The Fraud Advisory Panel

the fraud advisory panel Identity Theft: Do you know the signs?

IDENTITY THEFT: DO YOU KNOW THE SIGNS?

A guide for businesses and individuals

Executive Summary

It has been estimated that identity fraud in all its forms will cost governments, businesses and individuals world-wide US$221 billion by the end of 2003.[1] This figure is estimated to triple to $2 trillion by the end of 2005.

According to a Cabinet Office report the British Economy suffers a loss of £1.3 billion per year as a result of identity fraud.

CIFAS reported in 2002 that cases of identity theft for financial gain have doubled to 75,000 in two years.

The Department for Work and Pensions estimates that up to £50 million was lost by way of benefit fraud carried out by identity fraudsters in 2001-2002.

APACS have reported that credit card fraud, which is one form of identity fraud, caused annual losses of nearly £430 million in 2002.

In this paper the Fraud Advisory Panel deals with the prevalence and scale of identity theft, the ways in which identity theft manifests itself, and provides illustrations as to how identity theft is perpetrated against:

- Government and the Public Sector;
- Business; and
- Individuals.

In particular the Fraud Advisory Panel looks at the following methods:

- Application Fraud – where a fraudster applies for payment cards and financial products in the name of his victim;
- Account take-over – where the fraudster collates sufficient information about the victim to dupe the victim's bank that they are the victim;
- Wholesale assumption of the victim's identity – obtaining false passports and identification documents or using the identity of a dead person which may result in fraudulent claims for social security benefits;
- The fraudulent use of a business identity.

[1] The Aberdeen Group Identity Theft: A $2 Trillion Criminal Industry in 2005. May 2003

How can a victim, be they a business, a government department or an individual, reduce their chances of becoming a victim of identity fraud? How can identity fraud be prevented and detected?

The Fraud Advisory Panel has devised a number of methods by which the public sector, private sector and individuals can manage their affairs to assist in reducing the chance that they become a victim of identity fraud. The Fraud Advisory Panel has also produced a number of recommendations as to how to deal with a fraud once it has happened.

The paper looks at:

- Data-sharing and cross referencing of information between governmental agencies and the business sector;
- Technological and organisational methods which can be implemented to detect and prevent identity fraud;
- Fraud reporting systems and the appointment of personnel with specific responsibility;
- Protection of employees who blow the whistle on fraud;
- Duties of directors to deal with fraud;
- Asset recovery and how to reduce fraud losses via the civil courts;
- Compliance.

The Fraud Advisory Panel emphasises the importance that organisations take advice in relation to appropriate steps that they might take to monitor fraud and data-share. Identity fraudsters take advantage of the intelligence gap between businesses and government agencies in order to perpetrate this type of fraud.

Organisations must ensure that the chances of detecting identity fraud are not hindered as a result of a misunderstanding of the extent of the Data Protection Act 1998 and similar legislation. Organisations should ensure that they are fully appraised of the steps that they may legitimately take to monitor fraudulent activity.

Although it is necessary to take specialist advice before implementing data-sharing, databases and monitoring policies in order to detect fraud, it is in general permissible to do so if the steps are proportionate and for the purposes of monitoring suspected criminal activity.

The Fraud Advisory Panel is concerned that employees and individuals receive awareness training in order that they recognise the tell-tale signs of identity fraud.

The paper also includes a number of useful links and contact numbers.

IDENTITY THEFT: DO YOU KNOW THE SIGNS?

A guide for businesses and individuals

"Identity Theft in all of its forms is on track for $2 trillion in financial losses by the end of 2005" The Aberdeen Group, May 2003[2]

"Identity theft is the fastest growing form of white collar crime." IBM, June 2002

1. Introduction

1.1 What is Identity Fraud and how serious is it?

- Identity Fraud costs the British Economy £1.3 billion per year.
- CIFAS – The UK's Fraud Prevention Service – reported in 2002 that cases of identity theft for financial gain have doubled to 75,000 in two years.
- CIFAS also estimated that the reported cases have cost the victims £62.5 million per year.

Identity fraud involves the use of an individual or a company's identity information to open bank accounts, obtain payments or credit, fraudulently obtain social security benefits (in the case of individuals) or obtain goods and services.

The means by which the fraudster does this can vary extensively.

a) A fraudster may simply apply for credit cards or open bank accounts in the name of a different person using pieces of personal and financial information and old utility bills belonging to the victim. This type of identity fraud is sometimes referred to as 'Application Fraud'.

b) Identity fraudsters may also attempt to perform an 'Account take-over' by collating information about an individual and later contacting the individual's bank and informing them of an address change. The fraudster will then call the bank and order a new debit or credit card which is sent directly to the fraudster.

c) Alternatively identity fraud may involve the assumption of a person's identity. The fraudster will obtain a certified copy of the victim's birth certificate (which is both straightforward and lawful) and apply for identification documents on the basis of that birth certificate. Identification documents could include passports, driving licences and national insurance. Once you have those documents a myriad of benefits can be obtained in the individual's name.

---

[2] Jim Hurley, Vice President of Security and Privacy, The Aberdeen Group Study: "Identity Theft: A $2 Trillion Criminal Industry in 2005" 13 May 2003

d) In the case of a business identity a fraudster may simply use invoices or company stationary to obtain goods and services without paying for them or may create an entirely false trading history. Alternatively, using the Internet, a fraudster may set up a copycat or similar website in order to dupe the customers of one business to part with money or credit card details.

