



An Garda Síochána  
Ireland's National Police Service



**DON'T BE A VICTIM**

PRICEWATERHOUSECOOPERS 



# FRAUD ALERT

## AN ISSUE FOR EVERYONE

I am pleased to present Fraud Alert, a publication produced jointly between the Garda Bureau of Fraud Investigation (GBFI), the specialist agency within the Garda Síochána dedicated to this area of work, and PricewaterhouseCoopers.

This document highlights the more common types of fraud coming to the attention of An Garda Síochána. It delivers excellent fraud prevention advice to a broad section of the community including company directors, managers, staff and individual members of the public.

In recent years, advances in technology and the Internet have provided a new arena for business. These advances have also, regrettably, provided opportunities for the commission of fraud related crime. The challenge for law enforcement agencies in partnership with business and local communities is to ensure that adequate measures exist to combat this threat.

I would like to pay a special tribute to the people from PricewaterhouseCoopers and the Garda Bureau of Fraud Investigation who are responsible for this publication, in particular, Mr. Bob Semple and Ms. Ruth Caulfield of PricewaterhouseCoopers together with Detective Superintendent Eugene Corcoran and Detective Inspector Paul Gillen from the GBFI.

**Fachtna Murphy**  
Commissioner  
An Garda Síochána

PricewaterhouseCoopers was delighted to work again with An Garda Síochána to update this important joint publication on fraud.

Following the publication of the original 'Fraud Alert', 10 years ago, the production of an updated version could not be more timely. Recent PricewaterhouseCoopers research on economic crime has indicated that the incidence of fraud - and its cost - is on the increase in Ireland. These more challenging economic circumstances have led to increased vulnerability to fraud in organisations, large and small.

Directors have a special role to play in fighting fraud. Perhaps the most important role is in demonstrating an appropriate 'Tone at the Top'. This must reflect their determination to operate to the highest ethical standards. After that, the Board needs to oversee effective implementation of preventive and detective safeguards.

Fraud Alert provides an excellent starting point in raising awareness, along with practical measures to prevent and detect fraud. The combined efforts of directors, managers and staff can play a major role in reducing the cost of fraud to Irish organisations.

I would like to acknowledge the assistance we have received from many people and organisations in updating this document.

**Rónán Murphy**  
Senior Partner  
PricewaterhouseCoopers

# CONTENTS

<b>FRAUD - WHO CARES?</b>	<b>1</b>
<b>FRAUD 101 - KEY THINGS YOU NEED TO KNOW</b>	<b>2</b>
<b>⚠ HIGHLIGHTS</b>	
EXAMPLES OF FRAUD IN IRELAND	
TYPES OF FRAUD	
WARNING SIGNS	
<b>WHAT CAN I DO TO PREVENT FRAUD?</b>	<b>8</b>
<b>⚠ HIGHLIGHTS</b>	
PRACTICAL STEPS FOR EVERYONE	
FRAUD ALARM - THE PLAN FOR YOUR ORGANISATION	
<b>DETECTION</b>	<b>12</b>
<b>⚠ HIGHLIGHTS</b>	
FRAUD INCIDENT PLAN	
<b>INVESTIGATION AND PROSECUTION</b>	<b>15</b>
<b>RECOVERY</b>	<b>17</b>
<b>WHERE CAN I GET FURTHER INFORMATION?</b>	<b>18</b>

Published by An Garda Síochána/ PricewaterhouseCoopers.

ISBN 978-0-9564401

© 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.



# FRAUD - WHO CARES?

## "FRAUD COSTS YOU"

## "FRAUD COSTS EVERYONE"

### What is fraud?

In the broadest sense, fraud is intentional deception made for personal gain or to cause damage or loss to another person.

Fraud can take many forms including: theft, deception, fraudulent financial reporting, making off without payment, unlawful or unauthorised use of a computer, false accounting, possession of certain articles intended for use in fraud, handling stolen property and other proceeds of crime, forgery, money laundering, counterfeiting and corruption.

### Who should read Fraud Alert?

This publication is intended to provide a broad understanding of fraud, the obligations of various individuals and the measures that can be taken to prevent and detect fraud.

Often it is only after we have become victims of fraud that we become concerned with its prevention and detection. Everyone is vulnerable to the risk of fraud. For an organisation, a major fraud could put it out of business.

We protect our homes and our cars with alarms, yet most Irish organisations do not have a proper 'Fraud Alarm'. Individuals, too, are failing to take simple steps that could protect them from losses and the emotional upheaval of coping with a fraud.

The social and economic damage caused by fraud is immense. Although fraud by its nature is concealed, it is not a victimless crime. Fraud costs everyone. In insurance fraud, for example, everybody's premium for insurance is increased in order to reflect the cost of fraud.

Whether you are a director, a manager, employee or a member of the public, Fraud Alert contains advice for you.

### What are your responsibilities?

There are a wide variety of obligations under Irish laws and regulations in relation to fraud. Some of these include mandatory reporting (even where you may have only 'a reasonable suspicion'). Penalties are varied, up to and including a prison sentence.

This is a complex area and you should seek expert advice.

### Why you need to read Fraud Alert?

Fraud Alert will improve your awareness of the threat posed by fraud – both to you, as an individual, and to your organisation. It provides the practical steps you can take to prevent fraud. It tells you what to do should you discover a fraud and identifies where you can get further information.

### What should you do having read Fraud Alert?

After reading this publication, don't hesitate: take action! Decide how you should apply what you have learned to your own circumstances. Tailor the suggestions to ensure that the actions you take will address your particular vulnerabilities. If in doubt, seek expert advice.



# FRAUD 101 - KEY THINGS YOU NEED TO KNOW

## How much fraud is there in Ireland?

A fraud is being committed as you read this publication. Many Irish organisations, whether they realise it or not, have been a victim of fraud. The total cost of fraud in any one year cannot be measured with any certainty, and may run into hundreds of millions of euro.

