claim ignorance of the risks which arise from customer data falling into the wrong hands.

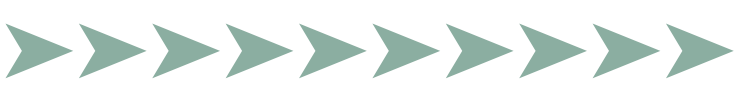
3.1.1 Policies and procedures

76. If a firm's management is committed to ensuring data security, it is likely to have specific written policies and procedures covering the subject. We were not convinced by firms that claimed to have detailed data security rules but were unable to produce written policies and procedures. Indeed, the existence or absence of an up-to-date, accurate and relevant data security policy can be a telling indication of whether the firm really understands the risk and takes it seriously.

Some firms' written policies and procedures did not reflect their actual day to day practices.

77. Firms with large or complex operations tended to have detailed policies and procedures. Typically, the data security policy was a high-level document supplemented by more detailed procedures and guidance for different business areas relating to the specific risks they faced. Small firms, with their more-manageable risks, did not always have formal policy documents and used simple guides of 'Do's and Don'ts' as an effective way of setting out expectations and communicating them. However, in a worrying number of cases, firms failed to record policies and procedures at all. In these firms, senior management were effectively relying on the judgement of individual staff – often with little or no understanding of the risks – as their only data security control. This approach was typical of some small firms whose managers appeared to treat data security more as a matter of office administration than as a potentially significant risk that could affect their business, reputation and customers.
78. Good policies and procedures specify exactly what staff and contractors must do – and not do – to comply with expected standards and provide the means for enforcing them. Firms that do not set out or communicate clearly the standards they expect are running the risk that their staff do not understand what is expected of them; data security risk in these firms is likely to be high. The importance of training and awareness is covered in Section 3.2.

A small financial adviser we visited did not have a dedicated data security policy. Some other internal policies covered the subject in a piecemeal fashion but some important aspects were not covered at all. Overall, the policies were inadequate.



3.1.2 Benchmarking

79. There is an international quality standard for data security: the ISO 27001 Security Management Standard which was introduced in 2005.¹⁰ Some firms, particularly larger firms with dedicated information security officers, were aware of this code of practice and used it as a benchmark. However, it was interesting to observe that even some of the largest firms had not obtained certification to this standard.

3.1.3 Risk assessment

80. As in any other area of their business, firms should take a proportionate, risk-based approach to data security, taking into account their customer base, business and risk profile. Like any complex risk area, managing data security requires a systematic attempt to understand which risks are greatest and where a data loss is most likely.
81. Many firms are failing to identify all of the data security risks they face, for three main reasons. First, some do not appreciate the gravity of this risk; second, some do not have the expertise to make a reasonable assessment of the risks and devise ways of mitigating them; and third, many fail to devote or coordinate adequate resources to this risk.

We found that some firms' staff could talk knowledgeably about data security risks facing their business, but the firm itself had never performed a data security risk assessment.

82. Very few firms had performed a risk assessment that identified and assessed all data security risks relevant to their business. We found that firms often had adequate resources across the business to manage data security risk effectively but failed to bring these resources together. Indeed, it was not unusual for many different departments to be working on different aspects of data security but not communicating with each other.

It is good practice for firms to ensure that data security risk management is joined-up and that different departments are not working separately.

83. This lack of coordination, further weakened when firms do not allocate ultimate accountability for data security to a senior manager, can result in serious weaknesses in otherwise well-controlled firms. Firms that have not given a senior manager ultimate responsibility for data security may struggle to ensure effective communication between key stakeholders in the business. They may also fail to ensure that systems and controls are updated to take account of emerging or evolving risk.

¹⁰ www.17799.standardsdirect.org/



A small number of firms had drawn on expertise from across the business to perform a data security risk assessment and formed an Information Security Committee (or equivalent) with all relevant functions represented. This coordinated approach is good practice.

84. We appreciate that, for small firms, a single senior manager often has wide-ranging responsibilities and they might not have in-depth expertise in all of these areas. Despite this, the increasing coverage of data loss incidents means firms should now be aware of the risks to consumers that arise from data loss. So, if firms think their in-house resources or expertise are inadequate to perform an effective risk assessment, they should consider seeking external guidance.

During our review, and when dealing with cases of actual data loss, we have observed that some firms have a reactive approach to data security risk assessment. It appears that some firms are willing to wait for a data loss to occur before considering data security risk.

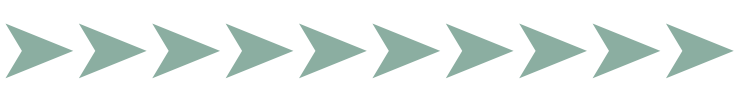
85. Without a dedicated risk assessment, firms may allocate their resources inappropriately and expose themselves and their customers to unnecessary risk.

3.1.4 Organisation, monitoring performance and communication

86. The few firms which we judged to have effective systems and controls to mitigate the risk of data loss had usually set up a committee or working group with responsibility for data security. The committees and working groups monitored the effectiveness of data security controls in practice and ensured that weaknesses were escalated to the board as appropriate. In addition, the existence of a data security committee sent a very clear message to staff about the level of importance senior management gave to data security. This helped to embed a good data security culture across the firm.
87. Interestingly, although many firms had controls in place that addressed key aspects of data security, they had not always been put in place for this reason, and the firm did not always consider them to be a data security control.

Effective and timely communication between line management, human resources, security and IT is essential in preventing unauthorised access to buildings and IT systems when staff leave firms. Despite this, line management and human resources were sometimes unaware about how the 'leavers process' was relevant to data security. Sometimes they believed it was there only to ensure staff were removed from the payroll or allocated to the correct cost centre in the business.

88. The example above highlights the importance of data security awareness and regular communication between key stakeholders in firms. It also demonstrates that an effective data security environment requires that management from across the business work in a coordinated way and assesses regularly the effectiveness of the firm's controls.



3.1.5 External liaison

The importance of sharing information about good practice

89. A good awareness of current and emerging data security threats is needed if firms are to assess risk properly and put in place effective systems and controls.
90. Many firms face similar data security risks, so it makes sense for them to share relevant knowledge and experience as widely as possible. Some firms recognised this and were networking extensively to discover and share best practice through professional and trade associations, networking meetings, conferences and online forums.
91. Our review found that IT managers who also had responsibility for data security tended to be the most active communicators. The professional groups and associations most commonly mentioned to us were the Jericho Forum, the British Bankers Association, APACS, CIFAS, the Information Risk Executive Council, the Security Institute, the North East Fraud Forum and the Information Systems Audit and Control Association. Managers of call centres focused on conferences and online message boards operated by the Customer Contact Association, which extends beyond financial services to other industry sectors.

One firm reviewed was not taking obvious opportunities to learn about best practice. The firm was the UK arm of a large financial services corporation based in the United States. However, the firm had not discussed data security with its parent company and its overall performance on data security was weak.

92. We encourage firms to share information on data security for the benefit of the financial services sector as a whole. This is in line with our general fraud policy and complements our direct communication with firms on financial crime issues.

Difficulties for small firms

93. Many firms, particularly small firms, had no relevant contacts, nor were they aware of opportunities to learn more about data security; so their level of data security poor. While some admitted they did not see any need for any such communication, others did not take available opportunities to learn more about good practice. A third group did not know where to find the information they needed to improve their knowledge. Without adequate understanding of the risks or any means to gain that understanding, these firms may well fall further behind their more inquisitive and well-informed peers.
94. Small firms tended to rely on small networks of their peers. One small financial advice firm included in the review informed other members of their network about our interest in data security. The firm's managers told us that they would also pass on the knowledge and issues learnt during our visit.



One small firm commented that a SOCA officer went to speak to their staff about financial crime issues, after the firm's senior management made contact with the officer at a conference.

95. As noted in paragraph 22, small firms are often wholly reliant on compliance consultants who, we found, do very little – if any – work on data security. We would encourage compliance consultants to do more work with small firms on data security. We intend to contact the compliance consultancy firms most often used by small firms shortly after this report is published to update them on our findings and the importance we attach to good data security.

3.1.6 Data loss reporting and response

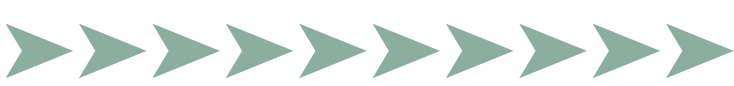
96. We expect senior management to encourage an open and honest culture of reporting data security incidents and issues. This may require transparent reporting mechanisms to be provided for staff and third parties. Reporting mechanisms do not need to be complicated. Staff must simply know that all data security breaches must be reported and who to report them to, and it is good practice for management to ensure the reporting process has been tested. An open culture where innocent mistakes or concerns can be reported by staff without fear of blame will help firms react quickly and appropriately both to control weaknesses and data losses.

A medium-sized bank had a well-documented and tested incident response plan. They regularly tested the plan with spoof data security attacks to ensure that escalation to Board level and response by the business was timely and adequate. Improvements were made to the response plan as a result of the test.

97. Overall, few firms had a plan for reacting to a data loss. It was noticeable that firms that did not have data loss reporting mechanisms or response plans in place had generally not identified any data losses in the past. In other firms, senior managers believed that if a data loss occurred, an effective plan could be created spontaneously.
98. A well-defined response plan enables a firm to bring together quickly knowledge and expertise to assess the impact of the risks arising from a data loss. This is good practice for all firms, especially those with substantial relevant risks such as large customer databases and the extensive use of laptops, other portable devices and third-party suppliers.

3.1.7 Notifying customers of data loss

99. When customer data is lost, consumers that are affected have a right to know the enhanced personal risk they face so they can take adequate precautions. Even if there is



no evidence of theft or fraud, it is good practice for firms to inform affected customers of a data loss in writing, unless the data is encrypted or there is law enforcement or regulatory advice to the contrary. Firms should consider telling affected consumers exactly what data has been lost, give them an assessment of the risk and give advice and assistance to consumers at a heightened risk of identity fraud.¹¹

100. Our experience of dealing with cases of data loss shows firms are still learning to communicate appropriately with customers affected by data loss. A financial adviser did the right thing by writing to a group of customers whose account-opening forms had accidentally been thrown away by cleaners. But the letter acknowledged the risk without helping customers take precautions against identity fraud. It said: ‘We wish to apologise for this most unfortunate incident, and also to let you know that the cleaning company stated that it was a genuine mistake and that the account opening information was destroyed at the compressing plant. We understand that this event will be of considerable concern to you, as it is to us. We hope that by notifying you of this matter, you will have the opportunity to take whatever remedial steps you consider appropriate.’
101. It would have been better practice for the firm to assess the risk itself, rather than quoting the cleaners’ assertion that the documents were destroyed. In addition, the firm could have suggested measures that their customers could take to protect themselves against identity fraud.
102. In a significant number of cases of data loss brought to our attention, firms have failed to consider the wider risks of identity fraud arising from data loss. Indeed, many firms appear more concerned about adverse media coverage than in being open and transparent with their customers about the risks they face. However, some firms are beginning to take a more responsible approach by writing to their customers to explain the circumstances, give advice and some are even offering to pay for precautions such as credit record checks and CIFAS Protective Registration.

A building society sent a computer cartridge containing 6,500 customers’ data to a government agency to fulfil legal reporting obligations. On arrival, the cartridge was missing from the package and could not be traced. Although the building society believed it was not at fault, it wrote to all customers concerned, explaining the circumstances, assessing the risk, and offering advice about how customers could safeguard their identities and credit records.

11 The government-backed Identity Fraud Consumer Awareness Group (IFCAG) gives consumers advice about how to protect themselves from identity fraud at: www.identity-theft.org.uk/protect-yourself.html

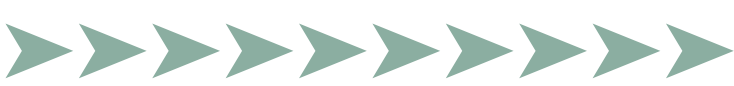


Governance – examples of good practice

- Identifying data security as a key specific risk, subject to its own governance, policies and procedures and risk assessment.
- 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.
- 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.
- Written data security policies and procedures which are proportionate, accurate and relevant to staff's day-to-day work.
- An open and honest culture of communication with pre-determined 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.
- 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.

Governance – examples of poor practice

- Treating data security as an IT issue and failing to involve other key staff from across the business in the risk assessment process.
- No written policies and procedures on data security.
- Failing to understand the need for sharing knowledge on data security
- 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.



- A ‘blame culture’ that discourages staff from reporting data security concerns and data losses.
- Failure to notify customers affected by data loss in case the details are picked up by the media.

3.2 Training and awareness

103. Many firms devote significant time and resource to creating and updating policies and procedures for ensuring data security. However, even the best policies and procedures have little value if front-line staff are not aware of them or do not understand what they mean in terms of their day-to-day responsibilities. Our experience shows that many instances of data loss occur because staff do not know or understand relevant policies and procedures. So it is good practice for senior management to put in place appropriate training and awareness mechanisms to ensure that their staff understand the relevance of policies and procedures to their roles.

‘Staff were required to self-certify that they had read and understood Nationwide’s procedures for information security. Staff received generic training on the application of the information security procedures; but no job-specific training was provided. Having designed and implemented its procedures for information security, Nationwide failed to establish controls adequate to ensure that its procedures were understood, and that staff adhered to these procedures.’

FSA Final Notice of Enforcement action against Nationwide Building Society,
14 February 2007

104. Our review found that firms in general have substantial shortcomings in this important area. Many firms provided no training at all, and those that did often focused on the legal and regulatory aspects of poor data security rather than the financial crime risks that can arise from data loss. We found this approach often resulted in front-line staff being unaware of the importance of data security in reducing financial crime.
105. Many small firms tended to rely on a single staff member – often a secretary or administrator – to create data security procedures and communicate them to others. We noticed these individuals are often vigilant in reminding others of good practice such as locking filing cabinets and using complex passwords. However, their work was not usually based on a proper data security risk assessment and many important aspects of data security were often overlooked. This resulted in patchy and ineffective controls.



The 39 firms we visited were split into three broad groups:

- Nearly half (17) offered no training at all.
- Nine firms asked their staff to read their data security policy and certify that they had done so, but did not test staff's understanding of the policy.
- The remaining firms offered formal training on data security; ten of them, including some small firms, repeated that training every six months or once a year.

However, most firms did not test employees' understanding of the training received.

3.2.1 Poor assumptions about risk awareness

106. We found that, in some firms, senior management wrongly assumed their staff were aware of good data security practice even when there was no formal training in place to explain relevant policies and procedures. In addition, there was often an assumption that otherwise well-trained and honest staff would instinctively understand data security risk and know how to deal with it. These assumptions were misguided and we found that most front-line staff expected precise instructions from management about the procedures they should follow.

The manager of a call centre at a medium-sized insurance firm was unaware of the risk of call centre staff being approached by fraudsters seeking to buy or extort customer data. This lack of relevant knowledge meant the manager was unable to warn his staff about a key risk.

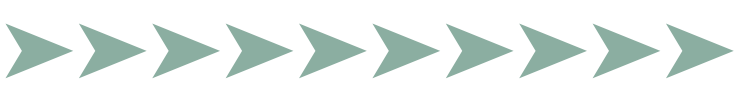
107. If data security is left to individual judgement, standards will vary and policies and procedures will not be followed.

3.2.2 Advantages of written guidelines

108. Written policies, procedures and guidance are fundamental in ensuring that staff are aware of data security risks and the procedures to tackle those risks. Firms with no written policies, procedures or guidance are unlikely to be training their staff properly and ensuring proper awareness of data security risk throughout their business. The importance of written policies and procedures is covered in greater detail in Section 3.1.1.

3.2.3 Effective training and awareness mechanisms

109. Even where firms have detailed written policies, they often fail to train staff effectively. We have dealt with several cases of data loss that have demonstrated it is not realistic to expect staff to read and act on policies simply because they are available on the firm's intranet or in an employee handbook.



A major insurance company relied on staff to read, understand and comply with a lengthy information security policy but took no steps to test staff's understanding of the policy.