Scotland Yard's Assistant Commissioner in charge of crime operations said recently, "It is now comparatively easy to assume the identity of another person and live in the UK without fear of exposure." He said that identity theft was an integral part of 30 to 40% of all white-collar crime.

The victim is usually totally unaware that their identity has been stolen until, for example, they make an application for a credit card, bank loan or mortgage and discover they have a low credit rating. The fraudster has incurred substantial debts in the name of the victim and it is up to the victim to establish to the satisfaction of the credit reference agency, and all others concerned, that a fraudster is responsible for the debt.

Example 1

It has been reported that the Police have said that an increasing number of 'mirror' sites have been discovered in the UK. Such sites may ask the victim to fill in online application forms which include current bank details allowing the identity fraudster to obtain the information he needs to carry out a fraud.

Both Barclays and Citigroup banks have been the victim of bogus or copycat websites which have been set up as part of a fraud by organised West African criminal gangs.[3]

Example 2

The largest online auction in the world, eBay, is another victim of identity fraudsters setting up mirror sites.

The fraudsters set up the website and then sent emails to customers requesting that they submit their financial details and passwords to ebayupdates.com using the ruse that the staff at eBay were experiencing technical difficulties with billing information.

Potentially 55 million eBay customers could have been affected. Fortunately the site was quickly detected and Internet users were warned by the US Internet watchdog SANNS. Subsequently eBay confirmed that it never requested customers to disclose their passwords.

[3] Business Day (South Africa) 4 March 2003 "Nigerian Conmen Sharpen Their Crooked Ways" by Thomas Catan and Michael Peel.

Example 3

Financial institutions have been targeted by a new range of identity frauds which have potential liability for UK banks. It was reported that West African fraudsters are infiltrating banks to gather information and pass the information to outsiders. Some fraudsters have hijacked the identities of banks to perpetrate fraud which has been highlighted by NCIS (the National Criminal Intelligence Service) in its latest UK threat assessment of serious and organised crime.

Confidential details are apparently passed to accomplices outside the bank who then make unauthorised transfers to drain accounts. The DTI and the City of London Police fraud squad has said that this is "the most significant trend at the moment".

Banks could be held liable if it is found that they did not make an effort to prevent identities being appropriated on the basis they failed to adequately protect personal data as required under the provisions of the Data Protection Act 1998. ('DPA')

[Financial Times]

Example 4

In May 2002 it was reported that Akinwole Alawode, a 26-year-old Nigerian citizen, stole the identity and social security numbers of his victims in order to obtain money from local banks. He obtained cheques and withdrew funds from victims' bank accounts. Once stolen cheques had cleared he issued further cheques payable to other stolen identities' bank accounts and withdrew the funds as cash, thereby using the identity of his victims not only to steal but to launder the proceeds of his crimes.[4]

As can be seen from the above examples, identity theft is usually carried out for financial gain and it is therefore important that the assets of the fraudsters are pursued. Developing a reputation for attacking the assets of identity thieves may be one way of deterring future fraudsters. (See 6 below)

1.2 Further Statistics

CIFAS reported that in 2002 9,000 identity frauds in the UK involved the use of a dead person's identification details as compared to 2,500 identity frauds in 2001. More recent statistics demonstrate that the number of reported identity frauds involving the use of the identities of the dead or recently deceased in 2001 totalled 5,000. The total number of identity frauds in 2002 was 42,029 as compared to 27,270 in 2001.

In the United States over 700,000 citizens are affected by identity theft and credit card fraud every year. The Federal Trade Commission reported that 42% of all complaints in 2001 were of identity theft. It is estimated that 750,000 US citizens had their identities stolen in 2002.

[4] FT.com 8/5/2002

The Association for Payment Clearing Services (APACS) reported that application fraud cost the UK £10.2 million in 2002 as compared to £6.6 million in 2001. Account take-over fraud cost the UK £10.4 million in 2002.

The National Audit Office Study into benefit fraud recently concluded that one of the main types of organised fraud faced by the Benefits Agency is identity fraud. The fraud is nearly always perpetrated by the use of forged documentation or by the use of a dead person's National Insurance Number. The Department for Work and Pensions estimates that the overall cost of benefit fraud is £2 billion of which up to £50 million is based upon "wholly fictitious identities".[5]

1.3 CIFAS & APACS

The Association of Payment Clearing Services ('APACS') is a UK Trade Association of banks and building societies. It has responsibility for the "co-operative aspects of money transmission and other payments-related developments". It regularly produces surveys of current trends in payment card fraud and guidance for both organisations and individuals.

CIFAS – The UK's Fraud Prevention Service – is a service for preventing fraud. Member organisations can exchange application details which are believed to be fraudulent because the information has failed verification checks. Amongst other services, the organisation allows members to share data relating to accounts which are suspected of being used for fraudulent purposes. CIFAS also runs the Protective Registration Scheme which means that a person's credit file can be flagged if their identity has been used for fraud.

1.4 The Offence

Surprisingly, it is not actually a crime in the UK to assume another person's identity. The situation has become so serious that the UK Government is currently considering whether an offence ought to be created. Currently the use of a false identity or the adoption of another person's identity is not a criminal offence unless it can be proved that there was some conspiracy to commit a criminal act or fraud, or it can be proved a criminal act took place as a consequence.