The one feature common to all frauds is that unscrupulous people take advantage of unsuspecting victims. You should not underestimate the time and trouble would-be fraudsters will take to steal from you. Here are a few examples to encourage you to be on guard.



## EXAMPLES OF FRAUD IN IRELAND

### 'Pyramid' scheme

An Irish businessman held himself out as an investment advisor and convinced friends and associates that he could gain an excellent return on monies invested. The fraudster used any new money 'invested' with him to pay returns to other investors until the scheme collapsed. Investors' losses amounted to more than €4 million.

### Conspiring employees

An individual working in a financial institution colluded with another person to fraudulently transfer a long term investment product to a new address. He pretended to be the policy-holder and cashed in the investment, sharing the proceeds with his co-conspirators. The fraud was discovered when the real policy holder rang to enquire about his investment. The loss amounted to €150,000.

### Abuse of power

A senior company executive set up a bogus company in the Far East and issued false invoices, claiming to have carried out work for his employer. He submitted the invoices and used his position to get staff under his direction to authorise payment of the bogus invoices contrary to company policy. The fraud cost the company in excess of €2 million.

### Hi-tech data theft

An organised criminal gang from the UK stole PIN Entry Devices from retail stores across the UK. They altered the devices to capture customers' personal data and PIN numbers which were passed electronically to a foreign web site. Masquerading as service engineers, gang members replaced original devices with the compromised devices in Irish retail outlets. By doing this, they could fraudulently obtain customer details as well as obtain new devices to compromise. Fortunately, close cooperation between GBFI and retailers affected, detected this threat and prevented what could have been substantial losses.

### Exploiting system flaws

A data entry clerk working for an international company discovered that by cancelling purchase invoices they automatically became due for payment again. The employee reactivated dormant accounts and changed the bank account details to bogus accounts he had set up. The funds in respect of the reissued invoices were then fraudulently transferred to these accounts. These offences occurred over a six month period and resulted in losses in excess of €259,000.



### Who commits fraud?

A fraud can be perpetrated against an organisation by any one of a diverse range of individuals including: employees, management, directors, contractors, suppliers, customers, consultants, shareholders, as well as strangers and opportunists.

Trust alone is not a control. While trust is essential for everyday life, fraud inevitably results from a breach of trust. Managers and directors, beware!

The typical corporate fraud is committed by a male member of senior management aged over 35 years, who has been with the organisation for more than five years. Although a single fraudster acting alone is more common, collusion with internal and external parties also occurs. This may happen where a system of internal control needs to be circumvented to commit or conceal the fraud.

Length of service is one of the most salient characteristics in the profile of a typical fraudster. This gives the individual the opportunity to identify weak controls and lax business processes that are open to abuse.

While it is not possible to predict who will commit a fraud, a recent survey by PricewaterhouseCoopers reveals some common traits that motivate fraudsters:

- Financial incentives/greed (57%)
- Low temptation threshold (44%)
- Maintaining a lifestyle unsupported by their salary (36%)
- Career disappointments (12%)
- Prospect of being laid off or made redundant (8%)

The risk of fraud is highest when three factors converge:

- Motive (for example, mounting personal debts)
- Opportunity (for example, lack of rigorous financial controls over payments)
- Rationalisation (for example, "I'm only taking what I'm entitled to")



Fraud is a criminal offence. People who commit fraud are criminals and are liable to prosecution in the same way as persons who commit any type of crime. However, the fact that the fraudster was a trusted employee can sometimes give the crime an 'air of respectability'. In truth, it is this sense of betrayal by an associate or colleague which often leaves the most serious emotional trauma for the victim or organisation defrauded.

### Who is at risk from fraud?

Every individual and every category of organisation are potential victims – from the largest public sector bodies processing revenue, social welfare and grant payments, to banks, insurance companies and private sector organisations, large and small. The fraudster will take advantage wherever and whenever he can. In addition to theft and deception, the main types of fraud and how they are committed are described overleaf.