110. We found that firms usually gave new recruits copies of lengthy data security policies and procedures, and sometimes asked them to sign to confirm they had read and understood them. In addition, some firms circulate policies and procedures regularly and ask staff to sign a declaration that they have read them. Firms must recognise there is a significant risk that staff will sign declarations without having read or understood policy documents, perhaps because they are too busy or, frankly, because they may find reading a data security policy boring.

A senior manager at a major bank told us he did not expect staff or even branch managers to read the firm's data security policy. Instead, he said staff were guided into compliance with that policy through training, awareness campaigns and detailed procedural guidelines. 'The control process allows people to meet that process without having to understand the policy', he said.

111. Despite the risks of staff failing to understand policies and procedures, we found it was rare for firms – including some large ones – to provide staff with specific courses or coaching on the importance of data security, even on a risk-based approach. A small number of firms recognised this risk and, in some cases, offered incentives to increase staff interest in understanding policies.

A data security quiz offering an iPod as the prize was the most popular staff competition ever at a large bank. The firm intends to repeat this successful initiative every six months.

A major bank offered a flat-panel television as a prize in a data security competition designed to raise awareness of policies. There were over 20,000 entries from its staff.

112. When small firms provide staff training, it tends to be informal; this can be effective and proportionate for the type of business and risk the firm runs.

A small financial advice firm's IT manager, who had a good understanding of data security, regularly reminded staff of good practice, checked the strength of staff passwords, and taught staff about the risk of customer data being used to commit fraud.

113. Although it is good practice for firms to assess staff understanding of data security policies and procedures regularly, we found it was rare for firms to require staff to repeat training or testing. In addition, training for front-line staff, such as those who work in call centres, tended to focus mainly on legislative and regulatory requirements. This



approach does not teach staff about why data security is an essential tool in reducing the risk of financial crime. However, some firms did have some innovative (and inexpensive) training methods for demonstrating how customer data can be used to commit fraud.

A medium-sized building society asked staff to identify items in a mocked-up handbag which could be used for identity fraud. The bag contained items such as credit cards, a driving licence and a utility bill. Once staff had picked out items that could be used by fraudsters, management reminded staff that the firm held similar customer data and emphasised the importance of keeping it secure.

114. Firms that are serious about ensuring good data security will try to raise awareness of relevant policies and procedures by bringing the subject to life and making it clear to employees what they need to do to protect customer data in their everyday work.

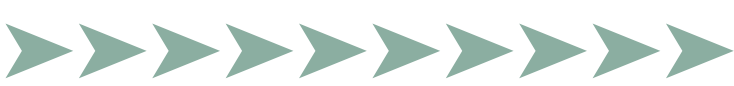
In June 2007, we dealt with a case where a medium-sized investment administration firm had suffered from a spate of identity frauds. One way the firm reduced further fraud was to play recordings to call centre staff of suspected fraudsters' calls. Staff learned to recognise the fraudsters' voices and were able to alert their managers to further suspected frauds.

115. Some firms used posters, messages on screensavers, email reminders, or articles in staff newspapers to promote awareness of data security. Others took more imaginative approaches.

A medium-sized investment firm set up a 'dodgy desk' that exposed all kinds of poor practice relevant to data security. For example, confidential information was left on-screen and confidential papers were left in open view. Staff were then asked to identify all the shortcomings.

Another firm tested its employees' awareness of data security risk by targeting them with spoof 'phishing' attacks requesting username and password details.

116. We found the best good-practice guidance for staff was packaged in a simple, memorable format and was supplemented by controls to ensure that policies and procedures could not be ignored. We also observed that good awareness campaigns usually translated into good practice. For example, desks were clear, passwords were carefully guarded, and staff were generally careful in handling customer data. Simple but effective awareness campaigns can be achieved even in the largest firms. A major bank, for example, reduced its relevant policies to a few simple messages: keeping a clear desk, locking a PC when not in use, using the confidential waste bins and keeping passwords safe. In conjunction with the firm's strong controls, these messages helped to ensure a secure environment for customer data.



A small firm produced a simple one-page list of 'Do's and Don'ts' for its employees that set out good data security practice.

Training and awareness – examples of good practice

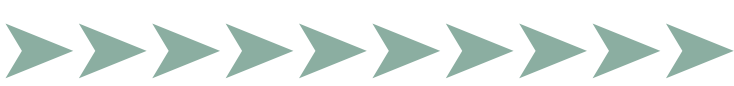
- Innovative training and awareness campaigns that focus on the financial crime risks arising from poor data security, as well as the legal and regulatory requirements to protect customer data.
- Clear understanding among staff about why data security is relevant to their work and what they must do to comply with relevant policies and procedures.
- Simple, memorable and easily-digestible guidance for staff on good data security practice.
- Testing of staff understanding of data security policies on induction and annually thereafter.
- Competitions, posters, screensavers and group discussion to raise interest in the subject.

Training and awareness – examples of poor practice

- No training to communicate policies and procedures.
- Managers assuming that employees understand data security risk without any training.
- Data security policies which are very lengthy, complicated and difficult to read.
- Relying on staff signing an annual declaration saying they have read policy documents without any further testing.
- Staff being given no incentive to learn about data security.

3.3 Staff recruitment and vetting

117. One of the most important controls that firms can put in place to prevent data theft and other financial crime is a good standard of staff vetting. There have been many well-documented cases of staff either stealing customer data to use fraudulently or sell on to criminals who specialise in identity fraud. Other staff have been threatened, bribed or otherwise coerced by criminals into handing over customer data. So firms must be able to trust that their staff will handle and use customer data securely, in line with relevant policies and procedures.



118. We examined firms' general recruitment and vetting policies and considered in particular whether vetting was appropriate for staff in roles that required access to large amounts of customer data, such as call centre, branch and IT staff.

'We know of organised crime groups who are placing people within the call centres so that they can steal customers' data and carry out fraud and money laundering.'

DCI Derek Robertson, Strathclyde Police

Source: BBC News online, October 2006

119. In addition, we examined whether firms conducted any ongoing vetting or monitoring of changes in employees' personal circumstances which could be an early indicator of susceptibility to financial crime. We also investigated whether recruitment standards for temporary and contract staff were equivalent to those applied to permanent staff, especially in higher-risk areas such as call centres.

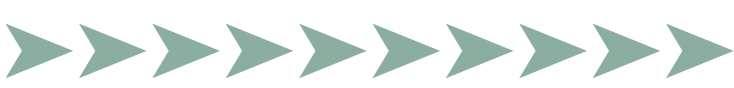
3.3.1 Initial Recruitment Process

120. Many of the 39 firms we visited adopted a two-tier approach to recruitment. Higher vetting standards were generally applied to senior staff and those in 'controlled functions' – positions which require FSA approval of the relevant individual. For these roles, many firms carried out credit checks and, sometimes, criminal record checks. However, most firms did not conduct such a high level of vetting for junior staff (e.g. in call centres, administration and IT roles), despite the fact that they often had wider access to customer data than their senior colleagues.

A small investment management firm's checks for non-FSA-approved staff were limited to references, right to work in the UK, and confirmation of academic qualifications. Only FSA-approved staff were subject to credit checks and no criminal record checks were carried out on any staff.

Conversely, a major insurance firm applied consistent vetting to all staff regardless of rank. This included credit checks and criminal record checks.

121. Many firms had simply not considered that access to large amounts of customer data could make junior staff a higher risk in terms of data loss and financial crime. We were disappointed by this as it indicated that, in terms of their vetting standards, many firms were not adopting an appropriate risk-based approach to preventing financial crime, as required by our Handbook.



A medium-sized insurance firm, that had high staff turnover in its call centre, employed staff solely on employment references. No credit or criminal records checks were carried out for reasons of cost. Furthermore, staff integrity was not routinely examined during the recruitment process.

122. However, we did identify a small number of firms who were applying a risk-based approach to staff recruitment and whose vetting standards were high.

A large bank's financial crime team assisted its HR department to perform rigorous vetting of job applicants. Checks of address; employment references; academic certificates; credit records; financial sanctions lists; fraud intelligence databases; and criminal records databases were carried out for staff in 'higher risk' positions.

The same firm also carried out an annual 'fit and proper' check for staff that included credit checks and financial sanctions list checks to identify changes in staff's personal circumstances which could increase data security or fraud risk.

123. Many small firms did not have a dedicated human resource function (this was mainly due to the low turnover in small firms generally) and recruitment would often be based on personal recommendation and references. Pre-employment checks such as credit references or criminal record checks were rarely carried out.

A small financial advice firm employed all advisers as graduates and all administration staff based on personal recommendation. So the firm had no formal recruitment policies or procedures. Strong reliance was placed on the trust built up with staff over time.

Another small financial advice firm's entire staff was made up of personal friends or recruits through personal recommendation to the manager.

124. Despite the low levels of staff turnover in many small firms, it is good practice for their senior management to consider the risk of customer data being stolen by staff employed on the basis of limited or no vetting. Several of the small firms we visited said we had raised their awareness of data security (and fraud) risks that could arise if a dishonest person was employed by the firm. In addition, many of them wished to be able to reassure their customers that their data was being handled by suitably-vetted staff.

125. Medium-sized and large firms tended to have higher rates of staff turnover than small firms. This was particularly true of firms with large call centres that sometimes had a relatively high number of temporary staff. We observed that high turnover in some firms often leads to conflicting priorities between different departments. For example, security and financial crime staff would wish to ensure that appropriate vetting was carried out on new recruits while line management were under pressure to fill vacancies quickly to maintain a good level of customer service. This was particularly evident in firms with call centre operations or large administration functions.

In a medium-sized insurance firm with high turnover, pressure to fill vacancies meant that call centre staff often had access to customer data for around two weeks before vetting was completed.

126. It is good practice for firms to manage work pressures without compromising the quality of their vetting. Some firms had in place measures to try and reduce pressures arising from high staff turnover. For example, several firms were training their staff in a number of disciplines (sometimes known as ‘multi-skilling’) to provide adequate cover if staff left suddenly. In addition, some firms were putting in place clear career development plans for call centre staff to increase staff morale and loyalty, and reduce turnover.

The importance of liaison between HR and Financial Crime in the vetting process

127. Some of the best practice we noted occurred in firms where there was close liaison between human resources and financial crime/anti-fraud departments. For example, a major bank assessed applicants against a ‘traffic light’ system of financial crime risk indicators, drawn up by HR and the firm’s financial crime team. The table below gives examples of how this system worked.

Examples of ‘red’ criteria	Examples of ‘amber’ criteria	Examples of ‘green’ criteria
Five or more declared County Court Judgments (CCJs)	Fewer than five CCJs declared in excess of £100	A single declared CCJ for £100 or less
Two or more undeclared CCJs	A declared dismissal from previous employment	Adverse information received from previous employer not relating to a dismissal
Adverse employment references in connection with financial crime or serious misconduct	A declared criminal record	Criminal records for motoring offences
Non-discharged bankruptcy or Individual Voluntary Arrangements (IVAs)		

Note: This table is an example of what we saw at one firm; it is not exhaustive and firms should consider all risk factors relevant to their business if they choose to adopt a similar approach.

128. Any applicant meeting an element of red criteria would not be hired while an applicant meeting an amber criterion could only be recruited following an independent review and sign off by HR. In addition, the firm was trialling CIFAS staff fraud database¹² and

12 The CIFAS Staff Fraud Database is used by CIFAS Members specifically for staff vetting and security screening purposes. CIFAS members use the Staff Fraud Database to file data about their staff fraud cases and access staff fraud records filed by other CIFAS Members. For more information, visit: www.cifas.org.uk/default.asp?edit_id=718-87



criminal record checks on all staff meeting amber criteria (around a fifth of all applicants) regardless of role. The firm advised all new applicants of the possibility of criminal record checks, hoping that this would act as a deterrent to applicants with relevant criminal convictions. Importantly, the firm's financial crime team reviewed the traffic light indicators regularly and added new or emerging risk criteria to the system based on their own, and industry-wide, experience.

3.3.2 Temporary staff

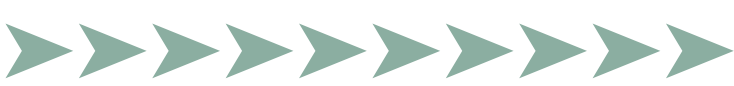
129. For many firms, employment agencies are a key third-party supplier with relevance to data security. Although employment agencies are unlikely to handle customer data, they often play a key role in recruiting temporary staff with access to firms' customer data. So it is essential that firms have a clear understanding of the checks conducted by agencies on prospective staff and that regular checks are made to ensure agencies are complying with agreed vetting standards.
130. It is good practice for firms to ensure that temporary staff are not subject to less-rigorous vetting than permanent staff in similar roles. This is consistent with a risk-based approach to reducing financial crime because the risk to customer data does not decrease when a temporary member of staff handles it.

A medium-sized investment firm did not tell their employment agencies the standard of vetting required for temporary staff. The firm's HR representative was unable to tell us what vetting was conducted by the agencies for temporary staff as he had never asked the agencies about their vetting standards.

131. The 20 small firms we visited very rarely employed temporary or contract staff because of their low levels of staff turnover. In contrast, the employment of temporary or contract staff was common in medium-sized and large firms, particularly in call centres or administrative roles. Many larger firms had contracts with 'preferred' employment agencies and used them to source temporary and contract staff. In general, larger firms relied on agencies to carry out relevant pre-employment checks on temporary and contract staff. However, a small number of firms chose not to rely on checks carried out by employment agencies and conducted their own vetting checks on staff put forward to them.

Some firms arranged for agencies to put in place a pre-vetted panel of temporary staff to enable higher-risk vacancies to be filled quickly by suitable individuals.

132. Our findings on controls over third parties that handle customer data are detailed in Section 3.7.



3.3.3 Ongoing vetting of staff

133. Although most firms recognise the risk of data theft by their employees, many firms had no formal process for identifying a change in an employee's personal circumstances. Bankruptcy, divorce and addictions to gambling, drugs or alcohol are all examples of lifestyle events that could affect an individual's financial soundness and make them more vulnerable to committing data theft and fraud.
134. Overall, we saw very few examples of formalised, repeated vetting of staff, even when individuals had access to large amounts of customer data. The exception was FSA-approved individuals, who were often subject to annual credit checks so that firms could satisfy themselves of the individual's continuing fitness and propriety.

A large insurance firm that carried out credit checks on new recruits repeated them once a year as part of an individual's performance appraisal process.

135. The generally poor standard of vetting for new recruits, coupled with the relative rarity of ongoing vetting, gives rise to significant risk of data theft from financial services firms. For both initial and ongoing vetting, firms should take a risk-based approach and ensure that staff access to customer data is one of the factors considered.
136. Small firms often relied on the close-knit nature of their organisations, where staff were well-known to each other and often long-serving, and staff vigilance to identify unusual behaviour among their workforce. Their employees often sat in close proximity and were generally aware of what their colleagues' roles entailed. This may be a proportionate, risk-based approach in some small firms, but it is good practice for them to support it with a formal data security risk assessment covering the risk of corrupt staff.
137. In larger firms, there were usually clearly-defined management structures and line managers were generally responsible for continually assessing staff performance. Many large firms relied on the general performance management process as the main tool for identifying changes in employees' circumstances that could give rise to increased data security risk. We are not convinced this informal approach to ongoing vetting will always be appropriate, particularly for higher-risk roles. A more-structured approach incorporating tools such as regular credit or criminal record checks on a risk basis is likely to be far more effective in reducing data security risk in financial services firms.

Staff recruitment and vetting – examples of good practice

- A risk-based approach to vetting staff, taking into account data security and other fraud risk.



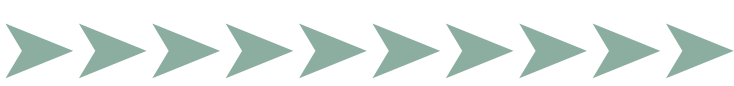
- Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists and the CIFAS Staff Fraud Database – for staff in roles with access to large amounts of customer data.
- Liaison between HR and Financial Crime to ensure that financial crime risk indicators are considered during the vetting process.
- A good understanding of the level of vetting conducted by employment agencies during the recruitment of temporary and contract staff.
- Formal procedures to assess regularly whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.