Identity frauds are therefore hidden in the statistics of deception or theft. If a credit card is stolen and used for 100 different transactions, this is still only logged as one theft.[6]

[5] Department for Work and Pensions: Tackling Benefit Fraud, 13 February 2003, page 15
[6] Fraud Watch – Issue 2 Vol 11 2003

2. Who can become liable as a result of Identity Theft?

Both the private sector and businesses can become the victim of identity fraud. A company could become liable as a result of identity fraud in a number of ways:

Example 5

A former Police Sergeant stole his dead nephew's identity so that he could borrow $10 million to finance property deals. The fraudster had been declared bankrupt in 1995 and so assumed the identity of his dead nephew who by co-incidence had the same name. Once the fraud came to light the fraudster was prosecuted and sentenced to over seven years' imprisonment.

The Lenders still lost $3.1 million and $3.4 million between them.

2.1 Credit Card Fraud

For example, if a fraudster makes purchases from a retailer using someone else's credit card details, the credit card company will usually indemnify the consumer for all of his loss although the cardholder is potentially liable for the first £50 of his loss. However the credit card company may then look to the retailer to indemnify its loss by way of a charge back. In June 2002 Experian reported that 73% of retailers were still experiencing charge backs from net fraud.

Credit card fraud is another form of identity fraud. In November 2002 APACS reported that credit card fraud caused annual losses of nearly £430 million in 2002.

One of the most prevalent forms of credit card fraud at present is skimming. Skimming is a method of counterfeiting credit cards and accounted for 35% of fraud losses in the UK in 2000. In 2002 counterfeiting cost the UK £148.5 million.

Skimming entails the passing of the credit card through a small electronic device which copies the magnetic strip and other details. These are transferred on to a machine which copies the details on to a fake card. The fake credit card can then be used by the fraudster or, alternatively, the details may be sold on and used in another country making it extremely difficult to pinpoint exactly who stole the details and to take any action against the individual who eventually carries out the credit card fraud.

This has commonly occurred in restaurants and bars throughout the UK where, as a matter of practice, payment cards are often taken out of the holder's vision for a period of time whilst the credit card is swiped behind the bar. This leaves ample opportunity for the bar tender or waiter to make his own copy. This problem will to some extent be eradicated by the introduction of microchips and the use of Personal Identification Number (PIN) technology which will make it increasingly difficult for credit cards to be counterfeited. However it will not prevent other forms of credit card fraud such as application fraud or card-not-present fraud.

2.2 Internet Service Providers ('ISPs') and Data Providers ('DPs')

The provision of large volumes of data from unscrupulous ISPs or DPs who hold or have access to vast quantities of personal or financial information such as credit card details or credit references is another way in which fraudsters may accumulate information about individuals.

It has been suggested that some fraudsters have obtained the requisite information by making payments to such organisations in return for this valuable data.

Example 6

In November 2002 three men were charged in New York with having brought about a huge identity fraud. The individuals stole around 30,000 victims' credit information costing around £1.7 million. Instrumental in the scheme was a software company worker who agreed to provide codes for downloading credit information about the victims. One of the individuals pleaded guilty to mail fraud having admitted that he changed individual credit accounts.

Example 7

Philippsohn Crawfords Berwald were retained in a recent case where a group of fraudsters obtained identifying documentation relating to a company including VAT certificates, invoices, and company stationary from one source. This documentation was subsequently amended slightly and used by the fraudsters to convince a supplier that they were genuine customers. The supplier carried out checks on the basis of that documentation. This sophisticated fraud included the use of a telephone number which was similar to that of a High Street Bank call centre. The suppliers were asked by the fraudsters to telephone the number to obtain confirmation that the funds had been received in order that they could release the goods. On the strength of that confirmation and on the basis of the documentary information the fraudsters had produced, the company supplied £100,000 worth of goods to an address in London. The goods promptly disappeared as did the fraudsters.

3. Possible Solutions

The Fraud Advisory Panel has recognised a number of ways in which corporate identity fraud can be reduced, prevented and detected. These include:

1. The concept of data-sharing and the effective use of shared and collated information;

2. Steps which may be taken to prevent and detect fraud;

3. The use of civil courts in order to enable victims to recover stolen assets;

4. Protection of employees who report frauds.

4. Data-Sharing

4.1 Data-Sharing – General

Data-sharing and cross-referencing will mean that there is a greater chance of detecting identity theft and at an earlier stage.

Any exercise involving the sharing of personal or financial data must take account of the provisions of the DPA which require that data is processed in accordance with the eight principles of data protection. The data must be:

a) Fairly and lawfully processed.

b) Processed for limited purposes and not in any matter incompatible for those purposes.

c) Adequate, relevant and not excessive.

d) Accurate.

e) Not kept for longer than necessary.

f) Processed in line with the data subject's rights.

g) Secure.

h) Not transferred to countries without adequate protection.

There are, however, exceptions to these principles and in particular Section 29 of the DPA allows for certain exceptions to be made when data is processed for the purposes of prevention of crime.

Each instance of data-sharing requires specific advice and as such it is impossible to give a general rule as to when data-sharing may be permitted.

It is also necessary to register with the Information Commissioner if your organisation wishes to process personal information.

4.2 Data-Sharing – The Government and Public Sector

(i) The Government needs to make legislative provision to clarify the situations in which data-sharing between organisations within the public sector will be lawful. The Government may also need to consider tightening up the procedures which allow access to birth certificates.

(ii) However Government bodies may need to consider the provisions of the Human Rights Act 1998 and Data Protection Act 1998.

(iii) In particular, the Government needs to consider the application of the Data Protection Act to situations where data-sharing is necessary in order to prevent and detect fraud. Some practitioners consider that the current state of affairs means that fear of the regulators is hindering attempts to reduce fraud by means of data-sharing.

