National Fraud Authority

# Fraud typologies and victims of fraud

## Literature review

University of Portsmouth

OFFICE OF FAIR TRADING

# Fraud typologies and victims of fraud

## Literature review

**Mark Button**, **Chris Lewis** and **Jacki Tapley**

**Centre for Counter Fraud Studies**,
**Institute of Criminal Justice Studies**,
**University of Portsmouth**

National Fraud Authority

# Contents


03 Executive summary

04 Introduction

06 The characteristics of frauds
06 Mass marketing scams
09 Identity frauds
11 Frauds against small businesses
11 Perpetrators of frauds
13 The techniques of fraudsters

19 The characteristics of victims of fraud
19 Victim typologies
21 Profile of victims
23 Low reporting of frauds
25 Impact upon the victim
26 Plural provision
28 What do victims want?

30 Conclusion

31 Glossary

32 References

35 Appendices
35 Appendix 1
36 Appendix 2

# Executive summary

**This review profiles a wide range of frauds which affect individuals and small businesses. In particular, it looks at mass marketing, identity and small business fraud.**

The review highlights the diversity within fraud including who perpetrates it. The report also shows the level of innovation and skill involved in committing fraud, thus coining the word 'scampreneurs' to describe these criminals.

There are a wide range of techniques used to commit frauds, which can be divided into four areas: victim selection techniques, perpetration strategies, detection avoiding strategies and securing the gains. The latter of which is beyond the scope of this review.

Victim selection techniques include the use of both open and illicit sources of information to target individuals. Typical sources are publicly available marketing lists, directories as well as so called 'suckers' lists of those who have already fallen for a scam.

Perpetration strategies vary according to the specific type of fraud but some of the most common include the use of sound business skills, the latest technology, promoting professional appearances, utilising 'good' sales techniques, seeking small sums of money and operating in a legal hinterland, amongst others.

There are another wide range of techniques specific to identity fraud, ranging from stealing waste to secure personal information to the use of sophisticated software to hack into victims computers to steal personal data.

Fraudsters also use a wide range of techniques to avoid detection. They often operate in jurisdictions where they are unlikely to be bothered by law enforcement. They move locations regularly to avoid detection as well as operating in a legal hinterland and seeking small sums of money.

Significant numbers of people have been the victim or nearly the victim of fraud.

The characteristics of victims, however, do vary. Typologies distinguish differences in their knowledge of the fraud, the degree of co-operation and in the loss.

The profile of victims also varies. For instance, mass marketing fraud does not attract one type of victim. Men, women, the old and the young tend to fall for different variations within this field of fraud.

Another example is identity frauds where research suggests those 26-45 years old, working in a professional occupation, owner occupiers (usually in a detached house), earning over £50,000 (these are 3 times more likely to be victims), and Directors of companies are most at risk.

Identity fraud is generally reported, but mass marketing fraud tends to have very low rate of reporting, often 1 to 3 per cent.

There are a wide range of reasons for low reporting which include: the victim may not know they have been defrauded, they feel partly responsible, the embarrassment, the low financial loss, the ambiguity of the fraud, the attitude of statutory bodies and confusion, amongst others.

There are also major impacts on victims because of the fraud. These include financial losses, loss of employment, emotional impacts, health problems, disintegration of the family, self blame and behavioural changes.

The provision to support victims of fraud compared to other crimes is also much more pluralised and confusing for victims.

There is also research to illustrate some of the things victims want, which include: individual case workers, been kept up-to-date with progress, a more sympathetic approach, better training of staff dealing with victims, better and clearer information, restitution and for the offender to be caught and punished.

# Introduction

**Fraud encompasses a wide range of behaviours that are linked by trickery or deceit with the intention it will culminate in some form of gain.**

It can range from 'internal' frauds where a previously law abiding employee exploits an opportunity to embezzle monies from his/her company to 'external' frauds perpetrated by organised criminals on an industrial scale, such as stealing identities to secure loans. The passage of the recent Fraud Act 2006 has provided some clarity to the crime by defining most of the offences under:

- Fraud by false representation
- Fraud by failing to disclose information
- Fraud by abuse of position

What is clear, however, is that fraud embraces a broad scope of different crimes. This is illustrated further by some of the attempts to produce typologies of the different types of fraud. One of the most comprehensive has been produced by Levi (2008a: 391) and is presented in Table 1.