Staff recruitment and vetting – examples of poor practice

- Allowing new recruits to access customer data before vetting has been completed.
- Temporary staff receiving less-rigorous vetting than permanently employed colleagues carrying out similar roles.
- Failing to consider whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.

3.4 Controls

138. Earlier in this report, we set out our findings on how policies and procedures are implemented and staff are trained about their responsibilities. While these factors are important in setting the tone for how a firm manages data security risk, it is essential that firms also have in place effective controls to prevent data loss if policies and procedures are not followed.
139. Without effective controls, data can be lost or stolen, even where policies, procedures and training are of a good standard. Examples of how this might happen include staff ignoring procedures because of a time constraint, other work pressure or perhaps being unaware of their responsibilities; perhaps they were sick when they were supposed to have been trained or they simply might not have been listening during a training session.
140. There is also the very real possibility of data theft by corrupt employees. This can occur when criminals or their associates infiltrate a firm or when existing staff are coerced by criminals – perhaps with the offer of a bribe, the threat of personal injury or blackmail – to give them customer data.



Examples of incidents of data theft brought to our attention during our review included:

- a call centre employee in a major insurance firm who used a customer's credit card details to buy goods online; and
- a call centre employee in a major bank who stole customer data for her boyfriend 'to prove her love'. This led to fraud on at least three customers' bank accounts before the theft was discovered.

141. During our visits, we examined in-depth the controls firms have in place to prevent data loss. Of the 39 firms we visited, we judged that only eight had good controls in place to minimise the risk of data loss. All of these firms were large or medium-sized firms in the banking and insurance industries. Interestingly, two of them offered identity theft insurance; one specifically stated that the potential reputational damage of a data loss to their identity theft insurance business was a key driver to ensure the best possible data security control environment.
142. The remaining 31 firms were split roughly into two groups. The first group (16 firms) had implemented a range of controls across their business but weaknesses in some areas gave rise to a significant risk of data loss. Worryingly, this group of firms included some very large firms that held, in some cases, millions of customers' details. The second group (15 firms) – the majority of which were small – had a poor control environment which gave rise to a high risk of data loss. This was often the result of a lack of awareness of data security risk at senior management level, but may also be attributable to a lack of financial or human resources.

From our sample of 39 firms, just eight had good controls.

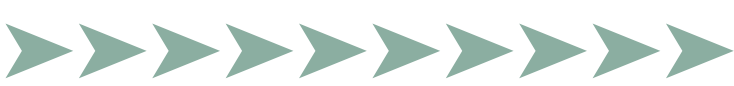
Sixteen firms had some good controls in place but had significant weaknesses too.

Fifteen firms had poor controls which gave rise to a high risk of data compromise.

3.4.1 Controls in offshore operations

143. A small number of the firms we visited had call centres both in the UK and in India. All of these firms believed the control environment in its India call centres, including physical security and recruitment, was at least equivalent to that of their UK call centres. These views are consistent with our previous work on offshore operations, published in 2005.¹³
144. One large firm told us its India call centre was subject to significantly higher physical security than the UK, including a 'paperless office'. This firm recognised the risk of data loss from its UK call centres but did not feel it could apply the rigorous security

13 www.fsa.gov.uk/pubs/other/offshore_ops.pdf



arrangements in place in India. There were several reasons for this, including the potential detrimental effect on staff morale and possible trade union concerns.

3.4.2 Access rights

145. Properly-configured IT access rights and a well-defined joiners and leavers process are essential tools in ensuring data is appropriately secured. There are three main points at which it is good practice for firms to take appropriate steps to ensure that access rights are reviewed: on recruitment; when staff change roles; and when they leave the firm.

On recruitment

146. It is good practice for firms to ensure that, when recruited, staff are only given access to the information they require to do their job. This is often referred to as ‘least privilege’ access.
147. During our review, we found many examples of insufficient procedures to ensure least-privilege access. The most extreme examples included some firms that gave all staff access to all of their customer data, regardless of whether they needed the information to do their jobs. More often, access rights were determined on a case-by-case basis by line managers with no independent checking they were appropriate. There is a risk that, without an independent check, this could lead to some staff having inappropriate access to customer data.

A medium-sized insurance firm had two main IT systems – a customer database and a workflow monitoring system. They contained a wide range of sensitive customer data, including financial and bank account details, scanned copies of customer signatures and detailed personal information required for life insurance applications. With the exception of medical information, access to this personal data was not restricted according to business need.

148. Some of the good practice we saw included detailed role profiles for each job – or type of job – that included a description of the access rights required to carry out the role, on a least-privilege basis. We observed this good practice in several firms of various sizes.

Several investment firms restricted IT access so advisers could only access information about their own clients, not all clients of the firm. However, there were other firms that allowed unrestricted access to all customer data for all staff, regardless of business need.



When a staff member changes jobs or is given new responsibilities

149. It is essential that firms have processes in place to ensure they review access rights when an individual changes roles or is given different responsibilities. Without such processes, staff can build up inappropriate access to large numbers of systems over time. This not only gives rise to data security risks, but also to more general fraud risks, as staff might be able to access information that has been segregated to prevent fraud.
150. Most firms had taken some steps to review the appropriateness of staff access rights in the event of a role change. Good practice we observed included:
- i. firms that had set up role-based access profiles for each role in their organisation that simply replaced the old role profile with the new one when an individual changed roles; and
 - ii. firms that effectively treated staff changing roles as new joiners. All existing access rights would be deleted and the user would have their new access rights set up from scratch by the IT department.
151. However, we found some examples of firms of various sizes – including one major firm – that did not have effective controls to prevent staff building up inappropriate access to systems containing customer data.

When staff leave the firm

152. When a member of staff leaves employment, it is good practice for firms to ensure their IT access rights are permanently disabled or deleted. If this is not done, there is a risk of a corrupt member of staff using the vacant user account for criminal purposes, including the theft of customer data.
153. Some firms had appropriate controls to ensure that leavers' IT access rights were disabled. In many firms, this included the regular reconciliation of HR records against the IT department's log of user accounts. This would help to identify staff who had left the firm, but who, for some reason, had not had their user account disabled or deleted.
154. We did, however, find some poor practice in this area, with some firms failing to put in place effective controls to ensure that redundant user accounts were disabled on a timely and accurate basis.

We spotted an example of very poor practice at a medium-sized insurance firm, which did not permanently disable redundant user accounts. Instead, their process was for IT support staff to change the user's password to a random string of letters and numbers 'which could not be guessed by anybody else'. The firm failed to recognise the risk that a corrupt member of IT support staff could note the new password and continue to use the user account to steal customer data and/or commit financial crime.



155. Three particular issues relating to access rights emerged during our review. In some cases, firms had failed to recognise the risk of data loss and weak access controls exposed the firm to a high level of data security risk.

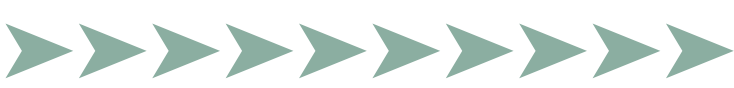
Wide access to scanned copies of sensitive documents collected for ‘know your customer’ purposes

156. We noted during our visits a general shift in the financial services industry – including in small firms – from holding customer data in paper files to the electronic scanning and filing of correspondence. There are clear benefits in terms of efficiency and customer service for businesses that scan documents. However, we visited a significant number of firms and call centres where scanned correspondence containing customer data that could be used to commit fraud was accessible to too many staff without a genuine business need. The types of scanned correspondence typically included documents collected by firms to verify customers for anti-money laundering (AML) purposes, such as passports, driving licences, utility bills and bank/credit card statements.

Several firms we visited – large and small – scanned ‘know your customer’ information on to their IT systems. In nearly all cases, access to this information was too wide. Sometimes, entire call centres could access scanned copies of documents like customers’ passports, driving licences and bank statements. And in some cases, scans could be printed off, downloaded to USB devices or emailed externally.

157. It is good practice for firms to consider carefully the types of scanned documents that staff need to access to do their jobs when determining access rights. The findings of our review indicate it is rare for staff outside of firms’ financial crime departments to need to see scanned copies of ‘know your customer’ information to do their job. Some staff in call centres told us they needed access to these documents to ensure that AML checks had been completed. However, when challenged, they conceded that a marker on the customer’s record stating whether AML checks for the customer had been completed would enable them to do their job.

A medium-sized insurance firm required customers to submit their credit card numbers and expiry details on their claim forms so that payments for the insurance excess could be taken. However, some customers (although not required to) also supplied their three digit security code. Copies of these claim forms – which included all of the information required to commit credit card fraud – were scanned onto the system and accessible to all call centre staff.



Wide access to recordings of telephone conversations containing sensitive data

158. It is common industry practice for telephone conversations with customers to be recorded either for training purposes or in case of a dispute with the customer. However, it appears that access to call recordings is not always on a least-privilege basis, even when access to other IT systems is.

One major firm – with several call centres in the UK and one in India – gave call centre team leaders and managers unrestricted access to recordings of every single call received by its many call centres. Many of these conversations included customers’ names, addresses, dates of birth, policy details, and credit card/bank account details. The firm believed this was necessary for training purposes but we contended that training on good customer service could still be provided if access to call recordings was significantly restricted. Interestingly, the team leaders we spoke to did not believe that their access to these call recordings was ever monitored.

159. Call recordings often contain sensitive customer data such as passwords and financial information. As with other IT systems, it is good practice for firms to ensure that staff only have access to recordings needed for their particular role.

A major bank authenticated its customers’ identities via touch-tone telephone before customers were put through to call centre staff. This meant that call centre staff did not need to ask customers for sensitive data to confirm their identity, so this information was not recorded.

Full credit card numbers and bank account details available to large numbers of employees with no business need

160. We found that some firms – including large firms – made sensitive financial data such as credit card numbers and expiry dates, bank account details and sort codes available to a wide range of staff and sometimes entire call centres. Many call centre staff told us it would not affect their ability to do their job if the sensitive financial details were partially obscured on their systems.

Some firms’ databases only displayed partial credit card or bank account details to minimise the risk of data loss. For example, one firm displayed 16-digit credit card numbers in the following format: 1234 XXXX XXXX 5678. Another firm was halfway through a project to obscure such details on their databases.



Access rights – examples of good 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.
- When 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.
- A clearly-defined process to notify IT of forthcoming staff departures so IT accesses can be permanently disabled or deleted on a timely and accurate basis.
- A regular reconciliation of HR and IT user records to act as a failsafe if the firm's leavers process fails.
- Regular reviews of staff IT access rights to ensure there are no anomalies.
- Least-privilege access to call recordings and copies of scanned documents obtained for 'know your customer' purposes.
- 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 staff's ability to do their job.

Access rights – Examples of poor practice

- Staff having access to customer data which they do not require to do their job.
- User access rights set up on a case-by-case basis with no independent check that they are appropriate.
- Redundant access rights being allowed to remain in force when a member of staff changes roles.
- User accounts being left 'live' or only suspended (i.e. not permanently disabled) when a staff member leaves.
- A lack of independent check of changes effected at any stage in the joiners, movers and leavers process.



3.4.3 Passwords and user accounts

161. It is important that firms ensure access to IT systems, both through desktops and laptops, is controlled using individual user accounts (often referred to as ‘user ID’) and each user account is protected by a strong password. There is a risk that passwords can be easily guessed and studies have shown people often use the names of relatives, pets, their favourite football team and sometimes even the word ‘password’ to access their systems. In addition, password cracking software is now widely available.

A senior manager of a small financial advice firm named Gill told us that her user ID was ‘Gill’ and her password was ‘Gill’ (name changed to protect identity).

162. During our review, we discovered many firms had poor password standards in place. This was mainly a problem in small firms but we also found examples of poor practice in some larger firms. In particular, several firms had policies in place recommending certain standards but had no controls in place to ensure these standards were met.

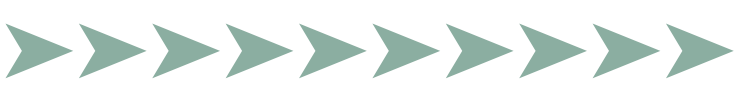
A major bank allowed passwords that were only six characters long and did not need to contain a mix of upper and lower case letters, numbers or keyboard symbols. This is significantly below recommended standards on password strength. Get Safe Online – a government-backed campaign group – recommends that passwords should be a combination of letters, numbers and keyboard symbols; at least seven characters long; contain a mix of upper and lower case letters, numbers and keyboard symbols; and be changed regularly.¹⁴

163. It is essential that firms have individual user accounts in place so they can monitor users’ activities to detect breaches of policies and procedures that could lead to data loss. However, we found some firms did not have individual user accounts in place and allowed all users to access their systems with the same password. This exposes firms to a significant risk of systems misuse, including data loss. For example, if a corrupt employee was systematically extracting customer data from a database using a generic password, the lack of an auditable, individual user account would make it difficult for the firm to find out – or prove – who was responsible.

Password sharing

164. In several small firms, we found examples of individual users’ passwords being shared with or known to senior management and other employees; this could lead to user accounts being compromised. For example, one small firm told us senior management knew every staff member’s password. The justification given was that some staff had particular software installed on their computers which senior management might need

¹⁴ http://www.getsafeonline.org/nqcontent.cfm?a_id=1127



to use from time to time. Password sharing is poor practice and had arisen in this case because the firm had not ensured that each user had access to the systems and software they needed to do their jobs.

Multiple passwords

165. We noted during our visits that most firms had more than one system requiring a password. The proliferation of passwords required by individuals – both at work and in their everyday life – could have undesired results in terms of security. For example, a member of staff might use the same password for several systems or they might write down their passwords so they do not forget them.

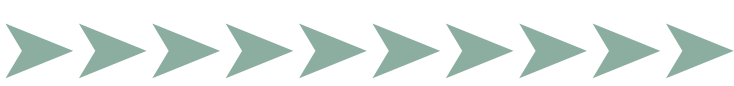
Two medium-sized firms – an insurer and a building society – had used password-cracking software on their staff's user accounts to check that passwords were robust enough. The building society did this regularly and, if a password could be cracked within an hour, they made staff change their password.

166. To reduce these risks, some larger firms said they were investigating moving to 'straight-through processing'. Straight-through processing allows users to log on to their computer with a single password and access all required databases or other software without the need for any more passwords. It is good practice for firms seeking to move to straight-through processing to have accurate, role-based access profiles in place (see paragraph 148) so staff only have access to the systems and data that they need to do their job. In addition, as only one password is required for straight-through processing, it is good practice for firms to ensure that each employee's password is strong.

A major insurance firm was investigating 'straight-through processing' – a method that gives a user appropriate access to all databases and software with a single password. They acknowledged they would first need to ensure that accurate role-based access profiles were in place for all staff to reduce the risk of inappropriate access to some systems.

Passwords and user accounts – examples of good practice

- Individual user accounts – requiring passwords – in place for all systems containing customer data.
- Password standards at least equivalent to those recommended by campaign group Get Safe Online. At present, their recommended standard for passwords is a combination of letters, numbers and keyboard symbols at least seven characters in length and changed regularly.



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

Passwords and user accounts – examples of poor practice

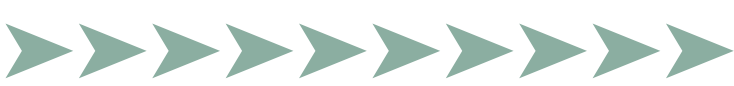
- The same user account and password used by multiple users to access particular systems.
- Names and dictionary words used as passwords.
- Systems which allow passwords to be set which do not comply with password policy.
- Password sharing of any kind.