Example 8

The National Audit Office report into benefit fraud reported that in one case a man claiming benefit in his own name and two other hi-jacked identities was estimated to have defrauded at least £50,000. A raid on his home later revealed evidence that the individual had 20 separate identities. The individual was later sentenced to 15 months' imprisonment.

a) Proposals

(i) Establishing links to credit reference agencies for checking passport and driving licence applications.

(ii) Assessing the liability of third parties who are able to pay for fraud losses.

(iii) Developing a database of known fraud and fraudsters.

(iv) Setting up a central register of stolen identities and documentation.

(v) Issuing more secure driving licences and passports to be recorded on an identity database shared between the passport and the driving licence agencies.

(vi) Checking applications for services against a number of databases used by the credit reference agencies or similar.

b) Points to consider

Example 9

The Home Office reported in its consultation paper on identity fraud and entitlement cards published in 2002 that in 2000/2001:

- 3,231 driving tests were terminated due to concern as to the identity of the candidate;
- 1,484 fraudulent passport applications were detected;
- 50 cases of fraudulent documentation were detected at Terminal 3, Heathrow Airport per month;
- 564 cases involving identity fraud were identified by the Benefits Agency.

Example 10

On 12 May 2003 it was reported that an asylum seeker was sentenced to one year imprisonment after which he would be deported. He had subsequently admitted using three false names to avoid deportation.

Example 11

In Ireland the Garda Immigration team is demanding that compulsory finger printing of all non-nationals living in Ireland is introduced. Last year 22,600 Irish passports were issued to citizens who reported their passport lost or stolen. The Garda believes that most are in fact illegally traded. Passports may be used by drug smugglers in order to disguise the frequency of their travel abroad from the authorities.

Example 12

All 19 of the terrorists responsible for 9/11 had Social Security numbers, most of which were stolen. This enabled the terrorists to open bank accounts, transfer money without detection and obtain driving licences without their true identity or presence in the US being detected.

As this illustrates, identity fraud is one method which enables to terrorists to fund their activities and to move that cash around whilst avoiding detection by the authorities.

Example 13

It was reported in April 2003 that a former British civil servant applied for a passport using a dead baby's name and birth certificate. The photograph of the ex-civil servant was recognised by a passport official. A request for further proof of identification was ignored and the address used was found to belong to someone else. The civil servant has since been sentenced to a term of imprisonment.

(i) These proposals may assist to increase detection rates and may also help to prevent identity fraud. However, it is necessary to balance any steps taken to control fraud and prevent crime with the individual's right to privacy.

(ii) A database of information on names and addresses known to be used for identity fraud should not be an infringement of Human Rights or the Data Protection Act 1998. The victims of identity theft are unlikely to object to the inclusion of their identity if that means extra care is taken before issuing a loan or credit card in their name.

(iii) It would be necessary to ensure that those victims were not further distressed by inclusion upon a list which may mean that they find it hard to obtain normal credit or a mortgage.

(iv) A flagging system may be of assistance such as those operated by credit reference agencies such as Experian and Equifax. The credit reference agencies flag the files of individuals who are known to have become the victims of identity fraud.

4.3 Data-Sharing – The Business Sector

Many of the benefits of data-sharing in terms of fraud prevention and detection in the public sector apply equally to the private sector.

a) Proposals

(i) Companies should consider creating a database of frauds which they suspect or know have been carried out against it. In addition, companies should consider sharing this data with other companies, in the same sector for example. An analysis of data relating to known past frauds can produce hard data that can be used to combat future fraud.

(ii) Companies should consider developing databases of known fraudsters, containing the addresses and names which are known to be used for identity fraud. The information could be collated on a database and circulated to both the public and private sector and insofar as the information relates to people who do not exist, there would be no data protection implications. This may also assist in identifying the characteristics of likely offenders.

(iii) Clear reporting procedures when a fraud is carried out against a business can assist in the preparation of a database.

(iv) Companies should consider creating a database identifying the various indicators of identity fraud (e.g. unusual calling activity, differing address details) which can be matched to a specific method of fraud operation. A fraud indicator is in effect a clue and linking the clues together can assist in early detection. Quantification of reoccurring indicators can be used to score and report fraud.

(v) Data-sharing with the public sector to access a central register of stolen identities and documentation – and selected biographical data relating to criminals held by the government.

(vi) A scheme to check applications for services against a number of databases used by credit reference agencies or similar organisations.

b) Points to consider

(i) The benefits of data-sharing in fraud prevention must be balanced with the risks and costs involved. Accusing the wrong person when inaccurate data is shared is a potential problem. This risk is exacerbated by the lack of a single identifier since data may be shared on the basis of a name, address or date of birth.

(ii) There will be the financial costs to consider of investing in technology to maximise the benefits of data-sharing. Any system would have to provide for security and accountability. A lapse in security would be likely to give rise to significant concerns of the threat to privacy.

(iii) For data-sharing to work effectively in the private sector individuals must be informed and accept the use to which their data will be put and the purposes for

which it will be shared. Companies must be careful to operate within the legal framework established by the Data Protection Act. Safeguards would have to be put in place in relation to the service providers as well as the data subjects. The individual's right to access information and to check the accuracy of information must be upheld.

(iv) Companies should ensure that retailers and customers are asked to consent to the storage of private information and ensure they obtain consent to keep the personal data on a separate database for security purposes. Companies should be clear that any information is required purely for security purposes and not for secondary marketing purposes. Equally companies must ensure that this is all the security information is used for.