The list identified by Levi could be expanded with further categories and sub-divisions such is the breadth and diversity of fraud. However, the terms of reference for this review are clearly focused upon fraud against individuals and small firms with particular reference to the following four:

- Mass marketing scams
- Investment frauds
- Identity fraud
- Fraud affecting small businesses

**Table 1**
**Levi's typology of fraud by victim**

| Victim sector | Victim subsector | Examples of fraud |
|---|---|---|
| Private | Financial services | Cheque fraud |
| | | Counterfeit intellectual property and products sold as genuine |
| | | Counterfeit money |
| | | Data-compromise fraud |
| | | Embezzlement |
| | | Insider dealing/ market abuse |
| | | Insurance fraud |
| | | Lending fraud |
| | | Payment card fraud |
| | | Procurement fraud |
| | Non-financial | Cheque fraud |
| | | Counterfeit intellectual property and products sold as genuine |
| | | Counterfeit money |
| | | Data-compromise fraud |
| | | Embezzlement |
| | | Gaming fraud |
| | | Lending fraud |
| | | Payment card fraud |
| | | Procurement fraud |
| | Individuals | Charity fraud |
| | | Consumer fraud |
| | | Counterfeit intellectual property and products sold as genuine |
| | | Counterfeit money |
| | | Investment fraud |
| | | Pension-type fraud |
| Public | National bodies | Benefit fraud |
| | | Embezzlement |
| | | Procurement fraud |
| | | Tax fraud |
| | Local bodies | Embezzlement |
| | | Frauds on Council taxes |
| | | Procurement fraud |
| | International bodies (but affecting the public) | Procurement fraud (by national against other – mainly but not always foreign – companies to obtain foreign contracts) |
| | | EU funds fraud |

# Introduction

The rest of this review will be dedicated to the growing literature that has been published on each of these frauds within the parameters set by the NFA. It is important to note, however, that compared to many other crimes, fraud is relatively neglected by researchers (Levi, 2008b). The focus of the review is the UK, but acknowledges the breadth of information published in North America and Australia, amongst other countries. There is much that can be learnt from this literature given the sometimes common structural conditions and the increasingly global nature of fraud. However, it is important to bear in mind that the characteristics of fraud in other countries can't always be applied directly to the UK without changes.

This review will begin by examining the range of fraud that falls under the four categories. It will also give a brief overview of the fraudsters themselves and an exploration of the techniques used. In the second part of the review typologies of victims will be outlined, followed by a profile of certain types. The review will also examine why there is such low reporting and the impact of fraud upon the victims.

# The characteristics of frauds

**The frauds to be considered in this review are diverse and can be differentiated further. This section seeks to do this by drawing upon the literature available. It then moves on to examine the characteristics of the fraudsters and the techniques used to carry out the frauds.**

## Mass marketing scams

There is no commonly accepted single definition of what is a 'mass marketing scam'. Such scams – or consumer frauds – generally fall into four categories:

- Pretending to sell something you do not have, and taking the money.
- Supplying goods or services which are of lower quality than those paid for, or failing to supply the goods and services sought.
- Persuading customers to buy something they do not really want through oppressive marketing techniques.
- Disguising one's identity in order to perpetrate a fraud (Verniero and Herr, 1997, cited in Muscat et al, 2002: 1).

The Office of Fair Trading (2006: 12) has attempted to produce a definition of mass marketing fraud as,

> "A misleading or deceptive business practice where you receive an unsolicited or uninvited contact (for example by e-mail, letter, phone, or ad) and false promises are made to con you out of money."

There are, of course, many other types of scams perpetrated on a one-to-one basis, but the focus here will be those initiated through mass marketing (see, Vaughan and Carlo, 1975; and Morton, and Bateson, 2007). There are a very wide range of these types of scams and such is the ingenuity of fraudsters new scams are always emerging.