3.4.4 Monitoring access to customer data

167. Even staff who have a legitimate need to access customer data can present risks. The most pertinent examples include corrupt staff who wish to use customer data to commit fraud themselves, staff who have been coerced by criminals to give them customer data and staff with links to criminal groups who have managed to get a job in a financial services firm.
168. For these reasons, it is good practice for firms to take a risk-based approach to monitoring employees’ access to customer data to ensure that access is for genuine business reasons. An example of a simple check is to take a sample of when staff have accessed customer records in call centres and compare it with records of telephone calls the call centre has received from customers. This could highlight instances where customer data has potentially been accessed without a valid business reason and the firm can ask the relevant employee for an explanation. In addition, where databases record the time and date of changes made to customer records, these can also be cross-referenced to recordings of particular phone calls to ensure the changes made were actually requested by the customer.

A medium-sized building society had software in place to track access, changes and other manipulation of data through exception reports, which the firm reviewed monthly. Importantly, the firm had invested significant time and resource to fine-tune the software from its ‘off-the-shelf’ format, so it would recognise genuine suspicious activity and reduce the number of false exceptions.

169. Few firms carried out proactive monitoring of their staff’s access to data, even on a sample- or risk-based approach.



A medium-sized investment firm had a database with an audit facility that could identify when customer data had been changed, who had changed it, and show the data before and after the change had been made. However, the firm failed to make routine use of the audit facility to ensure either that there were genuine business reasons for changes to customer data.

Superusers

170. ‘Superusers’ most often work in IT and are often responsible for database administration and creating staff access rights. Their technical knowledge means they often have the potential to access large amounts of customer data and sometimes to circumvent fraud controls. These factors are likely to make superusers attractive targets for organised criminals seeking to use an insider to steal customer data from a firm. So it is good practice for superusers to be carefully vetted and monitored.

Most large and medium-sized firms had some measures in place to prevent staff from accessing bulk customer data. Many call centres, for example, only allowed staff to access one customer record at a time. However, it was not unusual for some staff – particularly in ‘superuser’ or other IT positions – to be able to extract bulk data.

A major bank was unclear about the number of database administrators it employed and admitted these superusers had the capability to disable the audit trails used to monitor their activity.

171. We saw varied practice in larger firms in this area. Some had excellent controls including strict processes to prevent unauthorised changes to systems and data by database administrators. In other firms, superusers were not adequately controlled.

A large bank had recently completed a project to put superuser passwords into a ‘digital vault’. Superusers were required to complete a form stating the work they would carry out and get approval from independent staff before being able to ‘unlock’ the digital vault and access relevant systems with a single-use password. The superuser was then required to check the password back in to the digital vault within a given timeframe. At that point, the password would be automatically changed for its next use.

172. The monitoring of superusers poses real problems for small firms, as there is often a lack of technical knowledge, resource and understanding of the superuser’s roles elsewhere in the firm. As a result, there is usually no independent check of superusers’ work and trust is the main tool used to ensure a secure environment. Where this is the case, it is good practice for small firms to ensure the standard of vetting (see Section 3.3) is proportionate to the high risk posed by superusers’ wide-ranging access to customer data. In addition, these firms may wish to ask their IT auditors or compliance consultants to conduct a regular review of superusers’ activities.



A small investment firm did not conduct any independent check of the IT Director's work, even though he had completely unrestricted access to all IT systems in the firm. This risk was compounded as the firm did not check whether any of its staff, even in high-risk positions, had any criminal convictions. Situations like this were quite common in the sample of small firms we examined.

Monitoring access to customer data – examples of good practice

- Risk-based, proactive monitoring of staff's access to customer data to ensure that it is being accessed and/or updated for a genuine business reason.
- Using 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 it is tailored to their business profile.
- 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.

Monitoring access to customer data – examples of poor practice

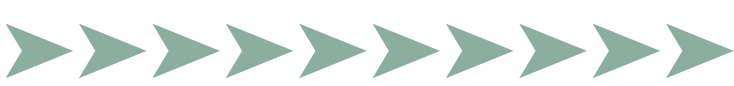
- Assuming that vetted staff with appropriate access rights will always act appropriately. Staff can breach procedures, for example by looking at account information relating to celebrities, be tempted to commit fraud themselves or be bribed or threatened to provide customer data to criminals.
- Failure to make regular use of management information about access to customer data.
- Failing to monitor superusers or other employees with access to large amounts of customer data.

3.4.5 Authentication

173. In August 2007, we published a special edition of our Financial Crime Newsletter which focused on the authentication and safeguarding of customer identity¹⁵ (our 'Authentication Newsletter'). In it, we called on firms to take the following key steps to ensure customers' identities are effectively verified and protected:

- establish a suitable and effective authentication process;
- protect customer data, so it cannot be stolen and/or used to defraud consumers and firms; and
- help customers be more security conscious.

15 www.fsa.gov.uk/pubs/newsletters/fc_newsletter8.pdf



174. The Authentication Newsletter contained good-practice guidance to help firms establish appropriate risk management systems. As this work was carried out recently, we did not focus on authentication during our review but, inevitably, the subject did arise from time to time. Our findings suggest there is still much for some firms to do if customers' identities are to be authenticated effectively.
175. Some of the medium-sized firms we visited asked customers to authenticate themselves by confirming details which were publicly available. For example, one firm's call-centre operators asked customers to confirm three random pieces of information about themselves to complete the authentication process. However, the firm had not considered the risk that call centre staff might ask for three pieces of publicly available information, such as name, address, and date of birth, creating significant opportunities for fraudsters to access customer accounts and/or data. Another firm had at least recognised the risk posed by the use of publicly-available data in the authentication process and was moving to a password-based system.

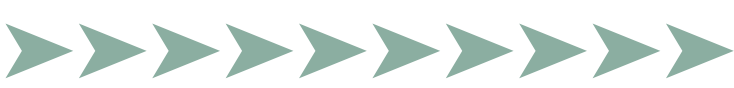
One firm, which used a four-digit customer reference number as a tool for customer authentication, routinely included the reference number in mailings to customers. This mail could be intercepted by criminals seeking to gain access to customers' accounts and financial information.

176. It is good practice for firms using password-based systems to put in place measures to protect passwords and we observed that some larger firms had done so.

Two banks had systems in place where call centre staff did not have access to entire customer passwords. Both firms asked customers to give two random letters from their passwords. Call centre staff then entered these random letters into the system to access account details.

177. In the worst cases we saw, two small investment firms had not considered any process at all for authenticating their customers. Instead, these firms told us they relied solely on advisers recognising their clients' voices. This could present significant opportunities for an identity fraudster to access or take over a customer account using impersonation.

Two small investment firms had not established a suitable and effective authentication process for customers who telephoned the office to request or change information on their accounts. Instead, they relied solely on their advisers recognising their clients' voices. One of these firms had an adviser to client ratio of around 1:1,200; the other around 1:150. It is not possible for advisers to recognise the voices of such large numbers of clients, some of whom may contact the firm infrequently. Poor controls like this can lead to significant fraud.



178. Interestingly, our Authentication Newsletter found that no firms routinely proved their own identity before asking the customer to authenticate themselves. During our review, we visited a medium-sized insurance firm whose products included mobile-phone insurance. The firm specifically instructed its call centre staff not to ask for customers' personal information until they had supplied the customer with basic information about their mobile phone and/or the call plan. While we were encouraged that the firm had thought about how they could prove their identity to customers before authenticating their identities, firms should take care they do not disclose customer data to somebody other than the customer. This would be a breach of the Data Protection Act and could expose customers to identity fraud.
179. As noted previously, our Authentication Newsletter contained good practice guidance for firms and highlighted areas for improvement.

3.4.6 Data back-up

180. Almost all firms with electronic systems back up their data on a regular basis to ensure that they would be able to continue operating after an adverse event such as a fire, flood or corruption of data held on IT systems. As part of this process, firms often take copies of all their data and store it offsite at one of their other offices, with a third-party supplier or at the home of a trusted employee.
181. Although the backing up of data is essential for disaster recovery purposes, the methods commonly used by firms give rise to several risks to data security that must be properly managed.

The sheer volume and detail of customer data held on back-up tapes and servers makes them very attractive to criminals seeking to commit fraud. Put simply, if backed up data is not transferred or stored securely, all other controls to ensure data security at a firm are undermined.

182. However, we found that many firms simply did not recognise the risks associated with transferring and storing copies of all their data offsite. Others failed to examine all of the risks involved. For example, a firm might put in place good controls over the transfer of data to an archiving firm, but then have no understanding of – or fail to check – how securely the data is held at the archiving firm. Appropriate management of third-party suppliers is examined in depth in Section 3.7.

A medium-sized insurance firm used a third-party supplier to store backed up data. Although the data – which included large amounts of customers' credit card and bank account data – was transferred to the third party using a secure, encrypted internet link, the data was held at the third party in plain text.

The insurance firm admitted it had not conducted any due diligence of the third party's data security arrangements and later found out from the third party that a large number of their staff could potentially gain access to the data. This illustrates the importance of firms understanding how securely their data is held at third parties.



How do firms store their backed up data?

183. We found that major firms and other firms with multiple offices or branch networks either stored backed up data at alternative offices (often on a reciprocal basis) or used third-party storage firms to hold the back-up tapes. Medium-sized firms with single offices mainly used third-party storage firms to ensure timely access to data, while some small firms also used this method. However, many small firms relied on a trusted member of staff to hold tapes overnight.

A building society had a dedicated back-up site with the same tight security arrangements as its head office. Designated staff at the firm personally transferred back up tapes to the storage site every day.

Appropriate encryption of back-up data both in storage and in transit

184. To minimise the risk of data loss, either in transit or at a third-party supplier, many firms ensured their back-up tapes were encrypted. However, we did see some examples of firms – including some quite large firms – that did not encrypt back-up tapes, leaving them vulnerable to compromise if they were lost or stolen either in transit or from the back-up site. It is good practice for firms to review the level of encryption applied to back-up tapes (and indeed other portable media) regularly to ensure it is appropriate.

A medium-sized bank used a third-party storage firm to store its back-up tapes. However, it had not conducted any due diligence of the third party's security arrangements. In addition, the back-up tape was often left with the security guard at the bank's premises for passing on to an employee of the storage company. The security guard was not employed by the bank, nor had he been vetted by them.

Poor practice in small firms

185. Many small firms rely on a trusted member of staff to hold back-up tapes securely off-site. We encountered several instances where there had been very little or no consideration of the risks involved, resulting in a complete lack of formal process or security over backed-up data. The following are examples of poor practice that we observed in small firms.



A partner in a financial advice firm with around 16,000 customers took a weekly back-up tape off-site. He kept the tape in his car so he would not forget to bring it back to the office the following week. There had been no consideration of the risk to customer data if the car was stolen.

The IT Director at a financial advice firm with over 6,000 customers did not know the name of the member of staff with responsibility for holding back-up tapes overnight. Back-up tapes were not encrypted and senior management had no idea about off-site security arrangements. In addition, the IT Director, who deputised as the holder of back-up tapes when the other member of staff was absent, told us that his storage arrangements were insecure.

A credit union had very disorganised data back-up arrangements. The main backup was copied daily to another server held onsite. However, senior management at the firm also took irregular back-ups of the servers and some databases using external hard-drives, memory sticks and laptops, which were then taken off-site. Senior management were unsure about whether any of these portable storage devices were encrypted. We discuss the use of portable devices in greater depth in Section 3.4.10.

186. Despite these worrying examples of poor practice, some small firms had secure back-up arrangements in place, including encrypted tapes and safes installed at the home of the responsible member of staff. These measures are not expensive and are a clear message to other small firms that cheap yet secure arrangements are not impossible to achieve.

Data back-up – Examples of good 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 encrypting backed-up data that is held offsite, including while in transit.
- Regular reviews of the level of encryption to ensure it remains appropriate to the current risk environment.
- Back up data being transferred by secure internet links.
- 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 data held off-site is done so in accordance with accepted policies and procedures.

Data back-up – Examples of poor practice

- Firms failing to consider data security risk arising from the backing up of customer data
- 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.
- Unrestricted access to back-up tapes for large numbers of staff at third party firms.
- Back-up tapes being held insecurely by firm's employees; for example, being left in their cars or at home on the kitchen table.

3.4.7 Access to the internet and email

187. The internet and email give firms the ability to communicate and access information quickly, easily and efficiently. However, they also present significant risks to data security if not properly managed and monitored. Most firms we visited gave internet and external email access to their staff, mainly by default, and many had not considered the risks of data loss or theft through these channels.
188. We would strongly encourage firms to consider whether there is a genuine business need for staff to have access to the internet and email and whether the benefits of giving internet access to staff handling large amounts of customer data outweigh the data security risks. A small minority of the firms we visited – mainly larger ones – had systems in place to restrict email and internet access only to staff with a genuine business need. Management sign-off was required for staff to have internet and email activated.

One major insurance firm gave its many call centre staff access to external email and had a policy which allowed them to send a certain number of external emails every day. However, call centre staff told us they had no business need for external email. Indeed, they were specifically instructed by the firm not to give out their email addresses to customers or to communicate with customers via their personal email accounts.

Monitoring of internet/email use

189. Most firms – particularly large and medium-sized ones – produced management information on how their employees used the internet and email. However, this monitoring very rarely considered the risk of data loss through these channels. Instead, firms were mainly focused on whether staff were using the internet or email excessively or accessing/sending inappropriate content. Some firms had measures in place to block



the sending of large attachments but this usually appeared to be for reasons of system performance, rather than to reduce the risk of data loss.

190. Several firms stated that, as a result of our visit, they would investigate whether the software they used to identify profanities or sexual language in emails could be adapted to search for strings of digits resembling credit card numbers or bank account details.

One large bank had software in place that routinely scanned emails for 16-digit card numbers and PIN numbers. Another had plans in place to introduce sophisticated email monitoring software, specifically designed to prevent data loss.

Web-based communication facilities

191. Although the subject fell outside the scope of our project and we did not examine it in depth, many firms assured us that they had anti-virus and anti-spyware software in place to reduce the risk of hi-tech attacks by criminals.

192. We looked much more closely, however, at whether firms were blocking employee access to websites or other internet content which we judge currently give rise to a high risk of data loss. Examples of such content include:

- web-based email (popular providers include Hotmail, Gmail and Yahoo);
- social networking sites which allow users to exchange messages (eg Facebook);
- instant messaging facilities which allow messages to be sent externally (eg MSN); and
- ‘peer-to-peer’ file sharing software, such as Limewire, BitTorrent and eDonkey, which allow users to share and receive files – usually music and videos – over the internet.

A 2007 study by researchers at the Center for Digital Strategies at Dartmouth College, New Hampshire, examined accidental data loss through peer-to-peer file sharing networks at a group of large financial firms. Sensitive customer data – including account information – was accidentally exposed when users searched for songs containing words which also appeared in firms’ names. In addition, the study found indications that cyber-criminals are using peer-to-peer networks specifically to steal customer data. For example, a significant proportion of search terms appeared to be looking for databases, account information, passwords and PIN numbers.

Many firms we visited were unaware of the data security risks posed by peer-to-peer file sharing. In addition, we spotted an adviser at a medium-sized investment firm with peer-to-peer file sharing software installed on his computer, potentially exposing the firm’s customer data to other internet users.



193. One of the main risks of web-based communication facilities is firms' inability to detect when data is being lost or stolen. For example, if a corrupt member of staff was leaking information through a firm's email system, the firm would have the means – via its IT audit logs – to identify who was leaking the data and what data was lost. The firm could then put in place protective measures on its customers' accounts, alert its customers to the potential wider identity fraud risks and take appropriate action against the individual who leaked the data. However, if the data was leaked, for example, by web-based email, the firm would not be in a position to see what had been sent from the employee's computer and would not be able to establish whether a data loss had occurred at all.

A medium-sized insurance firm allowed staff in its call centre – who had access to large amounts of sensitive customer data – access to web-based email.

194. We found that major firms blocked access to most web-based communication sites. This was usually achieved using software that allowed the firm to block categories of websites which they did not want their staff to access. Medium-sized firms also tended to block such websites but we found two that did not.

In general, small firms had very poor or no controls in place to prevent staff accessing web-based communication sites. Thirteen of the 20 small firms we visited allowed their staff to use web-based email, putting their customer data at unnecessary risk.

