

FRAUD AND FRAUDSTERS

Frauds are as varied as human ingenuity and imagination. Schemes by which to defraud are constantly being thought up and practised by the professional fraudster. The measure of their success is dependent upon the extent of their victim's gullibility. Their essential weapons are a combination of confidence, false representations, pretences, deceits and omissions, all of which they use to exploit the greed, compassion, sympathy and trust of their victims.

The successful fraudster must have considerable powers of imagination, know how to lie well, have the ability to seize any opportunity that arises and, above all, must be able to inspire confidence.

Many criminologists believe that fraudsters have no superior intelligence but are endowed with a certain facility for trickery, deceit, cunning and hypocrisy. They depend on speed of thought, tongue and action to assist them in their misdeeds. The most successful frauds are not perpetrated by strangers but by persons well known and trusted by the victim.

WHY DO PEOPLE COMMIT FRAUD?

People will generally commit fraud for one two key reasons: (a) Need – a hidden financial need, often fuelled by an addiction (gambling, drugs etc) or lavish lifestyle, or (b) Greed - the perpetrator has a defective set of values believing, for example, that he has a 'right' to more than he is properly entitled to. Opportunity, and a belief that the fraud will be undetected, at least in the short term, will frequently tip otherwise lawful people to commit fraud.

HOW DO FRAUDSTERS SUCCEED, IN THE SHORT TERM?

A Fraudster will usually be: a) Plausible: they will have a rational excuse for their actions, b) Likable: 'it couldn't be him', 'he wouldn't do such a thing', c) Confident: a lot of trust is given to them based on their ability to get things done d) In control: they are very slow to share responsibilities, and e) Ever present: they seldom take leave and usually never take sick leave (fearful that others will discover their fraud).

PREVENTING FRAUD WITHIN ORGANISATIONS

Awareness that fraud can happen is a significant first step in preventing fraud. Like any other business risk, it requires a plan to identify risk areas and for controls to be put in place to address these risks. There are three broad areas of risk which need to be addressed:

- Staff/Personnel
- Structural/Physical
- Operational/Financial

Staff/Personnel

Many frauds are committed by persons employed within the organisation. Often the fraud is discovered only when the fraudster is called away unexpectedly.

The initial opportunity to reduce the risk of fraud being committed by employees is at the recruitment stage. There are simple steps that can be taken to at the recruitment stage to reduce the risk of fraud by future employees.

Structural/Physical

The structure of the organisation may lead to an increased risk of fraud. For example, if an organisation has a number of warehouses or remote locations away from central management this may increase the risk of fraud as often these locations are given greater autonomy to enable them to operate effectively.

In particular, physical access controls play an important role in fraud prevention. Restricting access to cash, goods, stores, computers, documents and the premises are a critical element in reducing the risk of fraud. For example, physical access may be controlled by means of swipe cards. The existence of good security controls is very important as a deterrent to crime.

Operational/Financial Risks

Some organisations are more susceptible to fraud than others. Cash based businesses, for example, generally carry a higher risk of misappropriation or fraud.

A robust and comprehensive system of controls over the accounting and financial transactions of an organisation is an essential element in fraud prevention. Controls provide the framework within which the organisation operates as well as protection against abuse. For example, if an organisation deals in stock which is widely marketable, control measures should be put in place to ensure that both the physical stock, and the corresponding accounting records relating to them, are protected. Ideally, avoid having one person responsible for both the management of physical stock and for updating the stock records.

TYPES OF FRAUD-RELATED CRIME

The expression 'fraud' is used as a collective name for a number of statutory and common law offences, there being no specific offence of 'fraud', though there is a common law offence of conspiracy to defraud.

For investigation purposes, fraud is a very relevant term, constantly in use, and very descriptive of the specific activities whereby an advantage is gained by unfair means - the advantage usually being of a pecuniary nature and obtained by deceitful means.

Frauds are as varied as human ingenuity and imagination. Schemes by which to defraud are constantly being thought up and practised by the professional fraudster. The measure of their success is dependent upon the extent of their victim's gullibility. Their essential weapons are a combination of confidence, false representations, pretences, deceptions and omissions, all of which they use to exploit the greed, compassion, sympathy and trust of their victims.

The successful fraudster must have considerable powers of imagination, know how to lie well, have the ability to seize any opportunity that arises and, above all, must be able to inspire confidence.

Many criminologists believe that fraudsters have no superior intelligence but are endowed with a certain facility for trickery, deceit, cunning and hypocrisy. They depend on speed of thought, tongue and action to assist them in their misdeeds. The most successful frauds are not perpetrated by strangers but by persons well known and trusted by the victim.

Those investigating fraud-related crime must first establish that there has been a breach of the law. It frequently happens in fraud cases that there is no difficulty in identifying the culprit. The most common breaches of the law encountered in the investigation of fraud are:

- Theft
- Handling/Possession of stolen property
- Forgery
- Deception
- Possession of certain articles for use in the commission of offences
- False Accounting
- Money Laundering
- Counterfeiting
- Breaches of the Companies Acts
- Breaches of the Competition Acts

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

GARDA INVESTIGATION OF FRAUD

On initial complaint, the Garda investigator will obtain an overview of the account of the alleged crime being given by the complainant. In some cases this will require that enquiries are conducted by the Gardaí to facilitate a proper assessment of the complaint being made. At the Garda Bureau of Fraud Investigation (GBFI), a dedicated Assessment Section is in place for this purpose.

The key issues to determine are whether there has been a breach of criminal law and whether sufficient evidence exists to establish this breach against a particular individual. The more serious cases are referred to the GBFI for investigation.

It is a function of the Detective Chief Superintendent attached to the GBFI to decide on the venue for investigation in any given case. This may involve the case being investigated exclusively within the Bureau or alternatively, it may be referred for local investigation with assistance from GBFI personnel. The criteria which will determine the venue for investigation include the complexity of the complaint made, the value of money or other property defrauded, the geographical spread of the criminal offences alleged and whether extensive international enquiries are necessary.

STATEMENT OF COMPLAINT FROM INJURED PARTIES

At the outset of an investigation, a Garda will take a detailed statement, with backup documentation, from a fraud victim. Action will not be taken against a suspect until such a statement is available.

However, regard will also be had at the initial stage of the investigation to any urgent action which may be necessary, for example, where it is suspected that evidence will be destroyed or that the offender will abscond. All available evidence should be secured at the earliest possible opportunity. This includes evidence from computers, phones, bank statements or financial records which will now most frequently be maintained in electronic format. Where urgent action of this nature is contemplated, confirmation at least of the general nature of the complaint should be put in writing and signed by an appropriate person on behalf of the injured party or organisation.

Normally, it will be a matter for the financial controller within an organisation to identify what monies have been stolen by conducting an internal investigation and audit. In smaller organisations, an accountant or auditor should be in a position to conduct these enquiries. It is not a matter for Garda investigators to conduct an internal audit of an organisation to determine if and how a fraud has occurred.