(v) The assumption that data-sharing inevitably leads to the erosion of privacy could in future be contradicted by the development of privacy enhancing technology which may allow for an actual reduction in the amount of information needed, for example, electronic pseudonyms and smart cards.

(vi) It may prove to be the case that individuals are prepared to trade reduced privacy in favour of fraud prevention particularly in light of the increasing levels of fraud and the resulting cost to the economy.

(vii) Any decision to carry out data monitoring in terms of potential fraudulent activity by a company's employees must also take account of the provisions of the Regulation of Investigatory Powers Act.

5. Prevention & Detection

5.1 Prevention & Detection – Business Sector

It is an unfortunate fact that much serious fraud emanates from those a company expects to trust above all others – its own employees and management. Identity theft and credit card fraud may be assisted by insiders. For example in the retail industry certain cashiers may be part of an organised crime gang. Their role is to allow their criminal colleagues to use fraudulently obtained credit cards or cheque books to purchase high value goods without question.

This section will summarise some of the technological and organisational steps which may be implemented by companies and businesses in order to assist in the prevention and detection of identity theft.

Companies need to introduce methods of preventing and detecting identity fraud. There is some overlap in this area with the proposals relating to the sharing of data. Internal procedures are also a method by which a company may seek to avoid becoming a victim of fraud.

Example 14

It was reported in May 2003 that an employee of one well-known high street bank who had previously been described as an exemplary member of staff had carried out a £250,000 fraud over the period of a year. The Assistant Manager has reportedly been convicted of conspiracy to defraud having allegedly created fake customers for whom she had then obtained loans and overdrafts.

a) Proposals

(i) Organisational Steps

Companies should:

- Vet employees with access to personal information, including all temporary and part-time employees.
- The DPA requires that a record should be kept of all employees with access to personal information – ensure that your company does so.
- Keep hard copies of personnel information in locked files.
- Where possible operate a policy of job rotation increasing the chance that fraud is uncovered.
- Shred confidential paperwork that is no longer required.
- Develop and enforce procedures for transmitting personal information.
- Adopt a written protection policy and publish it in the company's literature and even on their website.
- Implement clear reporting procedures when fraud is carried out against a customer or the business or company concerned.
- Greater checks against the identity evidence provided by customers in compliance with money laundering obligations. Cross-referencing should be encouraged.
- Educate and train employees to know the signs of identity theft.
- Carry out credit reference checks of customers.
- Demand originals of identity documentation. Check for signs of tampering.
- Only accept UK photo ID and only from official sources. Never accept a hand-written passport.
- Check any unusual type of identity documents with in-house lawyers or the Law Society.
- Consider joining CIFAS and similar organisations.
- Check the statistics and fraud surveys in order to assist in the recognition of new types and methods of identity fraud.
- Consider the use of civil proceedings to recover losses as well as reporting the fraudulent activity to the police or other relevant authority.

- Implement a system of fraud and risk management audits of your departments. Risk analysis may assist to highlight deficiencies in current procedures.
- Report the occurrence of identity fraud. Ignoring it will not make it go away.

(ii) Technological Steps

- Encourage speedier implementation of microchip technology and other similar methods of fraud prevention.
- Develop an encryption system for computer-based information and evaluate its effectiveness regularly.
- Change passwords regularly.
- Ensure access is prevented as soon as a member of staff leaves or is transferred.
- Greater responsibility and care should be taken to ensure information security and assurance.
- Consider monitoring employees for fraud.
- Employers should consider multi-level security, including biometric finger printing employees, and implementing similar security procedures of this nature to ensure that employees are only permitted access to an appropriate level according to their role or seniority. Access levels should be reviewed on a frequent basis.

b) Points to consider

(i) Organisational Policy

Details of all employees with access to personal data should be kept on record. This is in any case a good policy as it may assist a company to establish patterns and cross-reference the incidents of identity fraud with a particular employee. It may be that the employee is involved in a fraud. Alternatively it may mean that an employee is not doing his or her job properly – for example not complying with rules as to forms of identity required.

Maintaining hard copy evidence of personnel details is good practice and reduces the possibility of a dishonest employee amending details.

Job rotation can be an effective method of uncovering fraudulent activity. Some companies insist on employees taking at least one annual holiday of at least two weeks duration precisely so that there is an opportunity for any such activity to come to light.

Implementing reporting procedures, a strict protection policy and ensuring that compliance with those policies is adhered to may highlight the identity of dishonest employees. Cross-referencing this information may also assist a company to recognise patterns of conduct on behalf of customers or employees which result in fraud. As such this may allow companies to react with further procedures aimed at defeating that type of conduct.

It is vital that companies implement a system of risk and security audits. This may highlight weaknesses in your company's procedures and allow you to take appropriate steps to prevent the company becoming a victim of identity theft.

(ii) Technological Policy

Encryption can be an effective means of protecting personal data which is due to be sent from one source to another. It may also help to prevent hackers from obtaining access to personal information which they may steal in order to sell to identity fraudsters. This would need to be teamed with an increased focus on information security policy and IT security software.

Data mining software is another technological step which can assist in the early detection of identity and other forms of fraud. However legal advice should be taken before using data mining software in order to ensure compliance with the DPA and Regulation of Investigatory Powers Act 2001.

5.2 General Public

In this section we will deal with the steps individuals ought to take in order to reduced the chance that they will become a victim of identity theft and to recognise the signs when their identity is already being used for fraudulent purposes.