# fraud /frɔ:d/

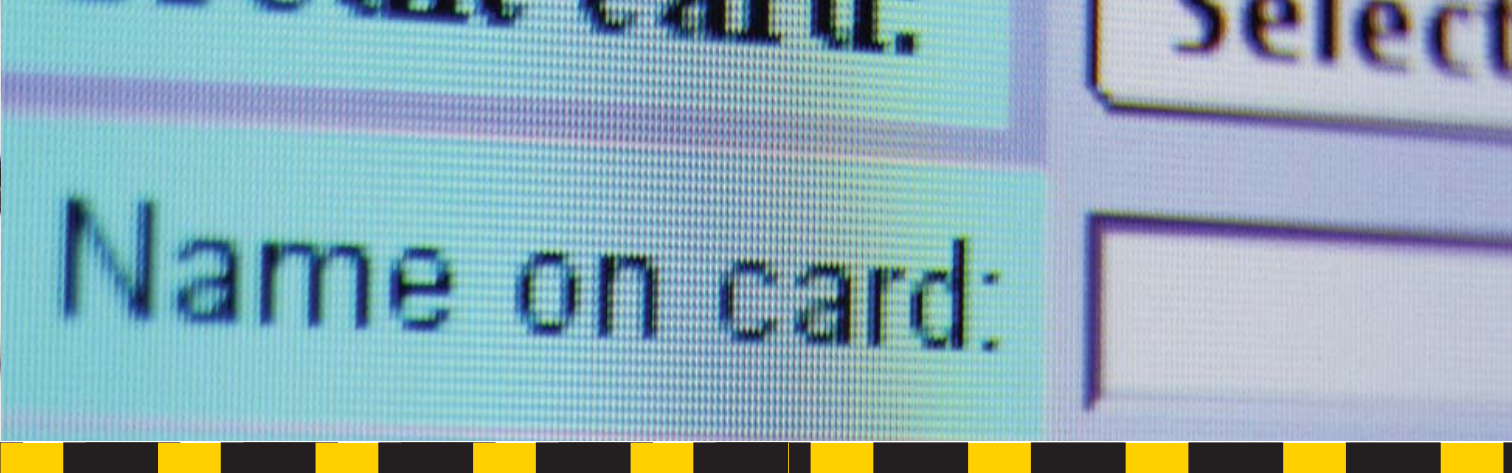
## tended to result

### thing inten

## ! TYPES OF FRAUD

Type of fraud	How it is committed
Advance Fee Fraud	The criminal offers the victim a 'windfall' in return for some small advance payment to 'hook' the victim. Examples are bogus lottery schemes, requests for assistance to transfer huge sums from dormant accounts and unsolicited offers of investment opportunities.
Bribery and Corruption	<p>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.</p> <p>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.</p>
Cheque and Credit Card Fraud	<p>Cheque fraud - Cheques are stolen (for example, by concealing the removal of individual cheques from cheque books), reproduced, or the amount or payee is altered for the fraudster's purposes.</p> <p>Identity theft on cards/stolen card fraud – a criminal uses fraudulently obtained personal information to open or access card accounts in the victim's name or uses a stolen card to obtain goods and services.</p> <p>Counterfeit card fraud (Skimming) – a counterfeit, cloned or skimmed 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 re-coded. Victims are often unaware of such fraud until a bank or credit card statement arrives, showing purchases they did not make.</p> <p>Card-not-present (CNP) fraud – conducted over the Internet, by telephone, fax and mail order. Criminals obtain card details through theft or by copying details during a transaction. It is now the largest type of reported fraud.</p>
Computer Crime (including hacking)	<p>Computer-related crime means a crime in which a computer is used as an aid to commit the crime.</p> <p>Computer-specific crime is where the computer or the data on the computer is the object of the attack. The common term 'computer hacking' falls into this category. It includes destruction of or unauthorised access to a computer system or the information stored on it.</p>
Currency and Other Counterfeiting	<p>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.</p> <p>Other counterfeiting covers a wide range of fraudulent activity including: software piracy, copyright infringement (especially music and film), illicit pharmaceutical manufacture, fake luxury goods and clothing, breach of other intellectual property rights and more.</p>





## TYPES OF FRAUD (CONTINUED)

Type of fraud	How it is committed
False Accounting - including Fraudulent Financial Reporting	<p>The falsification, concealment or destruction of accounting records, for example, by using fictitious employees or companies. It is commonly used as a way to trick people into parting with money or other property, or to cover up what has already been done by falsifying an account. It includes the use of records to support bogus Revenue refund claims.</p> <p>This type of fraud includes fraudulent financial reporting, the intentional preparation of misleading financial statements. Fraudulent reporting can result from distorted records, falsified transactions, or misused accounting principles.</p>
Investment Fraud	<p>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 misappropriates the funds entrusted to them.</p>
Money Laundering/ Terrorist Financing	<p>Money laundering is the process by which criminals disguise or conceal the true origin of the proceeds of their criminal activities thus facilitating the generation of wealth from crime. Terrorist financing involves using funds from whatever source for use in terrorist activity.</p>
Mortgage/Credit Fraud	<p>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 overvalued or does not exist at all. Cases sometimes involve professionals who fail to register the owner's or a financial institution's interest in a property and take out further loans secured on the property for their own unlawful benefit.</p>
Phishing and Identity Theft	<p>'Phishing' is a form of online fraud where fake emails or websites, supposedly from a legitimate company, are used to obtain your confidential bank and/or credit card account details. Identity theft occurs when a criminal uses fraudulently obtained personal information to open or access bank accounts in someone else's name.</p>

### Current challenges in tackling fraud

The level of fraud risk is constantly shifting. Improvements in IT security and technologies, for example, chip and PIN, provide improved protection. Conversely the ever increasing use of new technologies provide additional avenues for innovative fraudsters.

Furthermore, there is an increased risk of identity theft resulting from the large amounts of data and information being shared and stored in new ways, for

example, personal information on social networking sites, customer information held on laptops, personal digital devices and memory sticks.

Economic conditions also affect the level of fraud risk. As people lose their jobs, and those still in employment feel ever more threatened, the pressure to commit fraud will increase. Similar temptations may arise for organisations experiencing cash flow problems; for example, by withholding monies properly payable to the State.



## WARNING SIGNS

### Warning signs for organisations

#### Unusual behaviour

- Lavish lifestyle out of keeping with the person's known resources
- Employees not taking holidays – it could mean they can't afford to have someone else see what they are doing
- Sudden changes in work habits/lifestyles, for example, employees working very long hours
- 'Larger than life' personalities tending towards autocratic behaviour
- Extensive and unnecessary foreign travel
- Frequent changes of professional advisers
- Customers who, for no apparent reason, won't deal with anyone other than a particular member of staff
- High turnover of staff

#### Poor administration and weak systems of internal control

- Inadequately controlled cash transactions
- Loss of accounting records and/or unavailability of financial information for no good reason
- The same staff keeping records and being responsible for safeguarding the assets recorded
- Not knowing your customer, for example, where a mobile phone number is your only point of contact

#### Unusual circumstances

- Unusual transactions with connected parties
- Unexplained differences between accounting records and third party documentation, for example, suppliers' statements
- Payments for services (for example, to agents or consultants) that appear excessive in respect of the service provided
- Unexplained swings in cash business completed by salesmen or agents
- Unexpected drop in margins, or increase in expenses, that cannot be explained
- Unexplained change to customer address or bank details, particularly dormant accounts or reactivated accounts



