



# Your responsibilities for customer data security

APRIL 2008

**FACTSHEET**

## **This factsheet is for:**

- Senior management of small firms that handle, store or dispose of customers' personal data in the course of their business

## **It explains:**

- What you should consider when handling, storing and disposing of customer data
- What we found during a major project examining how firms handle customer data (the full report can be found on our website)

## **What is customer data?**

**Customer data is any identifiable personal information about a customer held in any format, such as national insurance numbers, address, date of birth, family circumstances, bank details and medical records.**

### **Key points**

1. Customer data is a high value commodity for fraudsters and securing it is your responsibility. In line with Principles 2 and 3 of the FSA's Principles for Businesses, you should make an appropriate assessment of the financial crime risks associated with your customer data.
2. SYSC 3.2.6R requires firms to take reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime.
3. This factsheet outlines the areas of your business that you should consider when assessing the risks to your customer data including; physical security, governance, staff recruitment and vetting, training and awareness, systems and controls, disposal of data, third parties and compliance.

*“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.*”

Richard Thomas – Information Commissioner

## Ensuring physical security over customer data

### Key point

Physical security should be appropriate to prevent unauthorised access to customer data.

Many small firms are responsible for their own office security. It is good practice to assess the risk of unauthorised access to your premises and ensure a commensurate level of security to protect your customer data.

You may wish to consider:

- Installing alarms or CCTV;
- Restricting access to the office with the use of door buzzers or key pad entry;
- Monitoring visitors to your office by recording access and departure with a signing-in book and supervising visitors to your premises at all times;
- Discussing with local businesses or your local police force the key security risks in your area;
- Raising staff awareness of the risks of poor physical security.

### Questions to ask yourself

- Are your premises vulnerable to a break-in?
- Is physical access to your premises and restricted areas, such as computer servers, properly controlled?
- Do you maintain a clear desk policy to reduce the risk of customer data being lost, stolen, or being accessible to unauthorised persons?
- Do you keep your filing cabinets locked when not in use?

## Governance

### Key point

It is good practice for senior management to assess data security risk and put in place appropriate policies, procedures and controls to reduce it

In the majority of small firms, data security is not considered as a specific risk and nobody is assigned responsibility for it. In addition, many firms treat data security solely as an IT issue and do not involve key staff from across the business (such as those with responsibility for human resources, security and countering financial crime) in their data security work.

We do not expect small firms to spend as much money or resource on data security as larger firms but you should make an assessment of the risks to your customer data. In addition, it is good practice to have written data security policies and procedures, which are proportionate, accurate and relevant to your day-to day business.

Some small firms have simple lists of 'do's and don'ts' in place of procedures. For some firms, this is an effective approach which makes the importance of data security easy for staff to understand.

### Questions to ask yourself

- Is there a specific focus on data security in your firm?
- Do you have any written policies or procedures covering data security and are they proportionate and relevant to your day to day business?
- Do you have an open and honest culture which encourages staff to report data security concerns?
- Do your staff understand why data security is important and do they know what to do to keep customer data safe?
- Do you seek external assistance or liaise with peers about data security risks and implementing good internal controls?

## Recruiting the Right Staff

### Key point

Your recruitment and staff management processes should give you comfort that your staff are not susceptible to stealing data or committing fraud.

Small firms recognise the requirements to determine whether staff in FSA-approved roles are fit and proper and carry out various checks to determine this, including credit checks and criminal record checks.

However, in most firms, more junior staff such as those in administrative roles tend to have access to the most customer data and therefore present a higher risk in terms of potential data loss or theft. In fact, there have been several cases where junior staff have been bribed or threatened by criminals who wish to obtain customer data to commit fraud. Small firms' recruitment processes for such staff often rely solely on personal recommendations or basic references. Firms should be applying a risk-based approach to reducing financial crime and enhancing recruitment checks where appropriate.

You may wish to consider:

- Credit checks and criminal record checks on staff with access to large amounts of customer data.
- Repeating credit checks periodically to ensure that staff in financial difficulties, who may be more susceptible to bribery or committing fraud, are appropriately managed.

### Questions to ask yourself

- Are you satisfied that people you recruit have the honesty and integrity to handle customer data?
- Do you conduct credit checks and criminal record checks on staff with access to large amounts of customer data?
- Do you hold regular meetings with staff and would you identify changes in employees' circumstances which might make them more susceptible to financial crime?
- Are there any aspects of your recruitment and staff management processes that could be improved to reduce the risk of data theft?