Access to the internet and email – Examples of good practice

- Giving internet and email access only to staff with a genuine business need
- Considering the risk of data compromise when monitoring outbound email traffic, for example by looking for strings of numbers that might be credit card details.
- 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 web-based communications are blocked and data cannot be transferred into the cyber-cafe, either in electronic or paper format.



Access to the internet and email – Examples of poor practice

- Allowing staff who handle customer data to have access to the internet and email if there is no business reason for this.
- Allowing access to web-based communication internet sites. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and ‘peer-to-peer’ file sharing software.

3.4.8 Key-logging devices

195. Key-loggers can pose a risk to the security of customer data, as well as other fraud risk. They work by recording each individual keystroke made by a computer user. So passwords to databases containing customer data, as well as encryption keys, can be compromised using key-loggers.
196. Key-loggers come in hardware and software forms. The risk of software key-loggers can be minimised by anti-spyware programmes and firewalls. However, it is more difficult for firms to protect themselves against hardware key-loggers, which can either be attached to a PC or inserted inside hardware such as keyboards and mice. The latter are particularly difficult to detect.

In 2005, an organised crime group tried to defraud a major bank in London. They used key-logging devices to obtain the codes required to make large money transfers overseas. The fraud was detected and foiled but it is thought that the fraudsters, if successful, could have stolen £220m.

197. It is good practice for firms to consider on a risk basis whether it is appropriate to perform sweeps for key-logging devices. In terms of protecting customer data, a firm might consider it worthwhile to conduct regular sweeps in areas where staff handle or have access to large amounts of customer data, for example, IT super-users or call centres.
198. It is also good practice for staff to be made aware of the threat of key-logging devices in case their computers are targeted by criminals. One firm sent detailed guidance to staff about the risk of key-logging which included pictures of key-logging devices and an explanation of how they work. This raised staff awareness of how to report any suspicious devices attached to their computers.
199. Only two of the firms we visited (both medium-sized) told us they conducted sweeps for key-logging devices and, in both of these firms, these sweeps were on an ad-hoc or informal basis.



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.
- Awareness raising 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.

3.4.9 Laptops

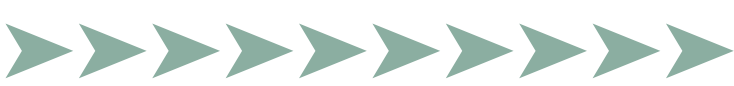
200. Laptops are often used by firms whose staff work offsite regularly. If not properly managed or secured, customer data held on laptops can be lost or stolen very easily. This was demonstrated by the theft, in August 2006, of a laptop containing a large amount of Nationwide Building Society's customer data from the home of a Nationwide employee. This theft exposed weaknesses in Nationwide's data security systems and controls and we fined them £980,000 in February 2007.
201. Despite the widespread publicity the Nationwide case received, we were very disappointed to find some firms still had poor controls over laptops that resulted in a significant risk of data loss or theft.

A medium-sized insurance firm had no policy on whether customer data should be held on laptops, had no means of establishing if customer data was being held on laptops, did not use laptop encryption and did not maintain a list of laptop users. So the firm may not have known if a laptop was lost or stolen and would not have been able to tell if customer data had been compromised. This is very poor practice.

Encryption of laptops – many firms are still exposed

202. As stated in paragraph 6, we support the Information Commissioner's position that it is not appropriate for customer data to be taken offsite on laptops or other portable devices that are not encrypted.

In January 2008, the Information Commissioner's Office (ICO) found Marks & Spencer (M&S) in breach of the Data Protection Act following the theft of an unencrypted laptop which contained the personal information of 26,000 M&S employees. The ICO ordered M&S to ensure that all laptop hard drives are fully encrypted by April 2008.



203. A significant number of firms – some of which were quite large – still allowed the widespread use of unencrypted laptops when they knew they contained customer data or when they had insufficient controls to prevent staff taking customer data offsite.

A major bank with a large number of laptops – most of which were encrypted – was introducing software which could detect unencrypted laptops logging on to the network remotely.

204. It was clear from our review that several firms had put in place laptop encryption projects in light of the Nationwide case. While this is encouraging, it concerns us that, previously, these firms may not have been making an accurate assessment of the risks they faced.

A medium-sized building society told us that encrypting their laptops was not an expensive exercise. A one-off payment of £1,500 was required for the encryption software, plus an extra £39 for each individual licence.

Over-reliance on staff complying with policies and procedures

205. Many firms had decided not to encrypt their laptops because they had policies and procedures in place that prohibited staff from taking customer data offsite. However, there was little consideration of the fact that staff can breach procedures due to work pressures, forget what policies are in place and, in some cases, steal data. It is good practice for firms to consider these risks and ensure they are appropriately mitigated.

A major firm told us that, to ensure a tightly-controlled environment, they operated on the assumption that staff did not know what the firm's policies and procedures were.

The importance of accurate asset registers

'A laptop could go astray for a couple of weeks without being noticed' – Group Security Officer at a medium-sized bank.

206. Some firms we visited did not maintain asset registers that recorded who had been given laptops or other portable devices such as blackberries and USB sticks. This could expose firms to significant risk of data loss because:
- i. they would be unable to monitor all relevant employees' adherence to policies and procedures;
 - ii. they would not be in a position to ensure that all relevant staff had received training on relevant policies and procedures;



- iii. they would not be able to ensure that all laptops and other portable devices had the most up-to-date security features in place; and
- iv. they might be unaware of the loss or theft of a portable device if an employee failed to report it. This would hinder the firm's ability to react appropriately if data was lost and could expose consumers to significant risk of identity fraud.

A medium-sized building society that had spent a significant sum on a laptop encryption project did not maintain an accurate asset register. This meant that some of the firm's laptops might have gone unrecorded and therefore unencrypted.

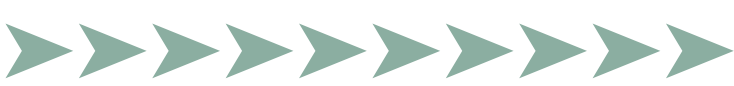
Laptop sharing

207. Some firms allowed the sharing of laptops within teams or had a pool of laptops that could be loaned out to staff for short periods. Such arrangements give rise to the risk that customer data downloaded onto an unencrypted laptop by one user is passed to another without them being aware that customer data is on the laptop. It is good practice for firms to consider the risks to data security that arise from laptop sharing and put in place procedures and controls to mitigate them.

A large bank had procedures in place to ensure that all shared laptops were returned to their IT department. The IT department then responsible for ensuring the laptop's hard drive was wiped before it was passed on to another user.

Laptops – examples of good practice

- The encryption of laptops and other portable devices containing customer data.
- Controls that mitigate the risk of employees failing to follow policies and procedures. We have dealt with several cases of lost or stolen laptops in the past year which arose from staff not doing what they should.
- Maintaining an accurate register of laptops issued to staff.
- 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.



Laptops – examples of poor practice

- Unencrypted customer data on laptops.
- A poor understanding of which employees have been issued or are using laptops to hold customer data.
- Shared laptops used by staff without being signed out or wiped between uses.

3.4.10 Portable media including USB devices and CDs

USB devices and CD writers

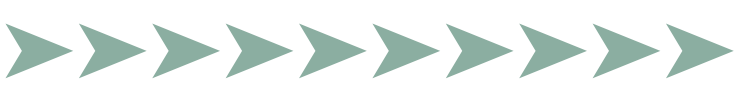
208. In the same way that laptops are convenient for staff who work offsite regularly, USB devices and CDs are often used to transfer data quickly and efficiently, for example to employees' homes or to third-party suppliers. However, if not properly managed or secured, customer data held on portable devices can easily be lost or stolen.
209. We found that large and medium-sized firms generally recognised the risks of data loss arising from the use of portable media and most had locked down USB ports and CD writers. Others which had not locked them down had projects planned to do so. However, most of our total sample – particularly small firms – failed to mitigate the risks arising from portable media when staff had access to customer data.

At least 26 of the 39 firms we visited – including one major bank – did not lock down USB ports when staff had access to customer data.

None of the firms that allowed staff to use USB devices could assure us that all of the USB devices they had issued to staff were encrypted.

Small firms were particularly weak in this area. We did not find a single small firm that locked down their USB ports. This was worrying considering that some small firms allowed all their staff to access all customer data.

210. In addition, very few of the firms that allowed the use of USB devices and CD writers had effective controls to ensure that:
- i. USB devices were encrypted;
 - ii. they knew which staff had been issued USB devices and were authorised to use them;
 - iii. personal USB devices capable of holding customer data – such as memory sticks, MP3 players and mobile phones – could not be used on their computers; and
 - iv. the downloading of customer data onto USB devices and CDs was adequately controlled and monitored.



A major bank had excellent controls in this area. Only staff who had made a strong business case had enabled USB ports. In addition, although USB devices were not encrypted when supplied, software installed on the bank's computers encrypted USB devices when they were used, regardless of whether they were owned by the firm or the individual. Specific types of USB device such as MP3 players could not be connected to any of the firm's computers, even if the USB port was enabled.

Encryption of portable devices

211. Where portable devices are used to store customer data, firms should ensure they are encrypted, as they are often and easily taken offsite.

A medium-sized insurance firm had seven IT staff who could access bulk customer data including full credit card and bank account information. It was possible for these staff to download bulk amounts of data onto personal and/or unencrypted USB devices and there was no formal management or monitoring of their activities.

Increasingly sophisticated mobile phones and other personal technology

212. Several firms were becoming increasingly concerned about the possibility of data theft using high-end mobile phones. Downloading data through USB ports and taking photographs of customer data on-screen are two methods by which this can be achieved. Some firms – particularly with call centres – had taken steps to mitigate this risk or were considering doing so.

Several firms prohibited call centre staff from having mobile phones on display at their workstations. In a mortgage firm, mobile phones had to be switched off in the call centre and staff were not allowed to take personal belongings to their desk. The firm provided storage facilities for their personal belongings.

213. Most of the 12 call centres we visited prohibited staff from using mobile phones at their desks and three gave staff lockers for personal belongings such as bags, mobile phones and MP3 players. However, it was unclear if these measures had been put in place to ensure data security, to increase productivity, or perhaps both. Of course, there are times when staff have a genuine and urgent personal need to use such equipment. Some call centres accommodated staff who needed emergency contact with, for example, their child's school or a sick relative by allowing line management to grant one-off approval for mobile phones to be switched on at the desk. However, such approval was usually time-limited and monitored closely by line management.



A medium-sized insurance firm's security staff used a device that could detect when a mobile phone had been switched on inside the firm's premises.

214. It is good practice for firms to assess continuously the risks posed by increasingly sophisticated mobile technology and put in place appropriate policies, procedures and controls to mitigate them.

Portable media including USB devices and CDs – examples of good practice

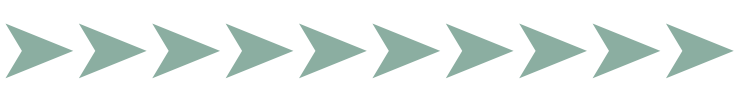
- Ensuring that only staff with a genuine business need can download customer data to portable media such as USB devices and CDs.
- Ensuring that staff authorised to hold customer data on portable media can only do so if it is encrypted.
- Maintaining an accurate register of staff allowed to use USB devices and staff who have been issued USB devices.
- The use of software to prevent and/or detect individuals using personal USB devices.
- Reviewing regularly on a risk-based approach the writing of customer data to portable media to ensure there is a genuine business reason for the activity.
- 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.

Portable media including USB devices and CDs – examples of poor practice

- Allowing staff with access to bulk customer data – for example, superusers – to download to unencrypted portable media.
- Failing to review regularly the threats posed by increasingly sophisticated and quickly evolving personal technology such as mobile phones.

3.5 Physical security

215. Physical security over customer data should be a prime consideration for all firms, irrespective of their size, nature of business and number of customers. During our review, we discussed with senior management, and conducted some limited examination of, the physical security around access to firms' premises, the secure storage of customer data and the implementation and policing of clear desk policies.



3.5.1 Access to firms' premises

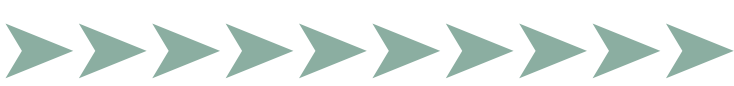
216. A firm's first line of defence in mitigating the risk of data loss is preventing unauthorised access to its premises. Nearly all firms had considered the physical security of their offices, and in 21 of the 39 firms visited we observed good physical security. This was often supplemented with either personal supervision around the office and/or authorised swipe access to areas of the business holding large amounts of customer data, such as call centres, IT areas and server rooms.
217. Many firms, particularly small firms located in vulnerable or run-down locations, had installed intruder deterrents such as buzzers or keypad entry doors, alarm systems, barred windows, and closed circuit television (CCTV) in strategic areas such as car parks and rear entrances. All of these measures gave some protection against the theft of customer data. However, small firms had a general lack of awareness of data security risk, which suggests such measures were in place primarily to prevent the theft of material items such as computer hardware.

At a small financial advice firm, physical access to the building was well controlled with a buzzer to enter the building and an additional keypad code required to access the office. CCTV was used and monitored and the firm maintained a log of who had keys to the office.

218. Larger firms tended to have additional controls such as a reception area for registering visitors, visitor logs, and timed and dated visitor passes. In larger firms, we observed a better understanding than in small firms of data security and financial crime risks in general; this was often coupled with a conscious effort by some to instil a 'data security culture' throughout the business.

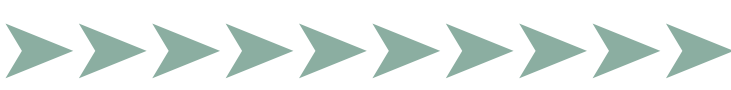
In a medium-sized insurance broker, physical security was excellent. Controls included CCTV, tools to detect the unauthorised use of mobile phones and PDAs, strict visitors procedures, employee training regarding 'tailgating' and enforced stop and search procedures.

219. We would encourage firms to ensure that data security training and awareness programmes cover the more basic risks to customer data such as 'tailgating' to gain entry to offices. In some larger firms, we saw the innovative use of in-house magazines and poster campaigns to raise awareness of basic risks, along with the promotion of key security messages via email, screensavers, mouse mats, and 'post-it' note logos. Training and awareness is covered in more depth in Section 3.2.



A medium-sized investment firm made a conscious decision to use as few third-party suppliers as possible to ensure appropriate security. Security guards and staff in the firm's India call centre were employed directly by the firm and subject to the same vetting as other employees. In addition, the firm had a policy to limit the sharing of customer data with third parties as much as possible.

220. Two larger firms chose to employ security guards as direct employees of the firm, rather than through a third-party supplier. These firms believed that there was a clear benefit with this approach as they did not need to conduct due diligence of a third party and they were clear about the standard of vetting applied to the security guards. In addition, these firms believed that directly-employed staff were more likely to feel a commitment and loyalty to the firm than an employee of a third party. The management of the data security risks arising from the use of third-party suppliers is covered in Section 3.7.
221. In 10 of the 39 firms visited, we observed some alarmingly basic lapses in physical security, which gave rise to a significant risk to customer data and other assets. When we raised our concerns with senior management at these firms, they were generally accepting of the need to review and strengthen current procedures. Examples of these lapses included:
- i. A small financial advice firm located in an industrial estate, whose management considered the risk of burglary to be high, but had no basic security protections such as an alarm or CCTV. In addition, all staff had unrestricted access to the firm's premises outside of office hours.
 - ii. A major insurance call centre where a door fault meant we could access the server room with a visitor's pass. In addition, the firm relied on staff (including a number of third parties not subject to equivalent vetting) to declare when they had accessed the server and communications rooms. There was no checking of electronic access records for undeclared access, despite a swipe-card facility being in place.
 - iii. A small financial advice firm which allowed 12 people, including a security guard, to access their server room. The security guard was not employed by the firm and senior management had conducted no due diligence of the third-party supplier which provided the security guard; in fact, they did not even know the name of the third-party supplier.
 - iv. A medium-sized investment firm, where the cleaners and main building receptionist had not been vetted but had full access to the firm's offices. We were told that the receptionist had no business need to access the offices but sometimes came in to use the microwave. The same firm did not operate a clear-desk policy.