As a matter of best practice, an organisation will usually have clearly defined roles and responsibilities for all staff employed and have appropriate control measures in place to ensure that all monies, stock and other property is properly accounted for. Elements of internal control include the following:

- Segregation of duties
- Structure of organisation
- Authorisation and approval
- Physical security
- Supervision
- Arithmetical and accounting procedures

STANDARD OF PROOF IN CRIMINAL CASES

The standard of proof in criminal cases is 'beyond a reasonable doubt' and this standard applies to all aspects of the evidence presented by the prosecution. It is critical that the complainant can establish precisely what has been stolen and can produce the evidence trail to support the allegations. If control procedures are weak within an organisation, it may not be possible to establish what monies were defrauded and by whom. Weak control procedures may create serious impediments in proving the alleged offences. Where it is considered that such weaknesses exist, Gardaí will submit a preliminary file to obtain the directions of the DPP and will be obliged to outline the nature of the weaknesses identified.

When a particular aspect of a fraud is being included in a statement, it will be found helpful to cover:

- When?
- Where?
- Who was present?
- What occurred?

This will help to keep matters in proper sequence by pinpointing locations, obtaining names of witnesses so as to verify the account given, together with details of the incident.

It is important to note that the Garda investigator will ultimately have to establish a breach of the law not just to the investigator's satisfaction but to the satisfaction of the courts. Therefore, evidence of the essential ingredients of the crime must be obtained and included in the statements taken.

Most fraud cases concern the movement of monies in bank accounts which are the subject of the crime under investigation. In these cases, it is not sufficient to show that a particular cheque has been drawn. Evidence must be obtained to prove the actual movement of the funds where one account was debited and another account was credited to the benefit of the accused person. This proof will often require the obtaining of orders from the Courts to permit the examination of the relevant accounts. Banks will not release this information to investigating Gardaí without such an order as to do so would breach their duty of confidentiality to their customers.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

EVIDENCE

PROTECTING DOCUMENTARY EVIDENCE

In recent years great advances have been made in the field of forensic science and it is now possible to glean valuable evidence from an expert forensic examination of documents and records. Forensic tests include finger print analysis, identification of handwriting, comparison of inks, identifying alterations and indentations, and forensic examination of documents and records from computer file back-ups.

Original documents will be required whenever possible. Documents should be preserved in the same state that they were found. No pencil or other marks should be made to the original document. Avoid unnecessary handling. Write up a label noting where they were found, by whom and to whom they were passed. Place each document in a clear plastic envelope. To avoid damaging the evidence, put the label on the plastic envelope only after the details have been written on the label. This will facilitate the subsequent examination of the document without the possibility of compromising the integrity of the exhibit.

Everything, no matter how insignificant it may appear, should be documented.

Details can be crucial – you can never take too many notes but you can often take too few.

The safe custody of documents and exhibits is vital – it must be proved that no unauthorised persons gained access to them and that no alteration was made to them by any unauthorised source.

HANDLING OF DOCUMENTS AND EXHIBITS

Documents are frequently critical in supporting the evidence of a witness and should be carefully preserved for use in Court if required.

PROVING DOCUMENTS IN EVIDENCE

Before a document is accepted in evidence, the following must be proven:

- The source of the document
- All entries in the document – best evidence rule
- The history of the document
- Location of the original – if not available, the witness must give evidence to the

effect that after a comprehensive search the original cannot be found and is believed to be irretrievably lost

- If the document was stored in non-legible form, that it has been reproduced in permanent legible form and that this reproduction was effected in the course of the normal operation of a specified computer or other system
- Where appropriate, state that the person who supplied the information cannot reasonably be expected to have any recollection of the matters dealt with – having regard to the time elapsed or other specified circumstances
- If the date is not shown on document, state date, or if not known, approximate date on which it was compiled
- Any other matter which is relevant to the admissibility of the information

© 2009 An Garda Síochána/PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

ADVANCE FEE FRAUD

WHAT IS IT?

The criminal offers the victim a 'windfall' in return for some small advance payment to 'hook' the victim. Examples are bogus lottery schemes or requests for assistance to transfer huge sums from dormant accounts.

Good investment returns will always attract attention. But is the underlying transaction legitimate? In recent years there has been a widespread increase in advance fee type frauds. The lure of substantial investment returns is used by the fraudster to extract advance fees to arrange the investment. The advance fee and any funds subsequently invested will not be seen again.

In other cases, the promise of access to funds is used as the 'hook' to extract an advance fee for a service that is never provided.

WEST AFRICAN E-MAILS

The most frequently encountered advance fee fraud in recent years relates to the receipt of letters emanating from West Africa. The writer usually purports to represent an important government official or other official agency and tells you that they have a large amount of money available which they wish to transfer out of West Africa.

The letter will indicate that the West African money accumulated as a result of over-invoiced contracts, the purchase of property, the sale of crude oil etc. and that due to restrictions in West Africa, the money is not at the disposal of the 'owners'. They ask for your bank details and copy invoices so that the money can be transferred to your account. In return you are promised a percentage. Numerous official looking documents are used to support their claim.

A small fee is first requested from the victim in payment for various taxes, legal fees, transaction fees or bribes in order that the funds can be released. The fee is designed to "hook" the unsuspecting investor and once 'caught' further payments will be demanded from the victim who feels compelled to continue in the vain hope of recovering the money he has already lost. Of course, no money is ever received by the victim. In addition, as they have all the details, the fraudsters may go further and plunder the victim's bank account.

More recently, this type of fraud has evolved into variations involving investments (See Investment Fraud), sometimes arising from 'cold calls'.

WHO DOES THIS MOST AFFECT?

Individuals are probably most at risk but organisations, too, can be vulnerable especially if they are strapped for cash. In extreme cases, victims can be sucked in to making additional payments or even take up invitations to travel abroad to meet fake government officials, sometimes at grave personal risk.

HOW MUCH CAN BE LOST?

In extreme cases, victims have suffered substantial losses up to and including their life savings.

WHAT SHOULD I LOOK FOR?

Advance fee type frauds are varied and are only limited by the imagination of the fraudster. They involve sophisticated deception and appeal strongly to the profit motive. They contain an element of secrecy so that the victim will not carry out checks or obtain professional advice before handing over the money. It is surprising how easily people, including experienced business people, are duped into believing transparently dishonest scams, simply by appealing to greed. A telltale sign is abnormally high returns in a short period. Another warning sign can be poorly worded letters and documentation.

WHAT PRECAUTIONS SHOULD I TAKE?

Recovery of funds by victims of advance fee frauds is often quite difficult. Under present legislation certain types of advance fee scams do not constitute a criminal offence, leaving civil action the only remedy.

Consider adopting the following preventative measures to guard against these types of fraud:

- Ignore all unsolicited communications
- Use only known business channels
- Thoroughly check the validity of any proposed business transaction before forwarding any money or business documentation
- If in doubt, carry out appropriate enquiries
- Remember, if a proposition appears too good to be true - it generally is

WHERE CAN I GET MORE INFORMATION?

Under the Investment Intermediaries Act 1995, anyone providing investment advice is required to register with the Irish Financial Regulator who maintains a public register. Additional information is available on related websites

Financial Regulator:
www.financialregulator.ie

An Garda Síochána:
www.garda.ie

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

BRIBERY & CORRUPTION

WHAT IS IT?

Bribery is a common law offence which concerns the practice of offering something, usually money, to gain an illicit advantage. It is usually confined to public officials.

Corruption includes an abuse of a position of trust in order to gain an undue advantage and involves significant overlap with the law of bribery. An example might be a person employed in either the public or private sector who accepts money to which he is not entitled in return for acting in a particular way in the course of his employment.