Some of those that have been perpetrated which have been identified by OFT – which do not fall into the investment category – will now be briefly described. They have been divided into: gambling scams, money making scams and bogus services and products (later in appendix 2 the extent and costs of each type of fraud is considered), for ease of reference.

### Gambling scams

There are a variety of scams where the victim is invited to become involved in lotteries and other gambling orientated schemes.

**1. Prize draw and sweepstake scams**
Fraudsters send out letters and emails to potential victims telling them they have won a prize or are entitled to a financial reward, but they need to pay a small 'administrative' fee to secure access to the funds.

**2. Foreign lottery scams**
These are similar to the above in that victims are told they have won a prize in an overseas lottery and they need to pay an 'administration' fee or tax to receive the monies. Again, these are perpetrated via mail, e-mail and sometimes the victims are also asked to contact an 'agent' by telephone.

**3. Bogus tipsters**
A variety of bogus tipster scams have been identified. Some will send out glossy brochures and charge fees for tips claimed to be secured from 'inside' information and often guaranteeing winnings for members. In reality, they often have no specialist knowledge.

# The characteristics of frauds

### 4. Premium rate and telephone prize scams
Victims receive a letter, text or automated phone call telling them they have won a prize, but they need to telephone a premium rate phone line to claim it. This call lasts several minutes and they invariably end up with a prize worth less than the cost of the call or nothing at all.

## Money-making scams

There are a variety of scams that offer the victim the potential to make 'easy' money.

### 1. Work at home and business opportunity scams
Fraudsters advertise work opportunities via newspapers, magazines, shop windows and even lamp posts that require few skills/qualifications, but claim to provide above average financial rewards. The fraudsters secure monies through up front fees to enable the victim to become involved, but, in reality, there is no paid work. Common jobs include stuffing envelopes, home assembly kits and home directories.

### 2. Pyramid selling and chain letter scams
Through letters, emails, websites, the Internet, advertisements people are enticed into a scheme for a fee, which promises high returns if they recruit more people. In reality, only a few at the top of the pyramid make money.

### 3. Internet matrix scams
Similar to pyramid investment schemes, they operate via adverts on the web offering free gifts. After buying a product a person goes on a waiting list to receive a gift once a prescribed number of others have also signed up, which encourages recruitment. There are always more members than gifts.

## Bogus products and services
There are also a variety of scams where bogus products and services are sold.

### 1. Miracle health and slimming cure scams
'Miracle' health cures for a very wide range of health conditions from obesity, impotence to cancer are advertised through mail or e-mail for ineffective and potentially dangerous products.

### 2. Clairvoyant and psychic mailing scams
Targets receive a letter from a clairvoyant or psychic that for a small fee offers to make predictions. Sometimes they are told something bad will happen to them, their family or friends if they do not participate.

### 3. Bogus holiday club scams
Under these frauds a person is approached in the street (often on holiday) or phoned and told they have won a holiday, but they need to attend a presentation to receive it. At the presentation they are subjected to high pressure sales techniques and end up paying for extras.

### 4. Career opportunity scams
Under these scams, like the bogus business opportunities, potential victims are recruited via advertising to a variety of activities that could enhance their careers. These include schemes to publish books, to attend conferences, to patent and market inventions and to become models or actors for which the victim has to pay a fee.

### 5. Loan scams
Fraudsters advertise fake loans in newspapers for which victims are made to pay an 'insurance fee' upfront.

# The characteristics of frauds

## Illicit scams

Scams set up to appear like an illegal activity looking for accomplices.

### 1. African advanced fee frauds/ foreign making scams

Fraudsters use mail, e-mail or faxes to target potential victims with usually a fictitious scenario of a corrupt government official who has 'procured' a large sum money and who needs a bank account to place it. Often a fee is sought to help facilitate the transfer as well as sometimes the bank accounts of victims have been targeted.

## Technological trick scams

Under these types of scams the victim is tricked into doing something which hides the fraudster's technological trick, which results in the payment of a premium rate without the victim's knowledge.