## Warning signs for individuals

- Offers to take part in a 'get rich quick' scheme, for example, lotteries, pyramid schemes, chain letters
- Unsolicited telephone calls about investing. Be sceptical. If something sounds too good to be true, it usually is
- Someone asking you to send cash or transfer money to them by overnight express, the Internet, mail, wire transfer or any other method. A common ruse is where the criminal sends on a cheque in excess of the agreed amount for some item you have offered for sale and asks you to forward the balance after keeping an additional commission for 'helping him out'. The criminal's cheque then turns out to be worthless
- Unsolicited telephone calls or emails asking you to update or validate your personal information, for example, user name, password, credit card number or bank account number
- Individuals invading your personal space while you enter your PIN number at an ATM or a PIN entry device in a shop or restaurant
- Web-based job advertisements offering easy cash for acting as a 'mail depot' for receiving goods or providing bank account facilities for unknown funds
- Online auctions offering items at knock-down prices. Be sure you know who you are dealing with and what exactly you are buying – beware of cleverly worded small print

Remember that you cannot trust information just because you find it on a website or receive an email.

Note: these are not exhaustive checklists of warning signs. Other conditions can occur that could put you on notice that the risk of fraud is high.

# WHAT CAN I DO TO PREVENT FRAUD?

**"CORRUPTION WAS RIFE,  
AND LEGISLATION ABOUNDED"  
TACITUS**

## **'Tone at the Top' – get it right!**

The Roman Senator and historian, Tacitus, contended that the mere existence of rules was insufficient to prevent wrongdoing. The incidence of recent frauds proves the point.

'Tone at the Top' refers to the ethical atmosphere that is created in the workplace by the organisation's leadership. If that tone upholds ethics and integrity, employees will be more inclined to uphold those same values. If management appears unconcerned with ethics and focuses solely on the bottom line, employees may be more prone to commit fraud because they feel that ethical conduct is not a priority.

You can use this simple question to help assess the 'Tone at the Top': "How much fraud is considered acceptable in the organisation?"

Honest answers will help prepare senior management and directors to focus on how they deal with problems of employee or manager misconduct.

Directors and managers must ensure that the 'Tone at the Top' in their organisation is appropriate, that it reflects the values of the organisation. Some of the practical measures they should take are shown opposite.

## **Establishing the right 'Tone at the Top'**

- **Communicate what is expected of employees** – use a code of ethics, formal training and frequent communications to reinforce the organisation's policies
- **Screen job applicants** – one of the easiest ways to establish a strong moral tone for an organisation is to hire morally-sound employees. Conduct thorough background checks on all new employees, especially senior personnel
- **Get employees to confirm compliance** – insist on all employees confirming in writing that they understand the organisation's policies and procedures and are compliant with them
- **Lead by example** – demonstrate commitment to ethics through both words and actions
- **Encourage reporting of violations (often referred to as whistle-blowing or good faith reporting)** – reassure employees that reporting mis-deeds is valued by management
- **Reward integrity** – ensure employees know that the bottom line is not the only measure of success
- **Announce remedial measures** – after fully resolving fraud incidents, make sure employees are told about them, the sanctions applied and the remedial actions taken
- **Ensure that specific measures are taken to prevent and detect fraud** – this would normally include a Fraud Prevention Plan ('Fraud Alarm') and Fraud Incident Response Plan

# PRACTICAL STEPS FOR EVERYONE

## **The big picture (for directors)**

- Understand your legal responsibilities as a director in relation to fraud
- Establish an ethical 'Tone at the Top'
- Establish preventive measures with an appropriate 'Fraud Alarm' for your organisation
- Ensure identified risks and weaknesses in internal control, including specific fraud risks, are rectified promptly
- Prepare an 'Incident Response Plan' that will allow the organisation to react decisively should a fraud come to light
- Implement appropriate whistle-blowing procedures
- Ensure the board gives appropriate attention to fraud at board meetings

## **Personal precautions (whether at work or otherwise)**

- Exercise caution with 'Card Not Present' payments and with cheques (especially third party cheques or cheques outside the cheque guarantee scheme protection)
- Be vigilant about protecting your personal information – to avoid identity theft
- Protect your PINs but don't write them down
- Watch out for counterfeit currency
- Be on guard against attempts to steal your account and other details ('phishing')

## **The detail (for managers and staff)**

- Ensure all employees receive appropriate ethics and anti-fraud training
- Integrate fraud risk management into the organisation's risk management processes
- Encrypt sensitive electronic data
- Report all information loss to the relevant authorities
- Use passwords to protect documents and send details of the password by independent means such as by telephone
- Secure all wireless networks and make everyone aware of essential security precautions
- Ensure that sensitive duties are segregated
- Adhere to the system of internal control (both manual and computerised) and challenge its adequacy to address fraud risks
- Look out for the warning signs that employees may be engaged in fraudulent activity
- Make appropriate use of spot checks and data mining
- Beware of 'tipping off' any suspected fraudster prior to reporting to management
- Report all incidents of suspected fraud to an appropriate level of management

## **Experts**

- If you have a special role already in relation to fraud (as compliance officer, risk manager, internal auditor, anti-money laundering officer, etc.), check the section on further information at the end of this document for useful links





## FRAUD ALARM - THE PLAN FOR YOUR ORGANISATION

A single fraud can be crippling, yet many organisations do not have procedures in place to help reduce the risk of fraud and loss to the organisation.

The following are the elements of an effective Fraud Alarm:

### Fraud policy

Drafting a fraud policy is the first step in protecting your organisation against fraud, acting as an instruction manual for installing your Fraud Alarm. The fraud policy articulates the organisation's attitude to fraud, commitment to ethical standards of behaviour and to a recrimination-free culture for whistle-blowers. The policy must be communicated to and adopted by all members of the organisation. Directors and managers must communicate a clear message that fraud will not be tolerated and that wrongdoers will be prosecuted. A practical step to reinforce the fraud policy is the development and promotion of a code of conduct.