- 
- v. A medium-sized insurance firm with a keypad entry system in place at its call centre, which left its main door wedged open for several hours during our visit.

3.5.2 Clear-desk policy

222. During our review, we observed some extreme examples of good and poor practice in terms of firms' implementation and policing of clear-desk policies. Small firms performed poorly. Eight of the 20 small firms either had no clear-desk policy whatsoever or a worrying lack of concern and understanding at senior management level. In several of these firms, the risk was exacerbated by poor physical security.

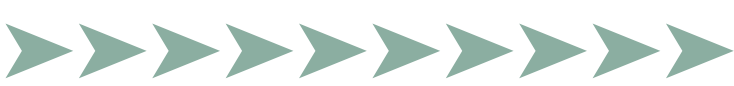
A small financial advice firm did not enforce a clear-desk policy. Documents containing customers' personal details as well as staff's user account IDs and passwords were left on desks when the office was unattended.

223. To minimise the risks of data loss or theft, it is good practice for firms to implement and monitor an effective clear-desk policy, supported by good physical security in and around their premises.

At another small financial advice firm, cleaners had unsupervised access to the firm's offices and alarm system. Despite this, the firm did not enforce a clear-desk policy.

3.5.3 Storage of paper customer files

224. Most firms, particularly small firms, kept paper-based customer records onsite in files. It is good practice for firms to ensure that, as far as possible, paper files are only accessible to staff with a genuine business need and that they are locked away overnight and protected from destruction by fireproof cabinets. Most firms used lockable filing cabinets to achieve this, although there were many occasions where filing cabinets were left unlocked all day, potentially allowing unauthorised staff to access customer data.
225. Seven firms displayed particularly poor and careless practice, such as customer records being stored overnight in unlocked cabinets or being left on the office floor due to a lack of storage facilities. In some firms, these factors combined with poor physical security, the absence of a clear-desk policy, and a poor understanding of the way that cleaners and security guards were vetted significantly increases the risk of data theft. Senior management at these firms gave no reasonable explanation as to why customer records were not stored securely.



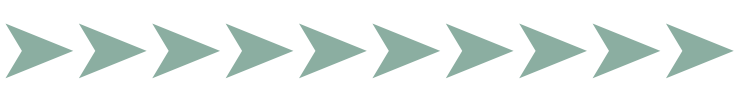
At a medium-sized investment firm with high net worth customers, customer files – including copies of sensitive documents such as passports, driving licences and bank statements – were often left on desks or in unlocked cabinets overnight. During this time, third-party cleaners, who had not been vetted, had unsupervised access to the office area.

Physical security – examples of good practice

- Appropriately restricted access to areas where large amounts of customer data is accessible, such as server rooms, call centres and filing areas.
- The strategic use of robust intruder deterrents such as keypad entry doors, alarm systems, grilles or barred windows, and closed circuit television (CCTV) on a risk-based approach.
- Robust procedures for logging visitors and ensuring adequate supervision of them while on-site.
- 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 which can arise through third-party suppliers accessing customer data.
- Use of 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.

Physical security – examples of poor practice

- Allowing staff or other persons with no genuine business need to access areas where customer data is held.
- Failure to check electronic records showing who has accessed sensitive areas of the office.
- Failure to lock away customer records and files when the office is left unattended.



3.6 Disposing of customer data

226. Every one of the firms we visited demonstrated an awareness of the risk that paper containing customer data could fall into the hands of criminals if disposed of carelessly. All were taking some steps to mitigate that risk by using shredders, locked bins for confidential waste or secure disposal companies. Even firms with poor systems and controls overall were taking some steps to dispose of customer data carefully. This encouraging finding suggests that, despite their failings in other areas, firms do have some awareness of the dangers of data loss, and will take steps to address those risks if there is a simple way to do so at reasonable cost.
227. This progress follows public censure in March 2007 by the Information Commissioner's Office (ICO) of 11 financial services firms which disposed of customer data carelessly.¹⁶ Unannounced checks by the ICO found that customer data had been placed in waste bins or other receptacles on the firms' premises or outside the building. All 11 firms were found in breach of the Data Protection Act. This action received significant media coverage.

'It is unacceptable for banks and other organisations to carelessly discard their customers' information. It is vital that banks and other organisations take security seriously. If they do not, they not only risk further action from the Information Commissioner but also risk losing the trust of their customers. Individuals must feel confident that banks and other organisations are safeguarding their personal information.'

David Smith, Deputy Information Commissioner, speaking after the public censure of 11 financial services firms.

3.6.1 Procedures for disposing of confidential paper

228. Firms in general appear to have learned from the ICO's Enforcement action and coverage of similar issues in the media (eg BBC Watchdog). All the firms we visited had processes in place to ensure the secure disposal of paper-based customer data.
229. Small firms – as well as branches of larger firms – tended to use shredders on their premises, while medium-sized and larger firms usually set up contracts with a specialist secure disposal company. These contractors usually provided locked confidential waste bins for the firm, the contents of which were collected periodically by the contractor. Some waste disposal firms brought a lorry to the premises, emptied each bin directly into the lorry, and shredded the contents onsite. Other contractors emptied the bins into their truck and returned to their own disposal site, where the waste was either shredded or incinerated. Several firms using contractors who shredded paper at the firm's premises ensured their own staff personally supervised the shredding process.

16 www.ico.gov.uk/upload/documents/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf



Some firms combined disposal methods for added security. A medium-sized insurance firm, for example, shredded paper in their offices, stored the shredded paper in secure bins, and employed a secure disposal company to remove and incinerate the shredded paper.

230. Several firms recognised the risk that confidential waste might be placed into general waste bins by mistake. These firms usually mitigated this risk by treating all waste as confidential. Others relied on checks.

A major bank required every one of its branch managers to search general waste bins at the end of the day and to certify that no confidential papers had been placed in them.

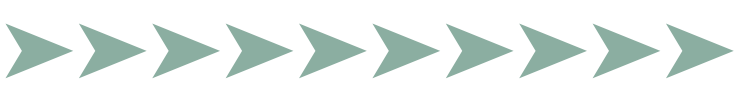
Another firm, which had been censured by the ICO, told us it had since placed confidential waste bins in its branches' banking halls so that customers could dispose of their own waste securely.

231. Some firms were aware of an industry standard for secure disposal firms: accreditation by the British Security Industry Association (BSIA). This is awarded only to contractors which hold the BS7858 accreditation on staff vetting (which includes a five-year background check on employees within 16 weeks of joining) and the BS8470 accreditation on secure shredding procedures. Accredited firms are inspected at least once a year, a procedure that includes testing staff understanding of procedures and spot checks of vetting files. Accredited contractors usually give their client a certificate of secure disposal. Although some firms' contractors will be accredited by the BSIA, we noted that many firms had neither inquired about the security standards used by their waste disposal company, nor had they visited the disposal site to examine security.

Disposal methods for confidential paper

- Fifteen firms out of 39 shredded customer data themselves on their premises.
- Twenty-four firms used confidential waste bins and a third-party secure disposal company instead.
- In nine of these cases, the secure disposal company shredded paper on the firm's premises.
- The other 15 firms used a secure disposal company that removed paper for shredding or incineration offsite.

232. Although firms' arrangements for secure disposal were generally sound, we noted some examples where a lack of adherence to procedures enhanced the risk of data loss.



A medium-sized bank used shredders at its London head office, but did not enforce the same standard at its regional branches, where shredders were either broken or not used.

A medium-sized insurance company left unsecured bags of confidential waste overnight in their car park, which could be accessed by climbing over a low wall.

233. Only a few firms, mostly large ones, had any guidelines or procedures covering the secure disposal of confidential waste for staff who worked offsite. In addition, onsite staff were rarely given guidance about the definition of ‘confidential waste’ and many firms had observed their own staff putting sensitive papers in general waste bins.

In some firms, cleaners who were not vetted or monitored held keys to the confidential waste bins.

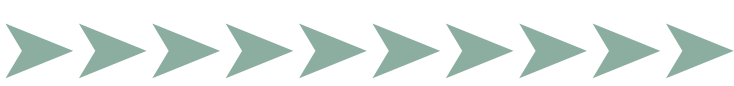
234. Despite these shortcomings, we were pleased that firms in general appeared to be continuing to improve the security of confidential waste disposal. Several firms stated they had recently made improvements to security arrangements even though generally satisfactory procedures were already in place. These improvements included:

- removing general waste bins so that all waste was treated as confidential;
- observing the disposal process to ensure that every bin was emptied into the secure disposal company’s lorry;
- checking how secure disposal companies vetted their staff; and
- auditing adherence to waste disposal procedures.

235. In addition, several firms were aiming to create a ‘paperless office’ so that very little or no confidential waste is ever produced.

3.6.2 Procedures for disposing of obsolete computers and other electronic equipment

236. It is important that firms not only dispose of paper-based customer data securely, but also that electronic customer data held on computers and other devices is destroyed after use. This is because fraudsters might try to obtain computers and other devices that have been discarded by firms in the hope of finding customer data stored on them. It usually requires technical knowledge and appropriate software to erase all traces of data.



In August 2006, the BBC reported that fraudsters in West Africa were able to find internet banking data stored on recycled PCs sent from the UK to Africa.

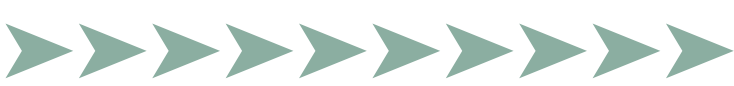
The ICO's Assistant Commissioner, Phil Jones, said 'It is essential that companies have appropriate procedures in place to ensure that personal records on computer hard drives are rendered unrecoverable when they dispose of computer equipment. Under the Data Protection Act, companies have a duty to store personal information securely and delete it when it is no longer required.'¹⁷

237. Although a user without technical expertise might delete files and believe that no files are visible on the hard-drive directory, fraudsters could use widely-available forensic software to retrieve, reconstruct and display files that have been erased. This risk can be mitigated, either by wiping the hard drive using specialist software or by removing or physically destroying the hard drive. The same applies to portable media such as USB sticks, CDs and cartridges.
238. We found that many firms showed some understanding of secure wiping techniques and technology. IT managers mentioned certain software products and explained the appropriate technical standard (stated simply, wiping and reformatting must be repeated many times). Others had been reassured by software providers that their software was used by UK and/or US government departments.
239. However, we found several cases where firms were not actually disposing of their obsolete electronic media. Several IT and Information Security managers with the knowledge and means to dispose of equipment securely were stockpiling old computers – in some cases for several years. This approach creates a new risk that obsolete computers might be stolen or copied. Other stockpiles of computers existed because firms recognised the risk of insecure disposal but did not know any methods of secure destruction.

A medium-sized mortgage administration firm stored 'a couple of hundred' obsolete computer hard drives in an area which could be accessed by up to 20 members of staff. With no register of the drives stored there, it would be impossible for the firm to detect if a drive was accessed or removed. The firm's information security manager planned eventually to drill holes in them to destroy the contents.

240. Large and medium-sized firms often employed a BSIA-accredited third party supplier to wipe and then shred obsolete hard drives, and to certify that process. Some IT staff in medium-sized and small firms preferred to use a hammer, screwdriver or drill to destroy hard drives by brute force. However, some firms were stockpiling old hard drives as they had not considered how to destroy them.

17 <http://news.bbc.co.uk/1/hi/business/4790293.stm>



241. Small firms tended to rely on third parties to wipe their computers securely. A small financial advice firm donated its old computers to a charity which certified that the machines had been wiped and reformatted securely before recycling. Other firms were less rigorous and did not, in our view, display a due standard of care.

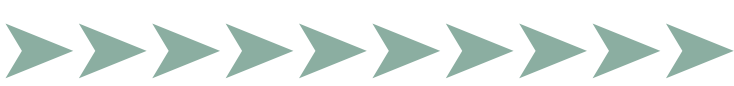
The senior partner of a small investment firm relied on his teenage son to wipe a batch of computers before sending them to a charity in Africa. He did not know what software was used or whether it was effective.

Disposal of customer data – examples of good practice

- Procedures that result in the production of as little paper-based customer data as possible.
- Treating all paper as ‘confidential waste’ to eliminate confusion among employees about which type of bin to use.
- 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.
- Checking general waste bins for the accidental disposal of customer data.
- Using a third-party supplier, preferably one with BSIA accreditation that 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.
- Providing guidance for travelling or home-based staff on the secure disposal of customer data.
- Computer hard drives and portable media being properly wiped (using specialist software) or destroyed as soon as they become obsolete.

Disposal of customer data – examples of poor practice

- Poor awareness among staff about how to dispose of customer data securely.
- Slack procedures that present opportunities for fraudsters, for instance when confidential waste is left unguarded on the premises before it is destroyed.
- Staff working remotely failing to dispose of customer data securely.
- Firms failing to give guidance or assistance to remote workers who need to dispose of an obsolete home computer.

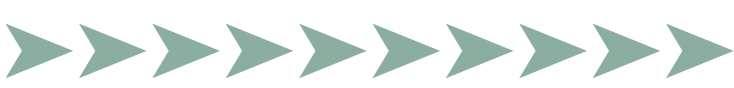


- Firms stockpiling obsolete computers and other portable media for too long and in insecure environments.
- Firms relying on others to erase or destroy their hard drives and other portable media securely without evidence that this has been done competently.

3.7 Managing third-party suppliers

3.7.1 Why do third parties matter?

242. For reasons of efficiency, nearly all firms now use third-party suppliers for certain aspects of their business. It is common for firms to enable these suppliers to access their customer data directly, either on the firms' premises or by sending copies of the data to them. In addition, some firms grant individuals who are not employed by the firm indirect access to their customer data by allowing them to access their premises. As mentioned in Section 2.6.1, firms retain responsibility for customer data, even when it has been transferred to a third party for processing.
243. Examples of the types of third parties used by the firms who have direct or indirect access to customer data include:
- printers and mailing companies;
 - marketing companies;
 - providers of off-site storage facilities for archived files and back-up tapes;
 - confidential waste disposal specialists;
 - couriers;
 - IT contractors and IT maintenance companies;
 - cleaners;
 - security;
 - catering staff; and
 - staff from other companies where offices and buildings are shared.
244. The type and number of third parties used by firms varied considerably. For example, a large bank outsourced all functions they deemed to be 'non-core' such as printing, marketing, cleaning, security and telephone sales. Each of these functions was carried out by a different third-party supplier and all required access to customer data. In contrast, a similar-sized insurance company retained nearly all functions in-house, with minimal reliance on third parties. Smaller firms tended to perform most operations in-house, simply due to the reduced scale of their business but nearly all firms relied on IT support from third parties.



245. It is therefore essential that firms are fully aware of the additional data security risks that arise from allowing third parties to access their customer data. As the number of third parties who have access to customer data increases, so does the risk of data loss.
246. It is good practice for firms to ensure that any individual or company with access to their customer data has appropriate data security standards. As discussed in Section 3.1.3, it is good practice for data security risk analysis to be embedded across the business, with all relevant business areas involved. In the same way, it is good practice for firms to assess the risks of allowing individual third-party suppliers to receive and handle customer data, as well as the risks arising from allowing third parties physical access to customer data on the firm's premises.

3.7.2 Firms' management of third-party suppliers

247. Nearly all firms had existing third-party relationships and most of them managed these relationships in different ways.
248. In general, we were disappointed to find that most firms – including some large ones – were over-reliant on third parties to comply with contractual obligations. There was little evidence that firms either performed data security due diligence on third parties before agreeing a contract or that they exercised audit rights to ensure that third parties were meeting agreed standards throughout the contract term.

Most firms – including some large ones – were over-reliant on third parties to comply with contractual obligations covering data security.