Example 15

One London investment banker reportedly became a victim of identity thieves. One of the thieves stole £100,000 from his bank account by collating personal information and convincing the victim's High Street bank to send out to him a cheque book and credit card in the victim's name.

a) Proposals

- Treat personal and financial information as an asset. Would you throw away cash or your cheque book? Financial information is just as valuable to an identity fraudster – if not more so.
- Individuals should be taking more steps to ensure they are aware of identity theft, credit card fraud and new trends in both forms of crime.
- Care should be taken when disposing of personal documentation – individuals should also consider investing in a shredder or at least ensuring that details are not legible.
- Care should be taken when giving out financial information and personal details. Are you sure that the person asking for your password or security number is from the bank? Ask for a telephone number to call back and check.
- Individuals should make a note of their billing cycles to increase the chance that they notice when a bill goes missing or is overdue.
- Avoid signing up for junk mail. Junk mail sent to a previous address may be utilised by an identity fraudster.

- Ensure that you advise banks and the mail to divert post to your new address at the earliest possible opportunity in the event that you do move house.
- Review monthly accounts, credit card statements and utility bills for unauthorised charges.
- Take care when disposing of ATM receipts. In particular, do not put them in the receptacle provided at the cash machine.
- Do not carry your National Insurance Card in your wallet. If your wallet is stolen this is a potential gold mine for identity fraudsters who may then use it to carry out benefit fraud in your name. Do not carry bank passbooks or plastic cards unless you need them.
- If you are concerned you may have become a victim of identity theft but are not certain, contact the major credit reference agencies and ask for your file. You are entitled to receive this under the DPA subject to payment of a reasonable sum for administration expenses.
- In more extensive cases thought should be given to civil recovery as well as police investigation.
- Do report the occurrence of identity fraud. Ignoring it will not make it go away.

b) Points to consider

It is not difficult to shred personal documents or take them to work and shred them there. Bin raiding is one method employed by identity fraudsters in order to build up the financial picture of their victim.

Experian, one of the two leading Credit Reference Agencies used by the Financial Services in the UK carried out a survey last year into identity theft. Experian contacted those responsible for refuse collection at urban local authorities. Out of the 71 local authorities, 53 said that bin raiding occurred in their area.

It was also reported last year that an analysis of 400 domestic bins in Nottingham showed that one in five contained a full card number and expiry date, enough data for a transaction to take place without a credit card holder being present.[7]

5.3 Protection of Whistleblowers

In this section we look at the protection which a company must offer to workers who report fraud and the mechanisms which should be implemented in order to ensure employees are able to make necessary reports.

In April 2003 Public Concern at Work reported that more than £10 million a year were paid in damages in the UK to whistleblowers.

a) Proposals

- All organisations should establish a culture of fraud awareness.

[7] FT.com 9/3/02 by Isabel Berwick

- Employees should be trained to recognise the signs.
- A firm policy of how to respond to fraud should be implemented.
- Employees should be made aware that they will be fully supported by the company in the event that they do blow the whistle on fraud.
- Provision should be made for employees to make internal anonymous reports.
- If a junior employee discovers a fraud then there should also be provision for that person to report to the directors.
- Companies should provide and make staff aware that there are also external bodies to which reports can be made or advice can be obtained.
- Companies should ensure that they make staff aware they can make reports to the relevant industry regulator.

b) Points to consider

(i) Employees

It should be made possible for the employee to report to management in different departments or management with no direct responsibility for that employee, given that the employee may fear that their direct manager is somehow implicated in an identity fraud.

In light of the recent survey by Ernst & Young, which indicated that 85% of the worst frauds in 2002 were carried out by insiders on companies' payrolls, with more than 50% in management positions, company directors must be vigilant.[8] The cost to companies is illustrated by figures recently released by KPMG showing the average value of "management" fraud cases was about £2 million, and for employee fraud, £500,000, double the 2001 figures.[9]

It should be made clear to employees that all reports will be treated as confidential. Where such reports are made in good faith, the employee would normally be protected under the Public Interest Disclosure Act 1998 (PIDA).

The employee is protected by PIDA if he makes a qualifying disclosure of information which he reasonably believes (and the employee can show that he reasonably believes) tends to show that one of the following offences or breaches have, are being or will be committed, irrespective of whether the employee is later shown to have been incorrect:

- A criminal offence;
- A breach of a legal obligation;
- A danger to the health and safety of any person;
- Environmental damage;

[8] "Fraud: The Unmanaged Risk – 8th Global Survey" Ernst & Young January 2003
[9] "Total value of fraud cases trebles in a year, says KPMG Forensic" KPMG Fraud Barometer 3 February 2003

- Intentional concealing of information which demonstrates that any of the above have occurred.

The disclosure is protected if the employee makes the qualifying disclosure to his employer either by company procedures authorised by the employer or directly to the employer or by making the disclosure to another person whom the worker reasonably believes to be solely or mainly responsible for the relevant failure.

If the employee wishes to make the disclosure to a prescribed body or person then he is protected if:

- he makes the qualifying disclosure in good faith;
- he reasonably believes that any allegation or information is substantially true; and
- he reasonably believes that the matter falls within the remit of the prescribed person or body.

For example if the information relates to a fraud the employee might reasonably think the Serious Fraud Office would be the correct body.

Where a company does not have the resources to set up a whistle-blowing mechanism internally, it is possible to outsource this service.

(ii) Directors

Directors' Duties to the Company

Directors have a duty to exercise their powers with a degree of skill and care. Directors should therefore take positive steps to familiarise themselves with the company's affairs. If they fail to do so they are potentially liable to the company.