### Fraud risk assessment

When installing your Fraud Alarm you need to assess your organisation's high-risk and vulnerable areas, in the same way as you would when installing a burglar alarm. The main objective is to prevent fraud or to minimise the risk of loss (financial and reputational), arising from fraud. The assessment will be specific to your organisation, however common areas of concern include: theft of cash or inventory, unauthorised electronic payments, inappropriate use by employees of company assets and theft of sensitive information. The fraud assessment should be integrated into your

organisation-wide risk management programme and should be re-visited on a periodic basis in order to maintain its relevance.

### System of internal control

Implementing a robust system of internal control is like putting the batteries in your Fraud Alarm. Fraud losses will not be avoided unless a targeted set of preventive and detective controls is implemented. Internal controls are the mechanism by which management safeguards assets and other valuable resources. They include a wide range of internal and external checks. Controls should not only operate but should also be seen to be in operation in order to deter potential fraudsters.

The fraud risk assessment will identify areas of specific focus when designing your system of internal control. Each fraud risk identified should be addressed by a suitable control. For example, if you operate a cash business such as a supermarket, till operators should be required to reconcile their takings to the till roll on a daily basis. A pattern of cash overs or unders can alert management to the possible occurrence of fraud.

Irrespective of obligations under law and regulation, all organisations should implement whistle-blowing arrangements appropriate to their needs. Whistle-blowing can provide an important safeguard that allows suspected or actual, irregularity or fraud to be safely brought to senior management attention in the event that established control mechanisms fail to do so. This is a complex area and you should seek expert advice to ensure you implement appropriate arrangements.

# "AWARENESS THAT YOU HAVE FRAUD PREVENTION MEASURES IN PLACE IS, IN ITSELF, A DETERRENT"

## Assurance - four lines of defence

Directors should seek assurance from four sources:

- Managers of business units
- Quality assurance functions, which operate across individual business units (such as compliance, risk management etc.)
- Internal Audit, who independently examine various aspects of the entire organisation
- External Audit, who are obliged to address certain aspects of fraud as part of their audit

Assurance is not the same as certification – management cannot obtain complete assurance that all incidents of fraud will be prevented/detected by the system of internal control. It is the responsibility of directors to constantly challenge the systems in place and to ensure that they obtain sufficient levels of assurance from these four lines of defence.

## Communications and Training

Employees must be kept informed about the organisation's Fraud Alarm and their responsibilities under it. Annual confirmation of compliance with the fraud policy will further strengthen the Fraud Alarm. A continuous programme of communications and training will raise the necessary awareness to act as a deterrent and contribute to an antifraud culture.

## Retention of information as evidence

Without information, fraud cannot be prevented, detected or investigated. What was information yesterday can become vital evidence tomorrow.

Evidence can include ledgers, bank statements, invoices, cheque stubs, pens, ink, CCTV records, security logs, and more. All of these can yield important information – evidence that is essential to your investigation of a case.

It is typically only after a fraud has occurred that steps are taken to identify and retain evidence. However, at this point it may be too late. In many cases, crucial evidence within logs and records has not been kept, has been overwritten or has not been protected from unauthorised access.

You should take steps to identify vital records, electronic and otherwise, and ensure that appropriate controls are in place to preserve these records for possible use in any investigation.

## Information sharing

Sharing information on suspected frauds among organisations within an industry can be effective in preventing others from becoming victims. Within the insurance industry, a shared claims database has proved effective in the fight against fraud.

Caution must be exercised to ensure that personal data is appropriately protected: it must be used only for the purpose for which it was collected and with the informed consent of the data subject. In particular, the sharing of personal data about the commission or alleged commission of criminal offences must be provided to An Garda Síochána only. If in doubt it is advisable to seek expert advice in this area.

# DETECTION



## FRAUD INCIDENT PLAN

Reacting quickly to the discovery of fraud is the key to recovering your losses and catching the fraudster. Implementing a structured Fraud Incident Plan is essential for a speedy reaction. Below is a basic blueprint for your organisation's Fraud Incident Plan. The plan will need to be tailored to meet your particular circumstances. In particular, special arrangements should be made to address 'serious incidents'.

### Your Fraud Incident Plan should:

- Indicate who is responsible for taking action – failure to make this clear could prejudice successful investigation
- Be approved at the highest level in the organisation
- Be capable of being put into operation inside or outside of business hours
- Include a process for regular review to ensure it is kept up to date

Individuals named within the plan should receive appropriate training. The existence of the plan should be communicated within the organisation.

### Prevent any further loss

If it is obvious who the likely perpetrator is or how the fraud has been carried out, measures must be put in place to prevent any further loss and to deny the suspect any opportunity of destroying or discarding vital evidence. Areas where evidence may be found include the suspect's desk, computer, filing cabinet, personal lockers, and company-supplied car, phone, or personal digital assistant.

Regardless of the urgency to take action, it is essential to have due regard to natural justice, fair procedures,

employment law and the suspect's employment contract. It may be necessary to suspend accounts, revoke access (to buildings and computer systems) and to temporarily suspend those suspected of wrongdoing, pending investigation.

### Preserve evidence

If you think you will need to produce evidence, take every possible measure to preserve it. Keep detailed notes as you go – these 'contemporaneous notes' will be vital in later stages of the investigation.


There are important guidelines you should follow in locating and securing all relevant evidence. In particular, documentary evidence must be preserved in the same state as you find it. 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 destroying vital forensic evidence. The safe custody of documents and exhibits is vital - it must be proved that no unauthorised persons gained access to them.