249. For example, an important third-party relationship for many firms is with employment agencies who supply recruitment and staff vetting services. We were disappointed to find that firms rarely examined agencies' recruitment and vetting standards despite specific contractual rights to do so. Instead, firms' senior management often said that the mere existence of such clauses gave them comfort that the agencies would perform in line with the contract terms. Firms' use and management of employment agencies is discussed in more depth in Section 3.3.2.
250. We saw good practice at a medium-sized insurance firm that was conducting a rolling review of all third parties which had direct or indirect access to customer data. The firm was assessing all of the third parties' data security policies and procedures and working with them to improve systems and controls. Firms which audited third-party suppliers commented that comparing data security controls was beneficial both to them and their third party in ensuring that customer data was held securely.

A major bank with over 50 third-party suppliers handling customer data had performed risk assessments on each supplier and visited them frequently to ensure that agreed data security standards were being met.



3.7.3 Issues for firms to consider when using third party suppliers

Who has access to electronic customer data?

251. We noted during our visits that firms sometimes were not aware of which individuals at a third-party supplier had access to their customer data and they did not monitor when or why third parties had accessed their customer data. The most common examples of this were where firms used third-party suppliers to maintain their customer database or provide off-site data back-up facilities.

Many small firms – and some larger firms – used third-party IT service providers to maintain their customer databases. In many cases, the firms did not know:

- who at the third party had access to their customer database;
- the vetting procedures used by the third party to screen their employees; or
- whether the third-party supplier’s staff were able to create copies of customer databases.

In addition, most firms had no monitoring systems in place to track when or why IT service providers had accessed their customer data.

252. Firms that did not know which specific individuals at third-party suppliers had access to their customer data failed to recognise the risk of allowing third parties unrestricted, unmonitored access to their customer data. We were not satisfied that such firms had effective systems and controls in place to protect customer data.

Who has access to paper-based data?

253. It is essential that firms have robust controls in place to ensure that access to paper-based customer data is restricted. The need is exacerbated when firms allow third-party suppliers such as cleaners, contractors and security guards access to their offices, contact centres or storage facilities without vetting them in line with their own recruitment procedures. Physical security arrangements for paper-based customer data are covered in more depth in Section 3.5.3.

How do third-party suppliers vet their staff?

254. Section 3.3 covers staff recruitment and vetting, and includes analysis of firms’ practices and good practice guidance. Where third-party suppliers have access to customer data, firms should ensure they have been vetted to an appropriate standard. Firms can achieve this by vetting third-party staff themselves or, perhaps more efficiently, regularly reviewing that the third-party firm has performed adequate vetting of its staff.



A large investment firm relied on an external recruitment agency to perform all vetting checks on applicants. The firm ensured that the service level agreement set out clearly the types of vetting checks required. The firm also carried out monthly audits and performed sample checking for 10% of all recruits to ensure that vetting was performed in line with agreed standards.

255. In general, we were concerned that firms were often unaware of the vetting standards third party staff had been subject to. In some cases, firms simply did not know whether third-party staff had been vetted at all.

Due diligence

256. As mentioned in paragraph 248, we found that firms generally over-rely on third parties meeting contractual terms relating to data security. Therefore, perhaps unsurprisingly, we found that due diligence of third party suppliers' data security arrangements was not often performed by firms before a contract was agreed.
257. Firms were often unaware of what data security controls, if any, third-party suppliers had in place. Some firms had not even visited off-site storage locations to assess whether the facilities were secure. We do not think it is appropriate for firms to allow third parties access to their customer data when they have not assessed the third party's data security control environment.

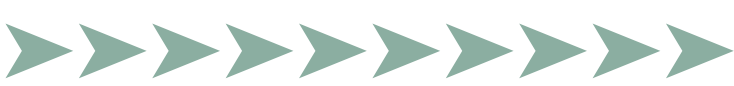
Many small firms selected third-party suppliers on recommendation or on the basis of personal relationships between senior members of the two firms. Due diligence was rarely performed.

258. As a minimum, it is good practice for firms to be clear about exactly which third party staff have access to their customer data and whether they have been vetted to an appropriate standard. This is because, even if a firm has conducted a thorough risk assessment of its own data security processes and procedures, data security will be severely weakened if relevant third parties do not have equivalent standards.

A medium-sized mortgage firm had drawn up a list of 'preferred suppliers' and performed data security reviews on them. However, the firm's purchasing department had identified breaches in purchasing procedures which meant that only 70% of third parties being used by the firm were 'preferred suppliers'; this meant the firm had not reviewed the rest.

How is data protected in transit to third-party suppliers?

259. There are many methods that can be used to transfer data to third-party suppliers but they split into two broad groups:



- electronic means such as email, shared access to networks or a secure internet link between the firm and the third party; and
- physical means such as tapes, cartridges, CDs, USB devices, laptops and paper. The transfer of physical media usually involves entrusting customer data to other third parties, such as couriers.

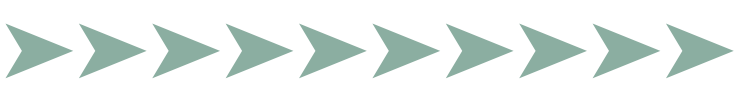
260. Over the past year, we have identified – during both our casework and this review – many examples of poor practice in this area. In general, large and medium-sized firms tend to transfer data to and from third parties using secure internet links but there are still occasions where data is transferred on physical media. These media are not always encrypted and, on rare occasions, unencrypted customer data has been sent by unregistered post.

Wherever possible, it is good practice for firms to ensure that customer data is transferred to third parties using secure internet connections. If there is no alternative to posting encrypted data, some form of recorded delivery is the best option. In addition, it is good practice for the recipient to be notified in advance and for them to confirm receipt of the data. This should ensure that any data loss is identified and dealt with immediately.

261. It is appropriate here to repeat our support for the Information Commissioner’s position that it is not appropriate for firms to allow customer data offsite on laptops or other portable media which are not encrypted.

Managing third-party suppliers – examples of good practice

- Conducting due diligence of data security standards at third-party suppliers before contracts are agreed.
- Regular reviews of third-party suppliers’ data security systems and controls, with the frequency of review dependent on data security risks identified.
- Ensuring third-party suppliers’ vetting standards are adequate by testing the checks performed on a sample of staff with access to customer data.
- Only allowing third-party IT suppliers access to customer databases for specific tasks on a case-by-case basis.
- Third-party suppliers being subject to procedures for reporting data security breaches within an agreed timeframe.
- The use of secure internet links to transfer data to third parties.



Managing third-party suppliers – examples of poor practice

- Allowing third-party suppliers to access customer data when no due diligence of data security arrangements has been performed.
- Firms not knowing exactly which third-party staff have access to their customer data.
- Firms not knowing how third-party suppliers' staff have been vetted.
- 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.
- Allowing IT suppliers to have unrestricted or unmonitored access to customer data.
- 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.

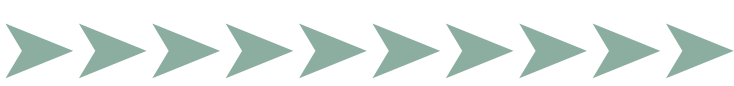
3.8 Internal audit and compliance monitoring

3.8.1 Internal audit

262. A firm's internal auditors are there to give an independent assessment of risks and to report its findings to senior management. As part of our review, we sought to establish the quantity and quality of work on data security by internal audit departments.
263. As anticipated, during our visits to the 20 small firms, we saw little or no evidence either of an internal audit function or of an independent assessment of data security risk. As previously mentioned, if firms consider their in-house resources or expertise are inadequate to perform an effective risk assessment of data security, they should consider seeking external guidance.
264. We saw some evidence of good internal audit practice and awareness in larger firms, but many large firms did not treat data security as a separate issue. Instead, the subject tended to be addressed in parts; for example, relevant IT controls would be examined in an IT audit, physical security during a security audit and vetting during audits of HR. This perhaps reflects many firms' poor governance and lack of coordination when dealing with data security risk and could result in some risks not being considered.

The head of internal audit at a large bank told us that data security had not been considered as a specific risk, and that audits considered processes rather than risks. Therefore, data security only featured in each audit as a risk to the process.

Similarly, overall data security was not considered by internal audit at a major insurance firm; the overwhelming focus of any data security-related audit work was on IT.



265. As noted in paragraph 82, it is good practice for firms to conduct a specific risk assessment of data security. It therefore follows that it is good practice for them to carry this through to their audit work by conducting general audits of data security. Some larger firms conducted specific data security audits and had also brought technical experts into their audit teams to focus on technical risk elements.

A large investment firm had recently employed an experienced internal auditor who had identified the need for an audit of data security across the whole business.

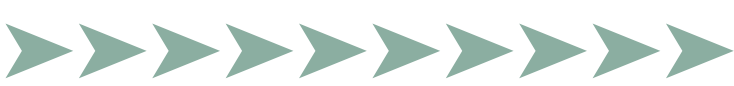
3.8.2 Compliance monitoring

266. We interviewed the compliance officer (or equivalent) in every firm we visited and, although they were generally aware of high-profile incidents of data loss, we found little or no compliance focus on data security in 18 firms. Where compliance departments did conduct some monitoring of data security, this tended to be narrow in its focus and often concentrated only on IT or compliance with data protection legislation; it tended not to focus on compliance with relevant policies and procedures. It is good practice for compliance monitoring of data security to be risk based and consider adherence to relevant policies and procedures, as well as the regulatory and legislative responsibilities set out in Section 2.6.

Following our enforcement action against Nationwide Building Society (see paragraph 53), a large insurance firm's compliance department conducted a gap analysis of its own data security standards. However, the focus was mainly on laptop encryption and access to laptop loss reporting procedures. It did not cover other important aspects of the case such as access to customer data and training and awareness.

267. Data security risk varies in different types and sizes of firm. In many small firms, the role of the compliance officer or external compliance consultant will be to assess, mitigate, and monitor those risks in the absence of a dedicated information security or risk officer. As previously noted, small firms were in practice often entirely reliant on external compliance consultants to provide a review of their business risks. We found evidence during our visits that some consultants may provide small firms with a 'one size fits all' solution to data security which does not take account of individual firms' risk profiles.

We visited two small financial advice firms who used the same compliance consultant. The consultant gave each firm identical Data Protection Policy documents, which both firms regarded as being their data security procedures. This was despite the fact that the firms had different customer bases and therefore ran different risks. These firms' policy documents did not cover specific risks to their business and were therefore inadequate.



268. External compliance consultants were present during some of our visits to small firms and showed an interest in our review and potential outcomes. During our visit to a small financial advice firm, a representative from a large compliance consultancy said that he intended to alter compliance programmes for his clients as a result of what he learned during the visit.
269. As noted in paragraph 95, we would encourage compliance consultants to do more work with small firms on data security. We intend to contact the compliance consultancy firms most often used by small firms shortly after this report is published to update them on our findings and the importance we attach to good data security.
270. In general, Compliance professionals – both in-house and consultants – must widen their view of data security risk and play their part in ensuring good standards of data security across all areas of a firm’s business.

Internal audit and compliance monitoring – examples of good practice

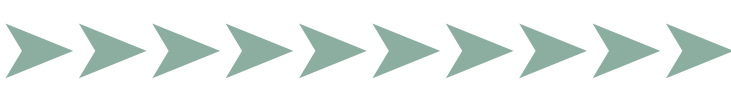
- Firms seeking external assistance where they do not have the necessary in-house expertise or resources.
- Compliance and internal audit conducting specific reviews of data security which cover all relevant areas of the business including IT, security, HR, training and awareness, governance and third-party suppliers.
- Firms using expertise from across the business to assist with the more technical aspects of data security audits and compliance monitoring.

Internal audit and compliance monitoring – examples of poor practice

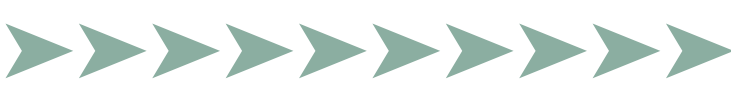
- Compliance focusing only on compliance with data protection legislation and failing to consider adherence to data security policies and procedures.
- Compliance consultants adopting a ‘one size fits all’ approach to different clients’ businesses.

4. Consolidated examples of good and poor practice

<i>Data security – consolidated examples of good and poor practice</i>	
Examples of good practice	Examples of poor practice
Governance	
<ul style="list-style-type: none"> • Identification of data security as a key specific risk, subject to its own governance, policies and procedures and risk assessment. • 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. • 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. • Written data security policies and procedures that are proportionate, accurate and relevant to staff's day-to-day work. • An open and honest culture of communication with pre-determined reporting mechanisms which make it easy for all staff and third parties to report data security concerns and data loss without fear of blame or recrimination. 	<ul style="list-style-type: none"> • Treating data security as an IT issue and failing to involve other key staff from across the business in the risk assessment process. • No written policies and procedures on data security. • Firms do not understand the need for knowledge-sharing on data security. • 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. • A 'blame culture' that discourages staff from reporting data security concerns and data losses. • Failure to notify customers affected by data loss in case the details are picked up by the media.

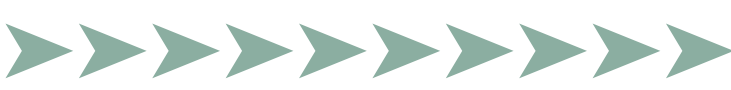


Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Governance	
<ul style="list-style-type: none"> • Firms seeking external assistance if they feel they do not have the necessary expertise to complete a data security risk assessment themselves. • 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. 	
Training and awareness	
<ul style="list-style-type: none"> • 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. • 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. 	<ul style="list-style-type: none"> • No training to communicate policies and procedures. • Managers assuming that employees understand data security risk without any training. • Data security policies which are very lengthy, complicated and difficult to read.



Data security – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
Training and awareness	
<ul style="list-style-type: none"> • Simple, memorable and easily digestible guidance for staff on good data security practice. • Testing of staff understanding of data security policies on induction and once a year after that. • Competitions, posters, screensavers and group discussion to raise interest in the subject. 	<ul style="list-style-type: none"> • Reliance on staff signing an annual declaration stating that they have read policy documents without any further testing. • Staff being given no incentive to learn about data security.
Staff recruitment and vetting	
<ul style="list-style-type: none"> • Vetting staff on a risk-based approach, taking into account data security and other fraud risk. • 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. • Liaison between HR and Financial Crime to ensure that financial crime risk indicators are considered during the vetting process. • 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. 	<ul style="list-style-type: none"> • Allowing new recruits to access customer data before vetting has been completed. • Temporary staff receiving less-rigorous vetting than permanently employed colleagues carrying out similar roles. • Failing to consider continually whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.



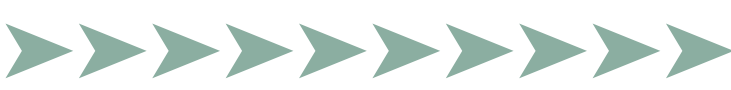
Data security – consolidated examples of good and poor practice

Examples of good practice	Examples of poor practice
Controls – Access rights	
<ul style="list-style-type: none"> • 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. • 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. • A clearly-defined process to notify IT of forthcoming staff departures in order that IT accesses can be permanently disabled or deleted on a timely and accurate basis. • A regular reconciliation of HR and IT user records to act as a failsafe in the event of a failure in the firm’s leavers process. • Regular reviews of staff IT access rights to ensure that there are no anomalies. • Least privilege access to call recordings and copies of scanned documents obtained for ‘know your customer’ purposes. 	<ul style="list-style-type: none"> • Staff having access to customer data that they do not require to do their job. • User access rights set up on a case-by-case basis with no independent check that they are appropriate. • Redundant access rights being allowed to remain in force when a member of staff changes roles. • User accounts being left ‘live’ or only suspended (ie not permanently disabled) when a staff member leaves. • A lack of independent check of changes effected at any stage in the joiners, movers and leavers process.