In Irish legislation, these offences are characterised by both giver and receiver being equally guilty. In practical terms, it can prove more difficult to secure the evidence to support a charge against both parties. As other fraud offences may be easier to prove (such as theft, deception etc), there have been relatively fewer prosecutions under the specific legislation governing this area.

WHO DOES THIS MOST AFFECT?

In the absence of prosecutions, it is difficult to characterise those most affected. But everybody is vulnerable.

HOW MUCH CAN BE LOST?

Similarly, it is difficult to quantify the losses involved.

WHAT SHOULD I LOOK FOR?

Persons in authority can both bestow or seek unauthorised payments. Persons in authority should never seek reward for simply doing their job. By the same token, offering a reward to a public official or person in authority for special treatment is an offence on your behalf. The crime occurs on the part of both the giver and receiver.

WHAT PRECAUTIONS SHOULD I TAKE?

Transparency and 'four eyes' review are two of the best measures to combat bribery and corruption.

WHERE CAN I GET MORE INFORMATION?

There are many websites on the Internet that give additional information on bribery and corruption, for example:

The Department of Justice Equality and Law Reform:

<http://www.anticorruption.ie>

Enterprise Ireland (pdf entitled: Irish Companies urged to ensure Anti-corruption measures in place')

<http://www.enterprise-ireland.com>

Transparency International:

<http://www.transparency.ie/resources/faqs.htm>

© 2009 An Garda Síochána/PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

CHEQUE AND CREDIT CARD FRAUD

WHAT IS IT?

Cheque fraud - Cheques and bank drafts are stolen or the amount or payee is altered for the fraudster's purposes. Alternatively a counterfeit cheque or draft produced in the likeness of a legitimate payment instrument is passed off as real. Recent trends have shown an increase in the number of counterfeit cheques and bank drafts in circulation.

Criminals tend to present counterfeit cheques/drafts outside banking hours when purchasing goods so that the draft cannot be checked immediately. To frustrate prosecutions or to give themselves an alibi they masquerade as or use couriers to collect the purchased items and hand over the counterfeit in an envelope.

Lost and stolen card fraud – a card is physically stolen from your wallet or home and is then used by a criminal, posing as you, to obtain goods and services. Most fraud of this type takes place before you have reported the loss.

Counterfeit card fraud (Skimming) – a counterfeit or cloned card is one that has been printed, embossed or encoded without permission from the card company, or has been validly issued and then altered or recoded. 'Skimming' occurs when the genuine data from the magnetic stripe on a credit card is copied without the cardholder's knowledge. Skimming may occur when a cardholder hands over their card to make a purchase, for example in bars, restaurants and petrol stations, and where a corrupt employee skims a customer's card before handing it back.

Skimming may also occur when the cardholder uses their card at an Automated Teller Machine (ATM). For example, a skimming device is attached to the card entry slot. A false keypad may be used or a miniature camera may be hidden overlooking the PIN pad to capture the user's PIN. The normal transaction takes place and the user does not lose their card.

The information obtained may then be used to produce the counterfeit cards; the details are used to carry out fraudulent card-not-present transactions. As with lost and stolen card frauds, cardholders are unaware of the fraud until a statement is received showing purchases they did not make.

Card-not-present (CNP) fraud – Criminals commit this form of payment card fraud by obtaining the genuine cardholder's details surreptitiously and then using these details to purchase goods over the phone or on the Internet. Criminals may obtain these details by intercepting post addressed to the victim or by obtaining the victim's discarded payment card receipts (bin raiding). Criminals have also been known to listen to the victim while they purchase goods over the telephone. The victim is often unaware that their account has been compromised until receipt of their next bank or credit card statement. This is the most commonly reported incidence of fraud.

Cash machine fraud (ATM) - Criminals commit fraud at a cash machine in a number of ways.

Shoulder Surfing - This involves criminals looking over a cardholder's shoulder to watch the PIN being entered then stealing the card using distraction techniques or pick pocketing.

Card-wrapping Devices (i.e. Lebanese Loop) - This is a device which is inserted into a cash machine's card slot and will retain the card inside the cash machine for subsequent recovery by the criminal. The criminal tricks the victim into re-entering the PIN while the criminal watches. After the cardholder gives up and leaves, the criminal removes the device, with the card, and withdraws cash.

WHO DOES THIS MOST AFFECT?

Any person or business making transactions using cheques, drafts, ATM or credit cards are at risk of these types of fraud.

HOW MUCH CAN BE LOST?

Transactions can vary, from small amounts up to the fraudulent payment for high value goods such as jewellery, laptop computers, televisions etc.

WHAT SHOULD I LOOK FOR?

Always be careful with your credit and debit cards; never leave your cards out of your sight when making payments. Be suspicious of people asking you to make unusual deviations for the "norm" with regard to payments, for example asking you to send cash or transfer money to them immediately by overnight express, the Internet, mail, wire transfer or any other method.

Always report suspicious behaviour at ATM machines to the Gardaí, if you are suspicious of an ATM machine or think it has been tampered with, make note of the machine. Do not try to remove any suspicious device, but rather report the matter to the Gardaí immediately.

When dealing with cheques and bank drafts, be suspicious of purported customers who send you a cheque or bank draft in excess of the agreed amount for some item you have offered for sale. In these instances the fraudster then asks you to forward the "outstanding" balance after keeping an additional commission for "helping him out". The criminal's cheque or bank draft will then turn out to be worthless.

WHAT PRECAUTIONS SHOULD I TAKE?

Be in control of your financial affairs, always review your bank and credit card statements and follow up on any suspicious transactions that you notice. Protect your personal data - it is valuable information that can be used to defraud you or someone else. Always shred unwanted documents which contain personal data.

WHERE CAN I GET MORE INFORMATION?

Banks and Payment Card Companies frequently issue security guidance to customers. Pay special attention to information on the website of your financial institutions. The 'Make IT Secure' website hosts valuable information on securing of your cards and personal information. The site also offers sound advice on Phishing, IT Security Basics, and Social Networking on the Internet etc.

Make IT Secure:
www.makeitsecure.ie

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

COMPUTER CRIME (INCLUDING HACKING)

WHAT IS IT?

The proliferation of computer systems, across so many applications, has meant that many so-called 'traditional' frauds now involve some use of computer systems. The nature of these computer systems can greatly increase the vulnerability of individuals and businesses to fraud – transactions are more complex, more voluminous and happen far faster than in a manual environment.

There is no crime of 'computer fraud' defined in Irish legislation. Nevertheless, related fraud legislation now addresses many aspects of computer systems, such as admissibility of computer evidence.

Computer crime refers to offences where the computer or the data on the computer is the object of the attack. The common term "computer hacking" falls into this category and can be described as a method of gaining access to a computer system to either destroy the system or obtain personal information or sensitive commercial information.

"Computer fraud" is a subset of computer related crime. It could be described as the use or causing the use of a computer resource for the purpose of illegally gaining goods or services or causing harm. It might be any traditional type of fraud that is aided through use of a computer including online auction fraud, phishing, identity theft, hacking offences and unauthorised access etc.