No marks should be made on the original document. If the document is challenged in court it will be necessary to prove its integrity. The fewer people who have access to the documentation, the better. If court proceedings are to ensue, the documents should be available in their original form for the courts; otherwise, copies will only be acceptable if authenticated and the absence of the originals can be explained to the satisfaction of the court.

# "IF NOT REPORTED, THE FRAUDSTER WILL STRIKE AGAIN"



Seek  
assistance



Deal with  
suspected  
wrongdoers

In relation to electronic evidence any interference with the computer may alter or erase essential evidence. Seek expert advice.

## Seek assistance

When suspicions or facts of a fraud are brought to your attention, management must make an initial decision on what course of action is appropriate.

### Deciding your course of action:

#### Criminal

if you suspect a crime has been committed, you must address your obligation to report the matter to *Án Garda Síochána*

#### Regulatory

regulatory compliance may require immediate reporting and other actions

#### Civil

you may wish to consider the remedies available under civil law (such as contract law)

#### Internal

you may wish to investigate a breach of internal policies and procedures

#### Moral

finally, even if none of the above apply, you may feel obliged to act in order to preserve and reinforce the 'Tone at the Top' for your organisation

As an investigation can be time-consuming and expensive, you should consider, at the very beginning, the outcome you are seeking from the investigation. For example, even where it may be difficult to gather the evidence, you might still proceed simply to 'send a message' that reinforces the 'Tone at the Top'.

Not reporting fraud can have unforeseen consequences as it sends a signal to the fraudster, and indeed others, that further fraud can be committed with impunity. Actual or suspected fraud should always be reported to senior management. If fraud goes unreported, not only will your business be affected but so too will the next organisation that the fraudster targets, where he may commit a more serious fraud offence and that next organisation could be you.

At this stage the assistance and advice of local Gardaí can be sought and, where appropriate, a formal report of fraud can be made.

If your fraud complaint is not criminal in nature there are others who may be able to assist you:

- Professional advisers (for example, accountants, auditors, lawyers, forensic experts, risk specialists)
- Regulatory bodies (for example, Central Bank, Financial Regulator, ComReg, Regtel)
- Consumer protection agencies (for example, National Consumer Agency, European Consumer Agency)
- Small Claims Court
- Ombudsman bodies
- Office of the Director of Corporate Enforcement
- Registrar of Friendly Societies
- Competition Authority



### Deal with suspected wrongdoers

In the initial stages of an investigation the main priority is to confirm or eliminate potential suspects and to secure all available evidence. A person suspected of crime is not obliged to incriminate himself and, as such, he is under no obligation to answer any questions put to him.

In criminal prosecutions, the use of improper procedures may render confessions inadmissible. As this is a very broad and complex area of law and procedure, it is better left to the Gardaí who are trained and experienced in interviewing and dealing with suspects.

If management decide to interview a suspect, they should proceed with caution. Tactically, a badly prepared interview could do more to educate the fraudster as to how much or little is known about their wrongdoing and thereby hinder further investigation, whether a disciplinary hearing or criminal prosecution.

The Fraud Incident Plan should set out clear policies, based on professional advice, on how best to interview a suspect to ensure fair procedures, natural justice, compliance with employment law and the person's contract of employment.

### Technology and skills for effective detection

While the Gardaí understand the need to find quick answers, experience has shown that investigations carried out by inexperienced personnel can cause problems, for example, in the reliability and admissibility of evidence taken.

In recent years great advances have been made in the field of forensic science and it is now possible to glean valuable evidence using forensic examination or specialist approaches such as pattern identification, face recognition or data mining.

#### Forensic tests include:

- Forensic computer analysis
- Finger print analysis
- Identification of handwriting
- Comparison of inks
- DNA analysis
- CCTV footage
- Identifying indentations
- Interrogation of computer file back-ups

Always seek expert advice to protect your interests.



# INVESTIGATION AND PROSECUTION

If your investigation is criminal in nature the Gardaí will be responsible for the investigation. This section describes the process involved. For other investigations you should seek expert advice on how best to proceed.

## Reporting a fraud to the Gardaí

Once a fraud is reported to the Gardaí (either at your local Garda station or directly to the Garda Bureau of Fraud Investigation) an initial assessment is made and if there is a breach of criminal law an investigation follows. Information provided is always treated with the utmost confidentiality.

The Gardaí are obliged to carry out a full and thorough investigation into all allegations where a criminal offence is disclosed. You should work with the members of An Garda Síochána but at the same time remember the Gardaí retain control of the scope and range of a criminal investigation. The nature of the case will determine the resources given to investigating your case, whether at local level or by the GBFI.

The Gardaí can carry out investigations into allegations of crime which have occurred within the State. Where the crime has occurred outside of the jurisdiction, the Gardaí will forward complaints via Interpol to the relevant Police force(s).

## Carrying out the investigation

Investigation of fraud is time-consuming and requires specialist skills. Most fraud investigations are carried out by plain clothes Gardaí who are trained in relevant investigation techniques. They are accustomed to working discreetly and would not normally reveal their identity to junior members of staff in your organisation.

All Garda fraud investigations commence by taking

a formal written statement of complaint. The Gardaí will take possession of any original/copy documents referred to in the statement for use in the investigation, and ultimately as evidence in any subsequent court proceedings. Frequently, the Gardaí will require formal written statements from more than one person in the organisation, depending on their role and responsibilities.

They will then carry out a similar exercise with any third parties who may be in a position to assist in the investigation. Depending on the nature of the material sought, applications to the courts may be necessary to have appropriate information and documentation released.

## Interviewing the suspect(s)

Once the Gardaí have completed all their enquiries, they will generally interview the person(s) suspected of fraud. In certain circumstances this may involve the arrest and detention of the individual for a specified period of time.