## Educating staff on data security

### Key point

It is important that your staff understand the importance and relevance of data security policies and procedures.

Many firms rely on staff signing an annual declaration to confirm they have read policies and procedures but do not check whether staff understand them. We have seen some firms using simple and easily-understood guidance and education for staff through group discussions, awareness raising emails, intranet sites, staff magazines and poster campaigns, none of which are expensive or time consuming. It is good practice to put in place simple and effective methods to raise staff awareness and periodically test your staff's understanding of data security.

## Questions to ask yourself

- Do your staff understand the importance of data security and know how to keep customer data secure?
- Do you provide your staff with any training on data security and has this been tested?

## Systems and Controls

### Key point

Your systems and controls should be appropriate to minimise the risk of data loss or theft.

There are many systems and controls which can minimise the risks to customer data. You should consider on a risk-based approach which of these it is proportionate to put in place. Poor controls lead to a greater risk of data loss or theft.

### Access Rights to IT systems

We appreciate that staff need access to customer data to do their jobs. However, it is poor practice for staff to have access to systems or customer data that they do not require. It is good practice to consider whether staff who change roles retain access rights that they no longer need and to conduct regular reviews of individuals' IT access rights.

You should also consider a risk based, proactive monitoring of staff to ensure that they are accessing or changing data for genuine business reasons.

## Questions to ask yourself

- Do my staff have access to customer data that they do not need?
- When my staff change roles, are unnecessary access rights removed?
- Could we perform random checking to ensure that staff are only accessing customer records for genuine business reasons?

### Passwords and user accounts

It is good practice for each staff member to have their own username and password for IT systems, for good password standards to be in place and for firms to ensure that staff do not share usernames and passwords, or write them down.

*Get Safe Online* ([www.getsafeonline.org](http://www.getsafeonline.org)) recommends that passwords should be a combination of letters, numbers and keyboard symbols at least seven characters in length and changed regularly.

### Questions to ask yourself

- Do each of your staff have their own username and password?
- Do your passwords meet the standards recommended by Get Safe Online?
- Do your staff understand the importance of strong passwords?
- Do any of your staff write down their passwords or share them with colleagues?

### Taking customer data offsite

Many firms have staff who work from home or use laptops and other portable devices such as memory sticks and CDs to store or transfer customer data. You should consider the risks to your customer data that could arise from these situations, particularly the loss or theft of a laptop or portable device. It is poor practice for you or your staff to hold customer data on laptops and other portable devices which are not encrypted. **The Information Commissioner has recently stated that firms should ensure that laptops and other portable devices used to store customer data should be encrypted. We support his view.**

Whilst we appreciate that portable devices such as memory sticks and CDs are good business tools, such devices can be easily concealed and used largely undetected. Therefore, you should consider the risk of data loss or theft that can arise if portable devices are used without authorisation or in breach of procedures. For example, you might wish to consider:

- disabling USB ports and CD writers on your computers if your staff do not need to use memory sticks or CDs to do their jobs; and
- issuing encrypted memory sticks to staff who need them.

It is good practice to maintain a clear record of who owns laptops and memory sticks to ensure that you would notice if one had been lost or stolen. In addition, you might wish to consider random checks of laptops to ensure that only staff authorised to hold customer data on their laptops are doing so.

### Questions to ask yourself

- Do any of your staff work from home or take customer data offsite on laptops, memory sticks or CDs?
- If so, are the files containing customer data, or the devices themselves, encrypted?
- Would you know if one of your staff's laptops, memory sticks or CDs was lost or stolen?
- Do you make regular checks of what customer data is being stored on laptops and other portable devices?
- If staff use home computers for business purposes, how securely is customer data held?
- Do you understand the threats posed by increasingly sophisticated and quickly evolving mobile technology?

## Backing up customer data

Many firms do not appreciate the risks of insecure data back up and storage methods. Our project highlighted a lack of clear and consistent procedures for backing up data, and a lack of awareness of how securely firms' backed up data was being held.

Many firms do not consider encrypting their back up data, and this raises further concerns when the back up is held offsite by a third party, particularly when due diligence on the third party is insufficient. Many firms also allow their backed up data to be held overnight insecurely. Some firms back up tapes were left in employees' cars or on kitchen tables.