If a director fails to act upon discovering a fraud he is not acting in the best interests of the company. It may be the case that the director has acted negligently. The above breaches of duty may both result in the director becoming liable for any further losses caused by his failure to act.

In one recent case it was held that a senior employee may owe a duty of care to report a fraud being perpetrated by directors in a company.[10]

(iii) Disqualification of Directors

Failing to report fraud can have serious consequences for directors of companies. In the event that a company becomes insolvent as a result of a director's failure to report a fraud of which he was aware, he may be subject of disqualification proceedings by the DTI. Those proceedings may well be based upon the director's misfeasance. It may be considered that a director has breached his duty of care and due diligence owed to the company by failing to report fraudulent activity.

[10] RBG Resources PLC -v- Rastogi [2002] EWHC 2782 (Ch)

Proceedings can be brought by the DTI in order to disqualify directors whether or not a company is insolvent. If successful the court may disqualify the person from being a director of a company for a specified period of time.

In relation to solvent companies a director can be disqualified, amongst other things, on conviction of an offence. An offence could be committed by failing to report suspicious transactions to the authorities. Other examples of cases include:

a) where there has been a failure to act on discovery of fraud or failing to report suspicious circumstances;

b) where trade creditors have been paid ahead of the Income Tax Authorities;

c) where the director did what he was told and did not exercise independent judgement, even though he had the benefit of professional advice;

d) where there is no effective control over a fraudulent employee.

In relation to insolvent companies, directors can be disqualified if the court accepts the person is unfit to be a director. There are a number of factors the court will take into consideration, the most relevant of which is any breach of a director's fiduciary or other duty. A failure to act on discovering fraud could amount to such a breach.

c) Scale of the Business and of the Fraud

It is necessary to maintain a procedure for dealing with any report of identity fraud. The procedure to be implemented will vary depending on the size of the business and the scale and seriousness of the identity fraud being investigated.

A firm may wish to appoint one person as responsible for investigating the identity fraud. They will in turn be responsible for researching the best methods of investigating a specific type of identity fraud.

This individual may also be given responsibility for assessing the in-house skills available for investigating identity fraud. For example whether the firm has anyone with the computer science skills to enable electronic evidence to be detected and preserved. It will also be necessary for that person to establish contacts with specialist lawyers and investigators.

6. Asset Recovery

Despite the development of increasingly sophisticated security measures and legislation designed to combat fraud, the statistics show that fraud is on the increase. This is due in part at least to the criminals' conception that "they can get away with it"[11] because of the accepted inability of the prosecuting authorities to produce an effective deterrent solution.

[11] "There is a perception that nothing will be done about fraud which is very dangerous. It encourages people to think they can get away with it" – SFO – April 2002

Following the attack on 9/11 and the financial scandals including Worldcom and Enron, the US Authorities had to grapple with the same problem, albeit related to different crimes. They responded by passing legislation[12] the purpose of which was to prevent the criminals either from using funds to commit their crimes or benefiting financially from their crimes.

In the case of identity fraud, it is invariably the criminals' sole purpose to steal and keep the proceeds of their crime. For this, they are quite willing to run what invariably is only a small risk of detection, prosecution and, even less likely, a relatively limited custodial sentence.

A possible solution, therefore, is to take effective steps to deprive the criminal of those proceeds which has the added advantage of loss recovery. Perhaps, equally importantly, corporate governance principles dictate that to avoid personal liability, Board Members should at the very least consider the viability of loss recovery. As Bob Ainsworth, a Home Office Minister said "…We can't just go after the criminals themselves, we've got to try to dismantle the gang. An important part is taking away their ability to commit further crime with the wealth they have acquired".[13]

6.1 Speed, Surprise and Strategy

If an organisation does intend to recover losses caused by identity fraud it must bear in mind the following:

- Speed
- Surprise
- Strategy

Money is transferable by one e-mail, telephone call or fax. It is therefore vital that not only is any investigation/analysis conducted in utmost secrecy but action is taken before the fraudster has an inkling that he is being investigated.

At the very earliest opportunity, an analysis should be carried out to assess:

a) whether there has been any fraud;

b) the extent of the fraud;

c) whether it is viable to try and recover the losses sustained.

To do this it may be necessary to examine Computer Server logs and individuals' computers. Before doing so it will be necessary to instruct computer experts and professional investigators in order to ensure that vital evidence needed for civil recovery or criminal action is not destroyed.

[12] (a) Executive Order 13224. (b) International Money Laundering Abatement and Anti-Terrorist Financing Act 2001 (c) Sarbanes-Oxley Act

[13] BBC 06.02.03 "Asset agency visits crime auction" Report

Companies should bear in mind that the motivation behind identity theft is financial. If a company adopts a policy of pursuing the assets of identity fraudsters they may find that in doing so this acts as a deterrent.

6.2 Third Party Disclosure as to Assets and Whereabouts

The English Courts provide invaluable assistance to a victim in that in certain circumstances they grant Orders which enable the victim, without notice to the fraudster, to discover:

a) the extent of the fraud;

b) who is responsible;

c) who was involved in the commission of the fraud and therefore could be liable as well.

The Court would, for example, grant Orders against third parties who have been unwittingly involved in the fraud, whether such fraud has been committed electronically or in the physical world. For instance, the court will require disclosure of relevant information by an Internet Service Provider or a Bank through whom, for instance, money stolen from the victim has passed.

Such Orders for disclosure can be combined with what is called a "gagging" Order which prevents the party giving disclosure from notifying the fraudster. Breach of such an Order will amount to a contempt of Court which is punishable by prison.