Modern business use computers to conduct business on a daily basis. As such "data" is a valuable economic commodity. Data such as financial information, credit

card information and personal information is frequently targeted by criminals. The sale of this "data" and information may be used for creating fraudulent identification documents, counterfeit credit cards or to create spamming lists to be sold on the black market. It is a lucrative market for fraudsters. Remote access to systems allows the criminal to commit computer related fraud without ever physically entering the victim's business premises so it is often seen as an easy target.

Even though there are stiff penalties for committing computer fraud, laws against it may be difficult to enforce. Some of the email scams for phishing attacks, identity theft, and PABX frauds originate outside the Irish jurisdiction. Also, not all cases of computer fraud may result in a criminal offence. Investigations may need to be carried out under civil proceedings in some cases e.g. copyright ownership and licensing issues.

Obtaining personal information or sensitive company information can also be the goal of criminals who steal company laptops, Personal Digital Assistants (PDAs) or other mobile devices. Where individuals including staff members have access to company systems, high capacity storage devices, known as USB "thumb" drives, can be used to copy and remove large volumes of data from unsuspecting organisations. This information can be sold to criminal organisations, competitors or used to commit fraud.

WHO DOES THIS MOST AFFECT?

Given the proliferation of computers, everyone – individuals and businesses – is at risk.

HOW MUCH CAN BE LOST?

Losses range from relatively small amounts to enormous amounts. Some of the largest frauds discovered in recent years could not have been perpetrated without computer generated documentation to support the fraudulent transactions.

WHAT SHOULD I LOOK FOR?

Deal with reputable sellers especially when buying online. Read the reviews on the buyers and sellers which are provided on most sales websites.

If you use internet banking, regularly check your transactions and report any concern you may have to your bank or the Garda Síochána, and act on the security advice which your bank provides.

WHAT PRECAUTIONS SHOULD I TAKE?

Security measures that protect data and computer systems are essential to protect against frauds in this area. Due to the complexity of the area, businesses should seek independent expert advice. For individuals, some of the more important precautions include:

- Always keep computer anti-virus, anti-spyware, and firewall software functioning and up to date.
- Never divulge security or identity details over the internet. Banks will never request this information over the internet.
- Rather than clicking on a banking link from an e-mail (which may re-direct you to a phishing website) type the website address directly into the browser yourself.

- Always use secure internet connection for transmitting sensitive banking information when shopping online. There should be 'https' at the beginning of the website address and a secure padlock symbol.
- Don't judge a company or individual solely by their website.
- Look for evidence of a physical address and telephone contact details. Be aware that these details can be fraudulently used by scammers to deceive e.g. landline number is for a public payphone or a mobile telephone number, the address is genuine but no such company is located there.
- Do your research – check information on the internet to see if anyone else has dealt with this company or individual.
- Use common sense – if it looks too good to be true, it probably is. If you haven't entered the lottery you cannot win it!
- Use a secure password that cannot be easily guessed.
- Vary your passwords; avoid the temptation to use the one password to gain access to your computers and for all services on the Internet.
- Always take a backup of your computer data in case of emergency or in case there is a need for urgent investigation.
- If you are a small to medium enterprise ensure you have secure practices and procedures over the use of the company IT system.
- Companies should always have an acceptable user policy for employees and contractors.
- All companies should keep an IT security policy document and should review its effectiveness regularly to ensure all modern threats are addressed.
- Companies should always have an IT Security - Critical Incident Response plan especially if your company relies on the Internet and IT system for business continuity.

WHERE CAN I GET MORE INFORMATION?

The security measures that individuals can apply are well documented in many websites, for example, the 'Make IT Secure' campaign. Many financial institutions offer security advice on their sites for users on their services and many professional companies offer IT security services.

Make IT Secure
www.makeitsecure.ie

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

COUNTERFEIT CURRENCY

WHAT IS IT?

Counterfeit currency is produced without legal sanction of the State or Government to resemble some official form of currency closely enough that it may be confused for genuine currency.

WHO DOES THIS MOST AFFECT?

Anyone handling cash is vulnerable to counterfeit currency.

HOW MUCH CAN BE LOST?

Counterfeit Currency Seizures from National Analysis Centre for 2008:

€5	€10	€20	€50	€100	€200	€500
59	433	816	12,343	614	800	2

WHAT SHOULD I LOOK FOR?

The following is a list of some of the security features of the euro currency that can be easily checked to help decide whether the notes should be treated as suspect or not.

- Firstly the euro banknotes are printed on special banknote paper made mainly from cotton fibres. It feels crisp – not limp or waxy. Counterfeiters should not be able to get hold of such paper.
- On euro banknotes you can feel the initials of the European Central Bank (i.e. the letters BCE, ECB, EZB, EKT, EKP), the value numerals and the window and gateway motifs. Age and wear can gradually reduce some of these properties.
- Look for the watermark, the security thread and the 'see-through' feature. Hold the banknote up to a light.
- The watermark is visible on both sides of the same unprinted area. You can therefore see both the main architectural motif and the value numeral. The watermark is created inside the paper by varying the paper thickness during the papermaking process. You can see various parts, some of which are lighter and some of which are darker than the surrounding paper.
- The security thread is also incorporated into the paper at the manufacturing stage. When the banknote is held up to the light you will notice a dark line across the entire width of the banknote. If you look very carefully at the thread against the light you will see the word "EURO" together with the value numeral (either the right way round or back to front).
- While being viewed against the light, the banknote can also be checked for the see-through register. This feature is in the top left-hand corner on the front of the banknote. Irregular marks, printed on the front and the reverse of the banknote join to create a complete and perfect value numeral when held up to the light.
- On the front right-hand side of the low-value banknotes (€5, €10 and €20) there is a hologram foil stripe. When you move the banknote from side to side, look for a brightly coloured euro symbol and the value numeral (5, 10 or 20).
- On the front of the high-value banknotes (€50, €100, €200 and €500) there is a hologram foil patch.
- When you move the banknote look for a brightly coloured numeral and the image of the architectural motif depicted on the banknote.
- Another feature which can be easily spotted on the four highest-value banknotes is the colour-shifting ink. You see it in the value numeral in the lower right-hand corner on the reverse sides of these four banknotes. This numeral looks purple when viewed straight on, but olive green or even brown when viewed at an angle.
- The lower denominations, the €5, €10 and €20 banknotes have an iridescent stripe. This only appears on the reverse side. It shines under a bright light and you can see a euro symbol inside the stripe together with the value numeral.

Always check more than one of the security features in order to ensure that a banknote is genuine.

WHAT PRECAUTIONS SHOULD I TAKE?

Various security features have been incorporated into the euro banknotes. They will help you to recognise a genuine banknote at a glance. The best way to check for forgery is to check three features:

Feel the raised print – special printing processes give banknotes their unique feel.

Look at the banknote against the light: the watermark, the security thread and the see-through number will then be visible.

Tilt the banknote: on the front, you can see the shifting image on the hologram. On the back, you can see the glossy stripe (on the €5, €10 and €20 banknotes) or the colour-changing number (on the €50, €100, €200 and €500 banknotes).

WHERE CAN I GET MORE INFORMATION?

Detailed information on the security features of euro currency notes is available at the Central Bank & Financial Services Authority of Ireland and European Central Bank website.

Central Bank & Financial Services Authority of Ireland: **www.centralbank.ie**

European Central Bank **www.euro.ecb.int**

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

INVESTMENT FRAUD

WHAT IS IT?