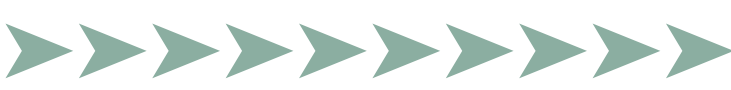


Data security – consolidated examples of good and poor practice

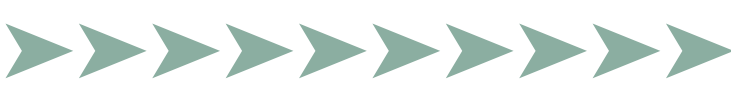
Examples of good practice	Examples of poor practice
<p style="text-align: center;">Controls – Access rights</p> <ul style="list-style-type: none"> ● Authentication of customers’ identities using, for example, touch-tone telephone before a conversation with a call centre adviser takes place. This limits 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. 	
<p style="text-align: center;">Controls – Passwords and user accounts</p> <ul style="list-style-type: none"> ● Individual user accounts – requiring passwords – in place for all systems containing customer data. ● Password standards at least equivalent to those recommended by Get Safe Online – a government-backed campaign group. At present, their recommended standard for passwords is a combination of letters, numbers and keyboard symbols at least seven characters in length and changed regularly. ● 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 password-cracking software on a risk-based approach. ● ‘Straight-through processing’, but only if complemented by accurate role-based access profiles and strong passwords. 	<ul style="list-style-type: none"> ● The same user account and password used by multiple users to access particular systems. ● Names and dictionary words used as passwords. ● Systems that allow passwords to be set which do not comply with password policy. ● Password sharing of any kind.



Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Controls – monitoring access to customer data	
<ul style="list-style-type: none"> • 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. • 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. • 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. 	<ul style="list-style-type: none"> • 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. • Failure to make regular use of management information about access to customer data. • Failing to monitor superusers or other employees with access to large amounts of customer data.
Controls – Data back-up	
<ul style="list-style-type: none"> • 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 encrypting backed up data that is held offsite, including while in transit. • Regular reviews of the level of encryption to ensure it remains appropriate to the current risk environment. 	<ul style="list-style-type: none"> • Firms failing to consider data security risk arising from the backing up of customer data. • 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. • Unrestricted access to back-up tapes for large numbers of staff at third-party firms.



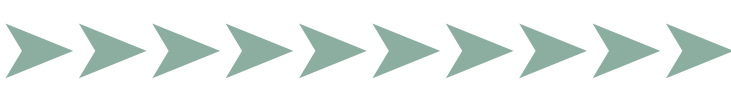
Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Controls – Data back-up	
<ul style="list-style-type: none"> • Back up data being transferred by secure internet links. • Due diligence on third parties that handle backed-up customer data 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 done so in accordance with accepted policies and procedures. 	<ul style="list-style-type: none"> • Back-up tapes being held insecurely by firm's employees; for example, being left in their cars or at home on the kitchen table.
Controls – Access to the internet and email	
<ul style="list-style-type: none"> • Giving internet and email access only to staff with a genuine business need. • Considering the risk of data compromise when monitoring external email traffic, for example by looking for strings of numbers that might be credit card details. • Where proportionate, using specialist IT software to detect data leakage via email. 	<ul style="list-style-type: none"> • Allowing staff who handle customer data to have access to the internet and email if there is no business reason for this. • Allowing access to web-based communication internet sites. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and 'peer-to-peer' file sharing software.



Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Controls – Access to the internet and email	
<ul style="list-style-type: none"> • 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. 	
Controls – Key-logging devices	
<ul style="list-style-type: none"> • 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. • Awareness raising 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. 	



Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Controls – Laptops	
<ul style="list-style-type: none"> • The encryption of laptops and other portable devices containing customer data. • Controls that mitigate the risk of employees failing to follow policies and procedures. We have dealt with several cases of lost or stolen laptops in the past year that arose from staff not doing what they should. • Maintaining an accurate register of laptops issued to staff. • 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. 	<ul style="list-style-type: none"> • Unencrypted customer data on laptops. • A poor understanding of which employees have been issued or are using laptops to hold customer data. • Shared laptops used by staff without being signed out or wiped between uses.
Controls – Portable media including USB devices and CDs	
<ul style="list-style-type: none"> • Ensuring that only staff with a genuine business need can download customer data to portable media such as USB devices and CDs. • Ensuring that staff authorised to hold customer data on portable media can only do so if it is encrypted. 	<ul style="list-style-type: none"> • Allowing staff with access to bulk customer data – for example, superusers – to download to unencrypted portable media. • Failing to review regularly threats posed by increasingly sophisticated and quickly evolving personal technology such as mobile phones.



Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Controls – Portable media including USB devices and CDs	
<ul style="list-style-type: none"> • 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. 	
Physical security	
<ul style="list-style-type: none"> • Appropriately-restricted access to areas where large amounts of customer data is accessible, such as server rooms, call centres and filing areas. • Using robust intruder deterrents such as keypad entry doors, alarm systems, grilles or barred windows, and closed circuit television (CCTV). • Robust procedures for logging visitors and ensuring adequate supervision of them while on-site. 	<ul style="list-style-type: none"> • Allowing staff or other persons with no genuine business need to access areas where customer data is held. • Failure to check electronic records showing who has accessed sensitive areas of the office. • Failure to lock away customer records and files when the office is left unattended.



Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Physical security	
<ul style="list-style-type: none"> • 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. 	
Disposal of customer data	
<ul style="list-style-type: none"> • Procedures that result in the production of as little paper-based customer data as possible. • Treating all paper as ‘confidential waste’ to eliminate confusion among employees about which type of bin to use. • 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. 	<ul style="list-style-type: none"> • Poor awareness among staff about how to dispose of customer data securely. • Slack procedures that present opportunities for fraudsters, for instance when confidential waste is left unguarded on the premises before it is destroyed. • Staff working remotely failing to dispose of customer data securely.

Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Disposal of customer data	
<ul style="list-style-type: none"> • Checking general waste bins for the accidental disposal of customer data. • Using a third-party supplier, preferably one with BSIA 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. • Providing guidance for travelling or home-based staff on the secure disposal of customer data. • Computer hard drives and portable media being properly wiped (using specialist software) or destroyed as soon as they become obsolete. 	<ul style="list-style-type: none"> • Firms failing to provide guidance or assistance to remote workers who need to dispose of an obsolete home computer. • Firms stockpiling obsolete computers and other portable media for too long and in insecure environments. • Firms relying on others to erase or destroy their hard drives and other portable media securely without evidence that this has been done competently.
Managing third-party suppliers	
<ul style="list-style-type: none"> • Conducting due diligence of data security standards at third-party suppliers before contracts are agreed. • Regular reviews of third-party suppliers' data security systems and controls, with the frequency of review dependent on data security risks identified. 	<ul style="list-style-type: none"> • Allowing third-party suppliers to access customer data when no due diligence of data security arrangements has been performed. • Firms not knowing exactly which third-party staff have access to their customer data. • Firms not knowing how third-party suppliers' staff have been vetted.





Data security – consolidated examples of good and poor practice	
Examples of good practice	Examples of poor practice
Managing third-party suppliers	
<ul style="list-style-type: none"> • Ensuring third-party suppliers' vetting standards are adequate by testing the checks performed on a sample of staff with access to customer data. • Only allowing third-party IT suppliers access to customer databases for specific tasks on a case-by-case basis. • Third-party suppliers being subject to procedures for reporting data security breaches within an agreed timeframe. • The use of secure internet links to transfer data to third parties. 	<ul style="list-style-type: none"> • 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. • Allowing IT suppliers unrestricted or unmonitored access to customer data. • 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.
Internal Audit and Compliance monitoring	
<ul style="list-style-type: none"> • Firms seeking external assistance where they do not have the necessary in-house expertise or resources. • 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. • Firms using expertise from across the business to help with the more technical aspects of data security audits and compliance monitoring. 	<ul style="list-style-type: none"> • Compliance focusing only on compliance with data protection legislation and failing to consider adherence to data security policies and procedures. • Compliance consultants adopting a 'one size fits all' approach to different clients' businesses.

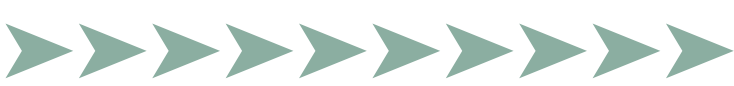


5. Glossary

CIFAS Protective Registration	CIFAS offers a service called Protective Registration that requires anyone applying for credit in that person's name to undergo additional checks. The product, supplied by the Equifax credit bureau, costs £12 plus VAT. CIFAS have recently launched a 'bulk' Protective Registration facility for firms to use in cases of mass data loss.
CIFAS Staff Fraud Database	The CIFAS Staff Fraud Database is used by CIFAS Members specifically for staff vetting and security screening purposes. CIFAS members use the Staff Fraud Database to file data about their staff fraud cases and access staff fraud records filed by other CIFAS Members. For more information, visit: www.cifas.org.uk/default.asp?edit_id=718-87
Controlled function	A role that requires FSA approval of the individual performing it. Controlled functions include senior management, compliance and advisory roles. They are specified in SUP 10.4.5R in the FSA's Handbook.
Customer data	Customer data is any identifiable personal information about a customer held in any format. Customer data includes but is not limited to national insurance numbers, addresses, dates of birth, financial details and medical records.
Cyber-café	A small informal restaurant where you can pay to use the internet.
Data Protection Act	The UK's data protection legislation, which requires anyone who processes personal information to comply with eight principles, that ensure personal information is: <ul style="list-style-type: none">• fairly and lawfully processed;• processed for limited purposes;• adequate, relevant and not excessive;• accurate and up to date;• not kept for longer than is necessary;• processed in line with your rights;• secure; and• not transferred to other countries without adequate protection.
Encryption	The process of changing electronic information or signals into a secret code that people cannot understand or use on normal equipment. Encryption software is widely available for computers and databases, USB devices and mobile telephones.



Hacking	The hacking referred to in this report is where a malicious person infiltrates firms' computer systems in order to manipulate or steal data.
HR	Human Resources
Information Commissioner's Office	The UK's regulator for data protection, responsible for investigating breaches of, and enforcing, the Data Protection Act.
Instant messaging	Communication between two or more people, typed using computers or other electronic devices such as personal digital assistants. Instant messages can be relayed via the internet or inside another network.
IT	Information Technology
Key-loggers	Key-stroke logging or 'key-logging' is a method of capturing or recording a computer user's individual key-strokes. Therefore, passwords to databases containing customer data, as well as encryption keys, can be compromised using key-loggers. Key-loggers come in hardware and software forms. The risk of software key-loggers can be minimised by anti-spyware programmes and firewalls. However, it is more difficult for firms to protect against hardware key-loggers, which can either be attached to a PC or inserted inside keyboards.
Offshoring	The practice of relocating business operations overseas, usually to reduce costs or improve efficiency. IT services and customer call centres are two of the major operations relocated offshore by financial services firms.
Peer-to-peer file sharing	A means of sending and receiving files on the internet, most often used by individuals to exchange music files.
Phishing	A fraudulent attempt to acquire customer data by impersonating someone else. For example, some individuals are duped into revealing their personal data by emails purporting to come from a known and trusted organisation such as a bank. Firms become targets when fraudsters create fake websites or email communications using their name or corporate identity.
Spyware	Software installed surreptitiously on a computer to intercept or take partial control over the user's interaction with the computer. Spyware programmes can collect personal information and can also interfere in other ways, such as installing additional software and redirecting Web browser activity. Anti-spyware software is widely available.
'Straight-through' processing	An IT access model that allows users to log on to their computer with a single password and access all the databases or other systems that they need to do their job without the need for further passwords.



Superuser	'Superusers' most often work in IT and are often responsible for database administration and creating access rights for other staff. Their technical knowledge means they often have the ability to access large amounts of customer data and sometimes to circumvent fraud controls.
Tailgating	Gaining unauthorised access to a restricted building or area by surreptitiously following an authorised person through a secure door or gate.
Third-party suppliers	A company or individual contracted to supply services to a regulated firm.
USB device	A device for storing data, readable by a computer that plugs into a computer's USB port. USB devices can hold large volumes of data and are generally very small and easily portable.
USB port	An outlet on a computer for connecting a USB device.



6. References and useful links

The **Anti-Phishing Working Group** is an industry association focused on eliminating identity fraud resulting from phishing and email spoofing. www.antiphishing.org

APACS is the UK trade association for payments and the banking industry's voice on payments issues. www.apacs.org.uk

Bank Safe Online is the UK banking industry's initiative to help online banking users stay safe online. The site is run by APACS. www.banksafeonline.org.uk

The **British Bankers Association** is a trade association representing banks and other financial services firms operating in the UK. www.bba.org.uk

The **British Computer Society** is an industry body for IT professionals. It plays an important role in establishing standards and training needs for information security professionals. www.bcs.org

The **British Security Industry Association** is the trade association for the professional security industry in the UK which covers, among other things, information destruction. www.bsia.co.uk

British Standards is among the world's leading providers of standards and standards products. Through engagement and collaboration with its stakeholders, it develops standards and applies standardisation solutions to meet the needs of business and society. www.bsi-global.com

Business Link provides advice for businesses on implementing and managing information security. www.businesslink.gov.uk

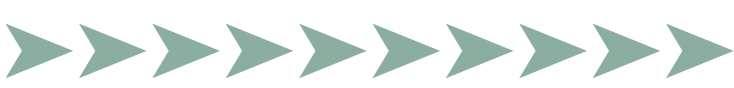
Central Sponsor for Information Assurance (CSIA). The CSIA in the Cabinet Office works with partners across government and the private sector to help maintain a reliable, secure, and resilient national infrastructure. www.cabinetoffice.gov.uk/CSIA

The **Centre for the Protection of National Infrastructure (CPNI)** is the government authority which provides protective security advice to businesses and organisations across the national infrastructure. www.cpni.gov.uk/

CESG is the Information Assurance arm of GCHQ and is the UK government's National Technical Authority for information assurance. www.cesg.gov.uk

CIFAS is the UK's Fraud Prevention Service with 270 Members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring, and share dealing. Its website includes information for consumers and businesses about the risk of identity fraud. www.cifas.org.uk

The **Department of Trade and Industry (DTI)** provides advice for businesses on protecting their information. www.dti.gov.uk/bestpractice/technology/security.htm



Get Safe Online is a site sponsored by leading businesses and the British government to promote security and safety on the internet. www.getsafeonline.org/

The **Home Office** is responsible for ensuring the UK's national infrastructure is protected as well as for policing for hi-tech crimes and gives internet crime prevention advice. www.homeoffice.gov.uk

We are a member of the **Home Office's Identity Fraud Steering Committee (IFSC)**. It has set up a website to educate consumers about identity fraud and the measures they can take to protect themselves from it. www.identity-fraud.gov.uk

The **International Information Integrity Institute** is a group of industry-leading organisations who share their expertise on managing information-related business risks. www.i4online.com

The **Information Assurance Advisory Council (IAAC)** brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection. www.iaac.org.uk

The **Information Commissioner's Office (ICO)** is the UK's independent authority set up to promote access to official information and to protect personal information. www.ico.gov.uk

The **Information Systems Audit and Control Association (ISACA)** publishes on information governance, control and security matters for audit professionals. www.isaca.org

The **Information Systems Security Association (ISSA)** is an international organisation for information security professionals and practitioners that provides educational forums and publications to enhance the knowledge and skill of its members. www.issa.org

The **Information Security Forum (ISF)** is an international association of more than 250 leading organisations which fund and co-operate in the development of practical research about information security. www.securityforum.org

The **Jericho Forum** is an international IT security group which seeks to define methods to deliver secure IT operations in an increasingly internet-driven and networked world. www.opengroup.org/jericho/

The **National Computing Centre** is a membership and research organisation for IT professionals, which promotes information security best practice and guidance. www.ncc.co.uk

The **Ponemon Institute** promotes responsible information and privacy management practices in business and government. www.ponemon.org

The **Security Alliance for Internet and New Technologies (SAINT)** brings together industry leaders and government to exchange information and best practice. www.uk SAINT.org

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: <http://www.fsa.gov.uk>

Registered as a Limited Company in England and Wales No. 1920623. Registered Office as above.