## Length of investigation

A number of factors have a bearing on the length of an investigation including: the complexity of the case, the number of witnesses and the volume of documents. Preserving evidence and providing the fullest information at an early stage, greatly speeds up the process.

## Prosecution - referral to DPP

At the conclusion of an investigation all the findings will, in the majority of cases, be referred to the Director of Public Prosecutions (DPP), the independent legal



officer responsible for all criminal prosecutions in the State. The DPP examines the Garda file on the case and decides whether a prosecution should proceed.

### Will I have to attend court?

If the DPP concludes that a criminal prosecution is merited, the suspect is then charged and brought before the court. In the initial stages of court proceedings your attendance, and that of any prosecution witnesses, is not usually required. Witness orders will be issued well in advance of the trial date. Witnesses will be required to give their evidence in open court and can expect to be cross examined by the defence.

### What is the Garda press policy?

Garda press policy is implemented by the Garda Press Office. It is Garda policy - as a crime prevention strategy - to inform and/or alert the public about possible criminal activity which may affect them. However, it is Garda policy not to:

- Discuss individual investigations
- Name individuals or organisations under investigation, or
- Give information to the media which may in any way hinder the proper investigation of a case

Unnecessary media attention is not in the interest of the Garda investigation or the organisation involved. The main concern is that a full and fair investigation should take place and that media attention will not prejudice a fair trial, or have an adverse effect on an individual or organisation under investigation.

### How should I deal with the media?

Before a decision is made to release information, consult the Gardaí. To ensure uniformity in the release of information, only one person should deal with media enquiries.

Any release of information should be brief and to the point. The information should not include any precise details of how the crime was committed. While it could include the fact that the matter has been reported to the Gardaí, it should make no reference to any past, present or future Garda activity. The last thing you want to do is to give the criminal an advantage or reduce your chances of a successful outcome.

### What information might get into the public domain?

The media and the public have an increasing interest in all forms of crime - fraud is no exception. Fraud involves deception and this immediately gives a 'human interest' angle to fraud cases. All court appearances are in public and accordingly, any new major fraud related crime is newsworthy. The influence and impact of blogs and social networking sites in spreading information about a case should not be underestimated.

### Are there special actions I need to take to protect the interests of others?

In limited circumstances, usually for crime prevention reasons, the Gardaí may want to give publicity to a type of fraud at an early stage to put others on guard and thus prevent further frauds. In these cases only the generic type of fraud is publicised, not the details of the organisation affected.

# RECOVERY

## "REMEMBER THERE ARE CIVIL REMEDIES"

### Do I have civil remedies?

The primary objective of the Garda investigation is to bring the fraudster to justice, rather than to recover any funds. The Garda investigation, by tracing the money, may well facilitate such recovery. In practice, civil remedies often offer the most effective means for the recovery of misappropriated funds.

This is an area where legal advice should be sought and reflected in the Fraud Incident Plan.

Steps you can take to recover funds include tracing and freezing. These actions must be taken quickly and effectively and are areas where specialist legal and accountancy advice should be sought.

### What options are there around tracing and freezing assets?

Once a fraud has been discovered you should follow the trail of the stolen funds, preserving all evidence. Court orders may be used to overcome any barriers that get in the way of the tracing process.

As soon as all or some of the funds have been traced it is possible to take legal steps to freeze the funds. Freezing of funds, whether in Ireland or abroad, can be achieved through the civil process; however, recovery of funds may take some time.

If the misappropriated funds are located in another jurisdiction freezing the funds may be more complicated. However, in many foreign countries examining magistrates have powers to freeze suspect funds, pending a full investigation.

### How long will it take to recover funds?

The length of time it takes to recover funds depends on many factors including where they are located, and the form they are in. Funds lodged directly to a bank account will take less time to recover than funds converted by some means to disguise their origin, for example, purchase of property.

Where funds have come into the possession of innocent third parties, the matter becomes more complex and may require the intervention of the courts to establish legitimate ownership. Further complexity may be added by cross border transactions. Because of the many factors involved it is not possible to state how long it will take to recover funds. In all cases, legal advice should be sought.

### What powers do Gardaí have to seize funds?

The Gardaí and the Criminal Assets Bureau have powers to seize funds suspected to be derived from the proceeds of crime. These powers are not exercised lightly and are used only after careful consideration.

If you can establish legitimate ownership of funds seized by Gardaí or the Criminal Assets Bureau you may apply to the courts to recover your funds.

# WHERE CAN I GET FURTHER INFORMATION?

## An Garda Síochána

If you require an instant response, dial 999 or 112 and ask for the Gardaí. Remember, however, that this is an emergency service. This approach is not usually appropriate for reporting a serious fraud offence and should only be resorted to when urgent action is required such as the arrest of a fraudster, the recovery of stolen property or to prevent the destruction of vital evidence.

Should you be concerned that a fraud may have been perpetrated in your organisation, contact your local Gardaí, who may, if appropriate, call on the assistance of The Garda Bureau of Fraud Investigation, Harcourt Street, Dublin 2.