Investment fraud occurs where monies entrusted to an individual or organisation are misappropriated. It includes cases where victims place trust in an individual holding himself out as an investment intermediary who eventually misappropriates the funds entrusted to them.

WHO DOES THIS MOST AFFECT?

Usually, individuals wishing to invest in a scheme with an expectation of high yield return.

HOW MUCH CAN BE LOST?

Victims have suffered substantial losses up to and including their life savings.

What should I look for?

Victims are often approached and offered products with abnormally high rates of return in a relatively short space of time. Individuals should be wary of the practice of unsolicited or 'cold' calls offering investment opportunities. Few details are made known to the victim concerning the investments in which their monies are being placed. Information relating to the investment should be received on a regular basis showing the amounts invested, movements on the investment during the period and the value of the investment at the end of the period.

WHAT PRECAUTIONS SHOULD I TAKE?

Checking the credentials of the intermediary

- Check out the investment firm or person with whom you are dealing and ensure that they are authorised by the Irish

Financial Services Regulatory Authority (IFSRA) to carry out investment business. Contact IFSRA with any concerns you may have before making an investment.

- Where an investment business firm sells different investment products it must hold an appointment in writing, from each product producer, which can be inspected.
- Consider inspecting the investment business firm's professional indemnity insurance.
- If in doubt, get further professional advice in advance of investing.

Once you are satisfied with the investment firm's credentials there are other steps you can take to protect your investments and reduce the risk of fraud:

- Ensure that your cheque is made payable to the company in which you are investing and not to the investment intermediary.
- Do not authorise the investment intermediary to be a co-signatory on any documents or cheques relating to transactions on your investment account.
- Do not give any authorisation for any other person to withdraw funds from the account.
- Ensure that you receive a policy document and satisfy yourself that it reflects your intentions.
- Obtain a receipt for all sums entrusted to the intermediary for onward payment.

WHERE CAN I GET MORE INFORMATION?

Under the Investment Intermediaries Act, 1995, the Irish Financial Services Regulatory Authority is responsible for the regulation of investment firms in Ireland.

The Irish Financial Services Regulatory Authority maintains a register of investment firms which are authorised to provide services in Ireland, including those from another EU state that provide investment services on an international basis. The register is open to public inspection. The regulator has powers to investigate and take action against unauthorised investment firms.

The advertising requirements issued by the regulator to authorised investment firms do not permit unsolicited calls to members of the public, except where there is an existing client relationship with the firm. You should not be 'cold called' by representatives of investment firms, whether authorised or not.

Central Bank & Financial Services Authority of Ireland:

www.centralbank.ie

© 2009 An Garda Síochána/PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

MONEY LAUNDERING / TERRORIST FINANCING

GARDA MONEY LAUNDERING INVESTIGATION UNIT

The Money Laundering Investigation Unit is attached to the Garda Bureau of Fraud Investigation and includes the national Financial Intelligence Unit which was established in conformity with EU Regulations on the matter. The Criminal Justice Act of 1994 created the offence of Money Laundering. The definition of Money Laundering was amended by the Criminal Justice (Theft and Fraud Offences) Act 2001.

WHAT IS IT?

Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully money laundering enables criminals to legitimise 'dirty' money by mingling it with 'clean' money, ultimately providing a legitimate cover for the source of their income.

A person shall be guilty of an offence if, knowing or believing that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of drug trafficking or other criminal activity, he (a) conceals or disguises that property, or (b) converts or transfers that property or removes it from the State, for the purpose of assisting any person to avoid prosecution for an offence or the making or enforcement of a confiscation order.

Terrorist financing usually works where funds are intended for use in terrorist activity

WHO DOES THIS MOST AFFECT?

The Criminal Justice Act 1994 as amended imposes legal obligations to report suspicions of Money Laundering / Terrorist Financing to An Garda Síochána. The

persons and organisations affected include credit and financial institutions, lawyers, accountants, estate agents and others. In 2009 this list was extended to cover dealers in high value goods, trust and company service providers and casinos. These reports are made pursuant to Section 57 Criminal Justice Act 1994 and must be forwarded to The Money Laundering Investigation Unit, Garda Bureau of Fraud Investigation Headquarters, Harcourt Square, Dublin 2.

The standard reporting form for Suspicious Transaction Reports or "STR's" can be obtained from the Financial Intelligence Unit at the Garda Bureau of Fraud Investigation, which is situated in Harcourt Square Dublin 2.

The legislation also places requirements on designated persons and organisations to have specific procedures in place to provide for the prevention of money laundering and terrorist financing, including the retention of documentation and records for a period of five years following the termination of business in respect of any transaction.

STAGES OF MONEY LAUNDERING

Money laundering is usually accomplished in three stages, each of which has its own characteristics and each of which may comprise numerous transactions by the launderer. These stages are commonly referred to as:

- Placement
- Layering
- Integration

Placement

This occurs when the launderer makes the initial placement of cash proceeds derived from criminal conduct. This

initial placement can be with a financial institution, solicitor, auctioneer, estate agent, accountant, casino or a dealer in high value goods such as jewellery, cars, expensive paintings and so on.

Layering

This stage of money laundering occurs when the proceeds of criminal conduct are distanced from their source by creating complex layers of financial transactions. It is also achieved by the passing of money through an international web of legitimate businesses and 'shell' companies. All of this is designed to disguise the audit trail and provide anonymity therefore making it extremely difficult for the investigator.

Integration

This is the provision of apparent legitimacy to wealth derived from criminal conduct. Where placement and layering have succeeded, the laundered proceeds now re-enter the economy with the appearance of normal business funds.

WHAT SHOULD I LOOK FOR?

- False names / doubts over identity / use of unknown agents
- Offers of unusual deals, particularly involving significant amounts of cash
- Non-commercial cash deals where the profit to you, or the lack of profit to the other party, is unrealistic.
- Reluctance by the other party to disclose usual information regarding their circumstances
- Source of funding for the deal is unclear
- Unusual transactions involving known source or points of transit for narcotics, for example, Middle East, Central Europe, Central and South America

- Unusual transactions involving tax haven countries where secrecy laws might facilitate money laundering.
- Use of intermediaries, many different banks or financial advisors for no obvious purpose.
- Clients and customers who could find the same type of services or goods you are offering nearer their home base.
- Exchange of cash in small denominations for large denomination notes
- Regular large cash transactions
- Slow paying customers repaying their account unexpectedly
- Business carried on by post or through nominees or other professionals or third parties where it is more usual to carry on business on a face-to-face basis
- Not knowing the true identity of your customers, suppliers or other business associates

An examination of your business records might highlight a number of additional features suggesting your organisation is unwittingly involved in Money Laundering such as:

- Unauthorised or improperly recorded transactions
- Accounting systems with inadequate audit trails
- Purchases by cheque made payable to "bearer" or transfers to numbered bank accounts
- Excessive or unusual sales commissions or agents fees

The law places an onus on you to be alert for Money Laundering. If you have suspicions, act carefully! You should seek professional advice as soon as possible.

With regard to Terrorist Financing, this has similarities to Money Laundering in that both are trying to disguise the sources of funds and the crime – to make the funds appear legitimate – by this process the criminal can enjoy his ill-gotten gains.

In relation to Terrorists the reason for disguising the funds is that the movement of funds connected to suspected Terrorists / Terrorist Groups could indicate to authorities that a Terrorist Groups is planning an attack or that it is now active with a particular jurisdiction.