Once the extent of the fraud has been assessed, decisions need to be taken as to whether it is commercially sensible (and whether there is an obligation) to pursue the fraudster and if so, to what extent. No victim, however large or small, should fail to assess the significance of publicity, given the fact that it has been the victim of fraud which is often caused by inadequate security measures or lack of judgement.

6.3 Get Your Money Back/Stop The Crime

a) Search and Freezing Orders

Once a Claimant has decided to pursue the fraudster, it may be possible to obtain freezing and search Orders to assist in preventing assets from being transferred and to prevent vital evidence from being destroyed by the fraudster.

Both search and freezing Orders are applied for without notice. The applicant for a freezing Order must have a good arguable case and there must be a real risk that any subsequent judgment may go unsatisfied. The effect of such an Order is to freeze the fraudster's assets and will bind any third party in the jurisdiction, such as a bank, given notice that such an Order has been made. It is therefore important to identify as many assets as possible before serving the freezing Order so that banks and other third parties can be notified of its existence before the fraudster has an opportunity to direct them to transfer his assets elsewhere.

The basis upon which a search Order is granted is slightly different. There must be a real risk that evidence will be tampered with or destroyed and they are, therefore, normally obtained and served in matters of urgency. Search Orders are normally executed at premises in England but Orders can be made for service elsewhere. The defendant does not need to be present as they can be served on the person having control of them at the time.

The claimant's search team is likely to include any enquiry agents instructed in the search for assets, and data recovery experts who will search the defendant's computer and its storage systems. The defendant is under an obligation to supply any passwords necessary to access his computer. If he fails to do so, an application can be made to the court whilst the search is being carried out for an order to remove the computer system in its entirety.

7. Collaboration with Government Agencies and Professional Advisory Bodies

Organisations should consider collaborating with governmental and professional advisory organisations to report how they manage information security and fraud threats and work with suppliers and users to co-ordinate information on incidents. This will assist businesses in plugging the knowledge and information gaps, assessing where risk management procedures are lacking and where a business's vulnerabilities lie.

In connection with this, organisations may find it of great assistance to collaborate with government and industry advisory bodies to produce educational materials on the nature of identity fraud, why it has posed a problem for their particular business and how they have obtained information and guidance on the subject.

The aim is to eventually raise general awareness among industry, accountancy and the legal professions of the law relating to identity fraud and its effective prevention.

8. Compliance

No procedure or control is effective unless properly implemented throughout an organisation. Regular checks must be undertaken in order to ensure that all necessary controls are being adequately implemented by employees at all levels, short cuts are not used in such a way as to dilute the controls' effectiveness and that controls remain effective in the light of changes in the law or in the development of the organisation's business.

With thanks to Steven Philippsohn, Head of the Fraud Advisory Panel Cybercrime Working Group and the Fraud Litigation Team at Philippsohn Crawfords Berwald together with Riten Gohil, Jack Wraith, Ron Warmington, Tony Neate, Alice Rigby, David Lennox, John MacGowan and Peter Yapp.

Useful Links

Fraud Advisory Panel
Tel No: 020 7920 8721
www.fraudadvisorypanel.org

Serious Fraud Office
Tel No: 020 7239 7272
www.sfo.gov.uk

City of London Police Fraud Squad
Tel No: 020 7601 2222
www.cityoflondon.police.uk/level1/crime/fraud_main.html

Metropolitan Police Fraud Squad
(for high value fraud over £750,000)
Tel No: 020 7230 1212
www.met.police.uk/so/so6.htm

National Criminal Intelligence Service (NCIS)
Tel No: 020 7238 8431
www.ncis.co.uk

Financial Services Authority
Tel No: 020 7676 1000
www.fsa.gov.uk

Confederation of British Industry
Tel No: 020 7395 8195
www.cbi.org.uk

Small Business Service
Tel No: 0114 259 7788
www.businesslink.org

Inland Revenue
www.inlandrevenue.gov.uk

HM Customs & Excise
www.hmce.gov.uk

Trading Standards
www.tradingstandards.gov.uk

Companies House
Tel No: 0870 333 3636
www.companieshouse.co.uk

National Audit Office
Tel No: 020 7798 7000
www.nao.gov.uk

Institute of Chartered Accountants in England & Wales
Tel No: 020 7920 8100
www.icaew.co.uk

Law Society
Tel No: 020 7242 1222
www.lawsociety.org.uk

Home Office
Tel No: 020 7273 4000
www.homeoffice.gov.uk

Public Concern at Work
Tel No: 020 7404 6609
www.pcaw.demon.co.uk

Crimestoppers
Tel No: 0800 555 111
www.crimestoppers-uk.org

Health & Safety Executive
www.hse.gov.uk

UK Online for Business
www.onlineforbusiness.gov.uk

Data Protection Commissioner
www.dataprotection.gov.uk

Department of Trade & Industry
Tel No: 020 7215 5000

Information Security Group Policy
Tel No: 020 7215 1962
www.dti.gov.uk

National Hi-Tech Crime Unit
PO Box 10101
E14 9NF
Tel No: 0870 2410549
www.nhtcu.org

Equifax
www.equifax.com

CIFAS – The UK's Fraud Prevention Service
www.cifas.org.uk

Association for Payment Clearing Services
www.apacs.org.uk

Experian
Tel: (44) 115 941 0888
Fax: (44) 115 934 4905
www.experian.com

The Fraud Advisory Panel
Chartered Accountants' Hall PO Box 433 Moorgate Place London EC2P 2BJ www.fraudadvisorypanel.org

OTHPLN2214 07/03