## Other Garda contact numbers

The Garda Bureau of Fraud Investigation: 01-666 3776/3706

Garda Confidential line: Freephone: 1800 666 111

Crimestoppers: Freephone: 1800 250 025

Internet: <http://www.garda.ie>

## Useful links

Irish	
Fraud Alert	<a href="http://www.pwc.com/ie/fraudalert">www.pwc.com/ie/fraudalert</a>
Central Bank & Financial Services Authority of Ireland	<a href="http://www.financialregulator.ie">www.financialregulator.ie</a>
ComReg	<a href="http://www.comreg.ie">www.comreg.ie</a>
Regtel	<a href="http://www.regtel.ie">www.regtel.ie</a>
National Consumer Agency	<a href="http://www.consumerconnect.ie">www.consumerconnect.ie</a>
Ombudsman	<a href="http://www.ombudsman.gov.ie">www.ombudsman.gov.ie</a>
Office of the Director of Corporate Enforcement	<a href="http://www.odce.ie">www.odce.ie</a>
Competition Authority	<a href="http://www.tca.ie">www.tca.ie</a>
Chartered Accountants Ireland	<a href="http://www.charteredaccountants.ie">www.charteredaccountants.ie</a>
Information Systems Audit and Control Association	<a href="http://www.isaca.ie">www.isaca.ie</a>
Institute of Internal Auditors	<a href="http://www.theiia.org">www.theiia.org</a>
Data Protection Commissioner	<a href="http://www.dataprotection.ie">www.dataprotection.ie</a>

## PricewaterhouseCoopers

For help with strengthening your defences against fraud, testing controls or immediate assistance in suspected or actual frauds, contact any of the following:

Bob Semple	01-792 6434 <a href="mailto:bob.semple@ie.pwc.com">bob.semple@ie.pwc.com</a>
Billy O'Riordan	01-792 8592 <a href="mailto:billy.oriordan@ie.pwc.com">billy.oriordan@ie.pwc.com</a>
Ciarán Kelly	01-792 6408 <a href="mailto:ciaran.kelly@ie.pwc.com">ciaran.kelly@ie.pwc.com</a>
Brian Bergin	01-792 8735 <a href="mailto:brian.bergin@ie.pwc.com">brian.bergin@ie.pwc.com</a>

or your usual partner or director contact.

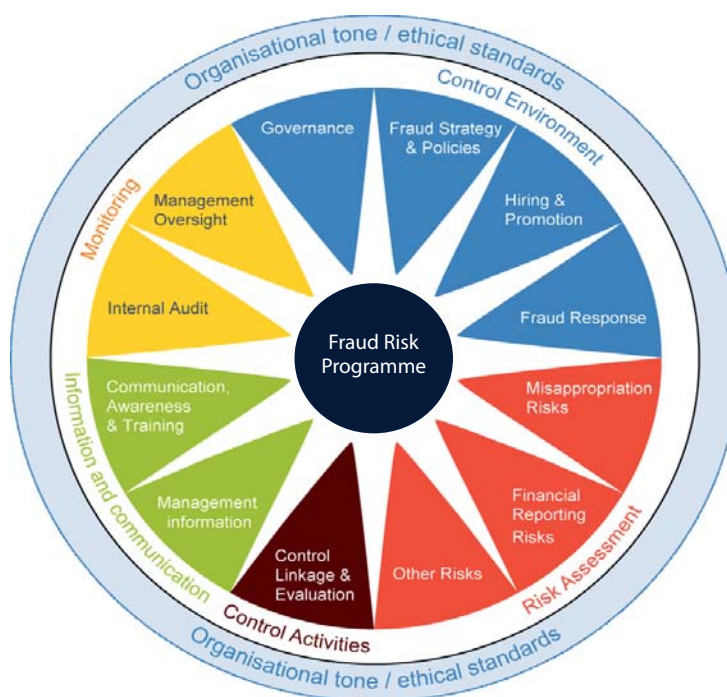
Offices at Dublin, Cork, Kilkenny, Limerick, Galway, Waterford and Wexford.

Internet: <http://www.pwc.com/ie>

Other	
Association of Certified Fraud Examiners (US)	<a href="http://www.acfe.com">www.acfe.com</a>
Interpol	<a href="http://www.interpol.int">www.interpol.int</a>
Europol (EU)	<a href="http://www.europol.europa.eu">www.europol.europa.eu</a>
PwC Fraud Academy (UK)	<a href="http://www.pwc.co.uk/eng/issues/fraud_academy.html">www.pwc.co.uk/eng/issues/fraud_academy.html</a>
Association of Chief Police Officers (UK)	<a href="http://www.acpo.police.uk">www.acpo.police.uk</a>
Financial Services Authority (UK)	<a href="http://www.fsa.gov.uk">www.fsa.gov.uk</a>
Serious Organised Crime Agency (UK)	<a href="http://www.soca.gov.uk">www.soca.gov.uk</a>
Federal Bureau of Investigation (US)	<a href="http://www.fbi.gov/becrimesmart.htm">www.fbi.gov/becrimesmart.htm</a>
Financial Executives Research Foundation (US)	<a href="http://www.financialexecutives.org">www.financialexecutives.org</a>
American Institute of Certified Public Accountants (US)	<a href="http://www.aicpa.org">www.aicpa.org</a>
Department of Justice (US)	<a href="http://www.usdoj.gov/criminal/fraud/fcpa">www.usdoj.gov/criminal/fraud/fcpa</a>



## The PricewaterhouseCooper's Fraud Wheel



In 1992, the Committee of Sponsoring Organisations of the Treadway Commission (COSO) developed a model for evaluating internal controls. This model has been adopted as the generally accepted framework for internal control and is widely recognised as the definitive standard against which organisations measure the effectiveness of their systems of internal control. We have adapted the COSO framework to illustrate some of the key elements of a fraud and integrity risk control framework.

### A selection of relevant PricewaterhouseCooper's publications

- **Economic Crime in a downturn**  
**The Global Economic Crime Survey**  
**November 2009**
- **Global State of Information Security**  
**Survey 2010**
- **Fraud in a downturn 2009**
- **A deeper dive**  
**Protecting Retail & Consumer companies**  
**against fraud and misconduct**
- **The emerging role of Internal Audit in Mitigating**  
**Fraud and Reputation Risks**
- **Key elements of Antifraud Programs and**  
**Controls**





**An Garda Síochána**  
Ireland's National Police Service

**PRICEWATERHOUSECOOPERS** 