The main difference between the two is the amount of money involved. Criminals would be trying to disguise large amounts of money raised from whatever criminal enterprise that they are involved in. Terrorists on the other hand usually move small amounts of money. It does not always take a large amount of money to mount a terrorist attack.

The indicators for Terrorist Financing could include all of those previously described for Money Laundering but could also include:

- Withdrawals from accounts with specific request for the funds to consist of €500 notes.
- Requests to transfer funds to potential conflict zones especially if no such requests had been made previously.
- After obtaining loans for specific items, drawing them down in cash with a request to transfer the funds abroad.

TIPPING OFF OFFENCE

Section 58 of the Criminal Justice Act, 1994 as amended provides for various offences of prejudicing an investigation under the Act including the offence of 'tipping off'.

A person shall be guilty of an offence where they, knowing or suspecting that an investigation is taking place, makes any disclosure which is likely to prejudice that investigation. This applies in relation to an investigation into drug trafficking or an investigation into whether a person has benefited from an offence in respect of which a confiscation order might be made, or an order under Section 63 of the Act has been made or applied for, or a warrant under Section 64 of the Act has been issued, or a report under Section 57 of the Act is made.

This offence carries a five year prison sentence on conviction on indictment.

WHAT PRECAUTIONS SHOULD I TAKE?

- Be familiar with current Money Laundering Legislation.
- When opening customer accounts, ensure that proper accounts opening documentation is obtained. Keep copies of all such documentation.
- Ensure that accounts are operated within the parameters that one would expect.

WHERE CAN I GET MORE INFORMATION?

- More in depth information can be obtained from the Guidance Notes issued by various professional bodies.
- Open source material (e.g. FATF publications) can also prove helpful.
- In relation to EU Sanction Lists, information can be obtained from the Central Bank of Ireland.
- For larger organisations the World Check Data Base or similar companies offering this service are available for checking individuals and entities.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

MORTGAGE/CREDIT FRAUD

WHAT IS IT?

The applicant misrepresents himself by use of fictitious documents to obtain a mortgage or other credit facility. Another form is where a secured property is grossly overvalued or does not exist at all.

Cases sometimes involve professionals who fail to register the owners or a financial institution's interest in a property and take out further loans secured on the property for their own unlawful benefit.

Other examples include applications for loans for fictitious plant or machinery based on bogus documents or where the applicant falsifies the true purpose of the loan as he knows the application would be unsuccessful. Collusion can complicate the arrangement under which this fraud takes place.

WHO DOES THIS MOST AFFECT?

Lenders typically carry any loss involved in this type of fraud. Organisations whose work is processed by unscrupulous agents can also suffer.

HOW MUCH CAN BE LOST?

Losses can be significant for lenders especially if there is orchestrated fraud over a wide number of properties.

WHAT SHOULD I LOOK FOR AND WHAT PRECAUTIONS SHOULD I TAKE?

There is no substituting for knowing your customer and performing detailed checks on loan documentation (for example, confirming that security has been properly registered rather than relying on representations) – before giving any approval. Random checks are a further useful detective method that can also serve as a useful deterrent. Finally, deep testing by an independent internal audit function can provide useful assurance to management and the Board.

WHERE CAN I GET MORE INFORMATION?

The Financial Regulator, the banks and the GBFI can provide further information and guidance.

Central Bank & Financial Services Authority of Ireland: www.centralbank.ie

Garda Bureau of Fraud Investigation: www.garda.ie

© 2009 An Garda Síochána/PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

PHISHING AND IDENTITY THEFT

WHAT IS IT?

'Phishing' is a form of online fraud where fake emails or websites, supposedly from a legitimate company, try to obtain your confidential bank and/or credit card account details.

A phishing scam is an attempt to make you think that a bank or other legitimate business is asking you to verify your confidential banking credentials such as username, password, PIN number, bank account number etc. There has been an increase in the number of phishing scams that attempt to obtain usernames and passwords for the purpose of bypassing the authentication information the banks have in place in the use of internet banking. The notification email looks genuine in appearance and may have correct bank logos on it. The message will appear somewhat urgent in order to get you to respond immediately and not give you time to think too much about what you are doing. The 'phishing' website that you are directed to looks authentic. However, no legitimate company will ever ask you to send sensitive information such as credit card PIN numbers via email.

Identity theft or ID theft occurs when a criminal uses fraudulently obtained personal information to open or access bank accounts in someone else's name. Criminals steal documents or details such as: utility bills, passports, driving licence, birth certificate, bank account number or PIN numbers, and use them to obtain goods or services illegally. There are two types – application fraud and account take-over.

Application Fraud

Application fraud involves criminals using stolen or false documents to open an account in someone else's name. Criminals steal documents such as utility bills and bank statements to build up usable information. Alternatively, they may use counterfeit documents for identification purposes.

Account take-over

This involves criminals taking over another person's account by first gathering personal information about the intended victim (bin raiding, dumpster-diving and so on). The criminal contacts the card issuer, masquerading as the genuine cardholder, requesting mail be redirected to a new address. The criminal then reports the card lost and requests a replacement to be sent to the new address.

Account take-over can also occur with the collusion of the account holder where:

- the account is purchased by criminals from foreign students or workers returning home from Ireland; or,
- a legitimate customer that either intentionally allows his/her account to be used to receive illegal funds or where the customer has been "duped" into allowing their account to be used

A recent type of phishing/identity theft attack against unsuspecting computer users is called 'the man in the browser' or 'man in the middle' attack. This occurs where a computer user inadvertently downloads a piece of malicious software called a 'Trojan'. Once installed on the unsuspecting computer user's machine,

the Trojan will watch for certain actions which will trigger it to record information like user names, passwords and personal identification numbers for key financial Internet services. Once the Trojan has secured the necessary information the fraudsters can use the information to access online banking, make money transfers and purchase goods in the name of the victim; in some cases the Trojan can perform all these actions automatically.

WHO DOES THIS MOST AFFECT?

Given the proliferation of computers, everyone – individuals and businesses – is at risk of phishing attacks. Likewise we are all at risk of identity theft, especially where individuals are careless with the protection and disposal of personal information.

HOW MUCH CAN BE LOST?

In the case of phishing attacks, the individual loss for each account varies but is usually between €3,000 and €5,000 for each bank customer.

WHAT SHOULD I LOOK FOR?

Individuals should treat security requests and similar approaches with extreme scepticism. Invitations to allow your account to be used to process or receive funds from unknown sources should be reported immediately to the authorities.

WHAT PRECAUTIONS SHOULD I TAKE?

Delete email requests from unknown or dubious sources. Exercise vigilance at all times and avoid disclosing personal information (especially bank or credit card details) unless you are absolutely certain of the identity of the sender.

Always keep computer anti-virus, anti spy ware, and firewall software functioning and up to date.

If you use Internet banking, regularly check your transactions and report any concern you may have to your bank. Act on the security advice which your bank provides.

WHERE CAN I GET MORE INFORMATION?

The Garda Bureau Fraud Investigation is working with the financial industry to investigate and prevent this activity and the actions taken so far have resulted in considerable savings to financial institutions and their customers.