Firms should consider reviewing their data back up procedures and consider the threats to customer data throughout the whole back up process – from the production of the back up tape or disk, through the transit process, to the ultimate place of storage.

### Questions to ask yourself

- Do you have agreed and consistent procedures for the back up of customer data?
- Are your storage facilities sufficiently secure to minimise the risks to customer data?
- Do you encrypt your backed up data?
- Have you carried out adequate due diligence on any third party that is entrusted with the storage of your back up data?
- If you rely on a staff member to hold backed up data overnight, do they hold it securely?

## Internet and Email availability

The internet and external email are important business tools for financial services firms but both increase the risk of data loss or theft if used in an uncontrolled fashion. It is therefore good practice to provide internet and email facilities only to staff with a genuine business need.

You should consider carefully the risks arising from allowing staff to access web-based communication facilities, examples of which include:

- web-based email (eg Hotmail);
- social networking sites (eg Facebook);
- instant messaging (eg MSN Messenger);and
- file sharing software (eg Limewire)

If your staff use these facilities, there is an increased risk that your customer data might be lost or stolen without you knowing. It is good practice to completely block access to these types of internet facilities, especially if staff have access to customer data.

### Questions to ask yourself

- Do all of my staff really need internet and external email access?
- Can my staff access web-based communication facilities such as Hotmail, Facebook and MSN Messenger?
- Do any of my staff use file sharing software to listen to music while they are working?
- Do I need to get software to block my staff accessing websites that pose a risk to my customer data?

## Disposal of data

### Key point

All customer data should be disposed of in a secure fashion.

Customer data can be held in paper and electronic format. It is important that you consider measures to ensure that all customer data is securely disposed of regardless of its format.

In 2007, there was significant media coverage of banks disposing of paper-based customer data insecurely. The reputational and regulatory risks of doing so are high, and so is the financial crime risk to your customers. Many small firms tend to dispose of paper records by shredding all confidential waste in-house and some use a specialist secure disposal company. It is good practice for you to use these methods.

On the electronic side, computer disks and CDs should be destroyed or shredded before disposal. In addition, you should consider the secure disposal of computers and hard drives when they come to the end of their life. It is poor practice to simply dispose of a computer at a rubbish dump, donate it to a charity or sell it to your staff, without first removing, destroying or wiping the hard drive. If you choose to wipe the hard drive, specialist software should be used. You should consult an IT specialist if you need advice.

### Questions to ask yourself

- Do you shred your customer data onsite and are your staff aware of how they should be disposing of customer data? Do they need reminding?
- If you use a third party to dispose of customer data, do you know the company, how it destroys your data, and how they vet their staff?
- If you have ever disposed of a computer or given one to somebody else, did you wipe the hard drive with specialist software or remove and destroy the hard drive?

## Third Party suppliers

### Key point

You should know who your third party suppliers are, the security arrangements around any customer data that they hold or have access to, and how they vet their staff.

Many firms use third party suppliers to carry out functions which could give them access to customer data, such as secure disposal, archiving, IT administration, office cleaning and security. It is good practice to satisfy yourself that you know your third party suppliers, how they vet their staff and have a good understanding of their security arrangements.

We have found that many firms do not carry out due diligence on third party suppliers before they hire them and some firms do not know who their cleaning and security staff are, which can put customer data at risk if files are not secure or there is no clear desk policy.

If you use third party suppliers, you should consider:

- conducting good due diligence to assess their policies and procedures, including recruitment, security and levels of service. You could achieve this by visiting third party suppliers to ensure that you understand how they will treat your customer data.
- monitoring and supervising their access to your offices and customer data.
- using secure internet links, encryption, and registered or recorded mail when transferring data to third parties.

### Questions to ask yourself

- Do you know all of your third party suppliers?
- Have you carried out any due diligence on third parties, including their security arrangements and staff vetting policies?
- Do you allow third parties to work unsupervised in the office? If so, do you lock away your customer data and enforce a clear desk policy?

## Compliance and monitoring

### Key point

Compliance monitoring of data security should be risk-based.

The majority of compliance officers within small firms do not check whether data security policies or procedures are being followed. In addition, external compliance consultants used by many small firms do little or no specific work on data security with firms.

This factsheet highlights many aspects to consider when implementing good data security measures. Compliance can have an important role in the monitoring and ongoing review of good practice in these areas.

### Questions to ask yourself

- Does your compliance officer or consultant do any work on data security?
- If so, does it cover any or all the areas highlighted in this factsheet?