The Irish Banking Federation, the Irish Payments Services Organisation, An Garda Síochána and the Police Service of Northern Ireland produced a leaflet which includes key warning signs that consumers should be on the lookout for and the steps they should take to protect themselves against online, card-based, ATM and Identity fraud.

The guide, 'Be Aware, Beat Fraud', can be viewed at: www.url.ie/2rkc

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

DENIAL OF SERVICE

WHAT IS IT?

A denial of service attack (DoS attack) or distributed denial of service (DDoS attack) is an attempt to make an internet network resource such as e-commerce or e-mail unavailable to its genuine users. It is the malicious efforts of an individual or individuals to prevent an internet website or service from functioning efficiently or to temporarily disable it. The most common method involves saturating the target machine with external communication requests so that it cannot respond to legitimate traffic in an efficient manner. All the resources are consumed with responding to the attacking requests and the website grinds to a halt. The attack may be coming from large networks of compromised computers known as a 'botnet' (short for roBOT NETwork).

WHO DOES THIS MOST AFFECT?

Those whose business is mainly or wholly delivered on the Internet.

HOW MUCH CAN BE LOST?

Businesses can face substantial losses as a result of DDoS: the time (and cost) taken to address the problem alone can be significant. In extreme cases DoS attacks have forced popular web sites to temporarily cease operation.

WHAT SHOULD I LOOK FOR?

Although the motive and format of the attack may vary, the offenders typically target high profile web sites such as banks, online betting stores, auction sites and shopping websites.

In Ireland in recent years there have been a number of high profile DDoS attacks which have been highlighted in the media. A DDoS attack can cost the target individual or company substantial time and money.

WHAT PRECAUTIONS SHOULD I TAKE?

Seek outside advice - this is a complex area and requires the expertise of skilled IT and forensic professionals.

WHERE CAN I GET MORE INFORMATION?

The Garda Computer Crimes Investigation Unit, Harcourt Square, Dublin 2 can offer advice and assistance. Additional information is also available on the Internet and the United States Computer Emergency Readiness Team offers additional information at:

<http://www.us-cert.gov/cas/tips/ST04-015.html>

© 2009 An Garda Síochána/PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

PABX FRAUD

WHAT IS IT?

A PABX (Private Automatic Branch eXchange) is a computerised system that manages an internal telephone network. PABX phone systems are commonly used within Irish organisations.

Most PABXs have engineering and maintenance access codes. If these access codes are compromised the attacker will have total control of the system.

If an organisation's PABX has voicemail and is DISA-enabled (i.e. can provide access to telephone services by dialling into the system from outside the PABX network) then it is susceptible to this form of fraud. Usually, the only indication that you will see is a substantial increase in your telephone bill.

WHO DOES THIS MOST AFFECT?

Any organisation that owns and operates a PABX system could be susceptible to this type of fraud.

What should I do if I become a victim of a PABX fraud?

PABX fraud is a criminal offence and in addition to reporting the incident to An Garda Síochána you should contact your telecoms provider and your PABX supplier who will assist in preventing further occurrences

HOW MUCH CAN BE LOST?

Substantial losses can be incurred every month – often without the organisation realising anything is amiss.

WHAT SHOULD I LOOK FOR?

Usually, the only indication that you will see is a substantial increase in your telephone bill. Detailed billing will assist in identifying any potential unauthorised calls, usually International calls but they can also be National telephone calls. Another indicator is where customers trying to dial, in or employees trying to dial out, find that the lines are always busy.

WHAT PRECAUTIONS SHOULD I TAKE?

- If DISA is not required ensure that it is disabled.
- If DISA is required, contact your PABX supplier or maintenance company, who can help you in configuring DISA properly.
- Toll Fraud Audit - this service is provided by your PABX supplier or maintenance company.
- Enable automatic logging of calls if available. This may help in identifying the extension number that is being used to compromise the PABX and it may also identify the source of the external call.

- Regularly check the log records for repeated short duration calls to the same number. This could be an indication of an attempt to attack your system.
- Activate PINs for voicemail, DISA and engineering access (if enabled) and change regularly.

If possible, remote engineering access should be permitted only on a 'call back' basis. This will prevent unauthorised access to this privileged account.

WHERE CAN I GET MORE INFORMATION?

Additional information can be obtained from the supplier/installer of your PABX system.

All incidents of PABX fraud can be reported at your local Garda station or to the:

Computer Crime Investigation Unit, Garda Bureau of Fraud Investigation Harcourt Square, Harcourt Street Dublin 2

© 2009 An Garda Síochána/PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

STAFF RECRUITMENT PROCEDURES CHECKLIST

Many frauds are committed by people employed in the organisation concerned. They possess detailed and in-depth knowledge of the organisation, its systems and its weaknesses.

The recruitment process provides the initial opportunity to reduce the risk of fraud being committed by an employee. Steps which can be taken during the recruitment process include:

ADVERTISING:

- When advertising a position make it clear that a person of integrity is sought and that references will be required. Also make it clear that the identity of the individual, regardless of nationality, will need to be checked by reference to sight of a passport or driving licence, and the necessary authority, if appropriate, to stay and work in Ireland.

THE INTERVIEW:

The interview provides an important means of establishing the integrity of the person involved:

- Ask questions requiring more than a 'yes' or 'no' answer.
- If you haven't been trained in formal interview techniques, seek professional support. The consequences of getting it wrong are worth the investment.
- Pose ethical questions using hypothetical situations, for example: "If you had to decide whether a particular course of action was ethical or honest how would you go about making that decision?"
- Be conscious that applicants may wish to give you the answer you want to hear.
- Look for signs (including body

language, rapid eye movement, nervous touching of the face and so on) that the interviewee is particularly uncomfortable considering matters of integrity and honesty.

- Use the interview to confirm all details on the application form or CV. Be wary of inconsistencies or hesitant answers to questions probing the background to the information presented. Any variance from the detailed information provided should be taken as a warning sign and great care should be exercised prior to progressing the application. In particular, check out any gaps in dates in a candidate's work history. Often, candidates may be tempted not to disclose any time spent in jail for previous criminal activities.
- Panel interviews (with two or more interviewers), have the advantage of the interviewers being able to compare notes and having a second opinion readily to hand. It is also good practice to maintain these records for at least 12 months subsequent to the interview.
- It is of utmost importance that any employer can verify that any employee is able to work legally in Ireland.

REFERENCES:

References provide very useful third party confirmation of your opinion/assessment of an applicant.

- Always take up references. In particular, verify any reference received directly from the candidate with the referee.
- Assess the referees. Avoid candidates with poor referees.
- Insist on receiving a reference from the current or most recent employer.

- Ask the key question "Are there any underlying reasons for me not to consider employing this individual?"
- Referees should be contacted by letter. (See Sample Letter to Referee below)
- Remember that many firms have standard references that they issue in response to such requests.
- Follow up referees' responses by telephone. You will obtain a better understanding of the reference by talking to the referee. A key question to ask is whether the referee would re-employ the candidate.

IDENTITY AND QUALIFICATIONS:

- Insist on obtaining proof of identity, for example driver's licence or passport.
- Verify qualifications to original certificates or seek confirmation from the qualifying institution.

CONTRACT OF EMPLOYMENT

- The contract of employment should specify that the employee is required to act all times with honesty and integrity. Ensure that you have a signed acknowledgement of receipt of these conditions in your files.
- It should refer to the disciplinary procedures in operation should the employee not adhere to the terms of the contract.
- It might also refer to the firm's security policy and the need for the employee to take appropriate action to apply that policy.

SECURITY POLICY:

Consider having a written security policy for distribution to all staff, including new recruits, which includes the following guidelines and information:

- Employees are responsible to ensure that any assets of the organisation in their charge are properly safeguarded and all reasonable precautions are taken to maintain a secure environment
- Contact details for the person to whom any suspicions of fraud or dishonesty should be reported
- Ensure that these are signed and distributed annually as reminders to your employees.
- In the event of a 'security alert' or fraudulent attack, that the employer requires immediate unhindered access to the employee's personal work area, desk, briefcase, filing cabinet, personal lockers, computer equipment (including organisers), electronic files, company car etc, in certain circumstances. In the event of a suspected fraud, this will facilitate a detailed search of personal and business files etc. which may provide valuable evidence.
- This is standard practice in many employers and it is reasonable to have this as a condition of employment.
- If you have a suspicion of a "Fraud attack", and feel the need to erect CCTV cameras around a site or in an office environment, put public notices up or distribute emails, setting out why and for how long. Keep your employees reminded that they too have an obligation to inform or advise of any seen or suspected wrongdoing.

PROBATION:

- All candidates should be taken on for a period of probation, usually six months.
- Use this period to evaluate the employee's integrity and honesty.

ONGOING ASSESSMENT AND REVIEW:

- Put procedures in place to assess and review employees' performance on a regular basis following the completion of the probation period.
- Ongoing assessment and review of the employee's integrity and honesty should be part of this process.
- Check out any feedback from customers or suppliers if appropriate.
- Review expense claims closely from all employees.

PERSONAL FILE:

The recruitment process provides the basic information you require to begin building up a personal file for the successful applicant. In this context, key material to be retained includes:

- A photograph of the employee, copy of passport etc
- All information obtained during the recruitment process: application form, CV, verification of qualifications, visas, work permits, references taken up etc
- The signed contract of employment
- Ensure that any necessary visa renewals are followed up

Personal details will change over time such as when employees move home. It is important therefore to keep the details recorded on the file up to date. In the event of fraud, information obtained from the personal file may be very useful to both the Gardaí and the organisation in bring a successful prosecution. Your corporate reputation is on the line if your files are not maintained adequately.

PART-TIME EMPLOYEES AND CONTRACTORS:

Apply these recruitment procedures consistently, including the hire of part time employees and contractors.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

SAMPLE LETTER TO REFEREE

Strictly Private and Confidential

[Date]

Dear [Name]

RE:

The above named is due to commence employment with us shortly and has given your name as a referee.

I should be grateful if you would respond to me as soon as possible setting out your views on their work performance. In particular, I would like you to address the following areas in your response:

- Dates of employment
- Position held
- Reason for leaving
- Performance level
- Relationship with others
- Attendance / time-keeping record
- Would you re-employ?
- Visa/Work permit details

I assure you that any information you provide will be treated in the strictest confidence.

Many thanks for your assistance.

Yours sincerely,

Etc.

© 2009 An Garda Síochána/PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.

USEFUL LEGISLATION

The expression 'fraud' is used as a collective name for a number of statutory and common law offences. There is no specific offence of 'fraud', though there is a common law offence of "conspiracy to defraud".

Those investigating fraud-related crime must first establish that there has been a breach of the law. It frequently happens in fraud cases that there is no difficulty in identifying the culprit. The most common breaches of the law encountered in the investigation of fraud are dealt with by the following legislation:

- The Criminal Justice (Theft and Fraud Offences) Act 2001.
 - Section 4 Theft
 - Section 6 Deception
 - Section 7 Obtaining Services by Deception
 - Section 10 False Accounting
 - Section 25 Forgery
 - Section 26 Using a False Instrument
 - Section 27 Copying a False Instrument
 - Section 28 Using a copy of a False Instrument
 - Section 29 Custody or Control of certain False Instruments
 - Section 48 Warrant to search
 - Section 52 Order to produce evidential material
 - Section 59 Reporting of Offences
- Criminal Justice Act 1984
- Criminal Justice (Forensic Evidence) Act 1990
- Criminal Justice Act 1994
- Criminal Justice Act 1999
- Criminal Justice Act 2006
- Criminal Damage Act 1991
- Proceeds of Crime Act 1996
- Criminal Justice (Miscellaneous Provisions) Act 1997
- Bankers Books Evidence Act 1879
- Companies Acts 1963 and 1990.
- Companies (Amendment) Acts, 1983, 1986, 1990 and 1999 (2)
- Company Law Enforcement Act 2001 (CLEA)
- District Court (Bankers Books Evidence) Rules 1998
- Central Bank Act 1971
- Criminal Evidence Act 1992 (sections 4,5,6,7 &30)
- Consumer Credit Act 1995 (Money Lending brief outline)
- Copyright & Related Acts 2000
- Taxes Consolidation Act 1997 (Section 1078)
- Disclosure of Certain Information for Taxation and Other Purposes Act 1996
- Data Protection Act 1988
- Non-Fatal Offences Against the Person Act 1997
- Prevention of Corruption Act 1906
- Prevention of Corruption (Amendment) Act 2001
- Misuse of Drugs Act 1977, as amended
- Proceeds of Crime (Amendment) Act 2005
- Criminal Justice (Drug Trafficking) Act 1996
- Criminal Justice (Miscellaneous Provisions) Act 1997
- Offences Against the State (Amendment) Act 1998
- Criminal Justice (Illicit Trafficking by Sea) Act 2003
- Criminal Justice (Terrorist Offences) Act 2005
- Criminal Justice (Mutual Assistance) Act 2008
- Statutory Instrument 167 of 1996 (defines "prescribed sum " for section 38 Criminal Justice Act 1994 as amended)
- Statutory Instrument 152 & 153 of 2002 ("Designated Countries")
- Statutory Instrument 242 of 2003
- Statutory Instrument 416 of 2003
- Competition Act 2002 as amended.
- Various Employment Acts

Disclaimer

SOME USEFUL CONSIDERATIONS FOR USE IN FRAUD INVESTIGATIONS

FIM: FRAUD INVESTIGATION MODEL.

Step	Name	Description
1	Awareness	What is the irregularity requiring investigation?
2	Offence	What is the exact breach of Criminal, Civil or HR Law?
3	Evidence	What evidence is required to prove your case
4	Availability	What is the availability of the evidence required? Is it available in Ireland, abroad, in a third party organisation etc.?
5	Accessibility	What is the accessibility of the evidence required? How do I gain legal access to the evidence? Do I need court orders etc?
6	Admissibility	What is the admissibility of the evidence required? How do I ensure that all the evidence I have gathered will be admissible in court?
7	Weight	What weight can be attributed to the evidence? Is the evidence irrefutable, circumstantial, etc?
8	Sufficiency	Is the evidence sufficient to sustain a conviction against the accused person?

© 2009 An Garda Síochána/PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

Disclaimer

While every care has been taken in the production of this publication, An Garda Síochána and PricewaterhouseCoopers do not accept any responsibility in respect of anyone or any organisation acting or refraining to act as a result of this publication. In all cases, appropriate professional advice should be sought.

References in this publication to the masculine gender include the feminine gender.