### 1. Internet dialler scams

Fraudsters send out emails or create pop up boxes on websites, which when downloaded or clicked upon downloads software that changes their Internet settings. This then links the person to the Internet through a premium telephone line, which the victim is often unaware of until they receive their bill.

## Other scams

There was also evidence that some scammers are moving into online dating sites where they create fictional profiles for the purposes of securing monies from the victim (Consumer Direct, n.d.). There are also a wide range of other scams that are perpetrated, many using less 'industrial' scale communications (see Morton and Bateson, 2007). For example, tradesmen who charge excessive fees to do home improvements which are shoddy or even non-existent. Many of this type of tradesmen will call door-to-door or distribute leaflets to potential victims. There are also tradesmen who may even advertise. Vaughan and Carlo's (1975) study of the appliance repairman provides a picture of long-term fraud over several years of a person unable to do many of the duties regarding repair of appliances that he was paid to do. A range of TV programmes have emerged publicising these types of 'rogue traders'.

## Investment frauds

There are many parallels between the mass marketing scams and some investment frauds. Indeed the OFT (2006) report cited above covers some investment frauds alongside scams.

### 1. High risk investments

Consumers are contacted via letter, e-mail or telephone and invited to participate in an investment scheme that is to be very lucrative. The investments are for shares, fine wine, gemstones, and art amongst many other opportunities. In reality, the 'investments' are worthless or very over-priced.

### 2. Property investment schemes

Fraudsters advertise or send out glossy brochures that invite prospective 'investors' to attend a presentation where they will learn how to make money from the property market. They are then pressured into joining for a fee or to buy 'future' properties at a discount. Variations on this also seek to entice investors into the buy-to-let market for non-existent properties or those in serious disrepair.

### 3. Ponzi

A Ponzi fraud is where a fraudster sets up what appears to be a legitimate investment scheme with usually above average rates of return. In reality the fraudster is skimming off a slice of the money and using the rest to pay the returns. Their survival inevitably depends upon bringing new investors into the scheme, so that eventually it will collapse.

# The characteristics of frauds

**4. Market abuse**
There is some literature on the American stock market that exposes some of the frauds and sharp practices perpetrated to manipulate the prices of legitimate stocks traded through the main stock markets. Often this abuse is focused upon so called 'penny stocks' with companies where much less information is in the public domain and where it is easier to manipulate the market. The Internet and e-mail have made the task of those operating in this area much easier. Some of the most common practices used include spreading false rumours through the Internet, discussion forums and e-mail which are likely to encourage greater demand for a stock and thus increasing its price and then selling before the rumours are exposed. The practice is known as 'pump and dump' (Walker and Levine, 2001). The victims in these cases are left with stock they have paid a premium for which has lost its value based upon false rumours.

## Identity frauds

Identity fraud is to be distinguished from 'identity theft' where the victim's identity is permanently appropriated (Semmens, 1999).
Far more common are the various types of identity fraud, which involves unlawfully using another person's details for gain or to avoid an obligation (Pascoe et al, 2006). This type of fraud can cover a large range of scams that vary in their use of the other person's details. Identity fraud has been defined by the Home Office Identity Fraud Steering Committee (n.d.) as:

> "… when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of identity fraud."

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

> "Identity fraud can be described as the use of that stolen identity in criminal activity to obtain goods or services by deception. Stealing an individual's identity does not, on its own, constitute identity fraud and this is an important distinction."

Below provides a rudimentary list of how identity fraud is perpetrated, from using a stolen credit card to the complete theft of a person's identity.

**1. Lost or stolen cards/documents**
This is where fraudsters use cards/documents stolen or lost from the victim to obtain goods and services.

**2. Card-not-present**
This is where a fraudster secures enough information from a victim's bank account details to make payments on the telephone, via the Internet, emails etc.

**3. Counterfeit cards/documents**
This is where fraudsters counterfeit existing cards/documents and uses them to obtain goods and services in the victim's name.

**4. Account takeover**
This is where a fraudster takes over the account of a legitimate customer and uses monies/credit facilities in them.

**5. Creation of new accounts, loans etc**
Fraudsters use the personal details of a victim to create bank accounts and apply for credit.

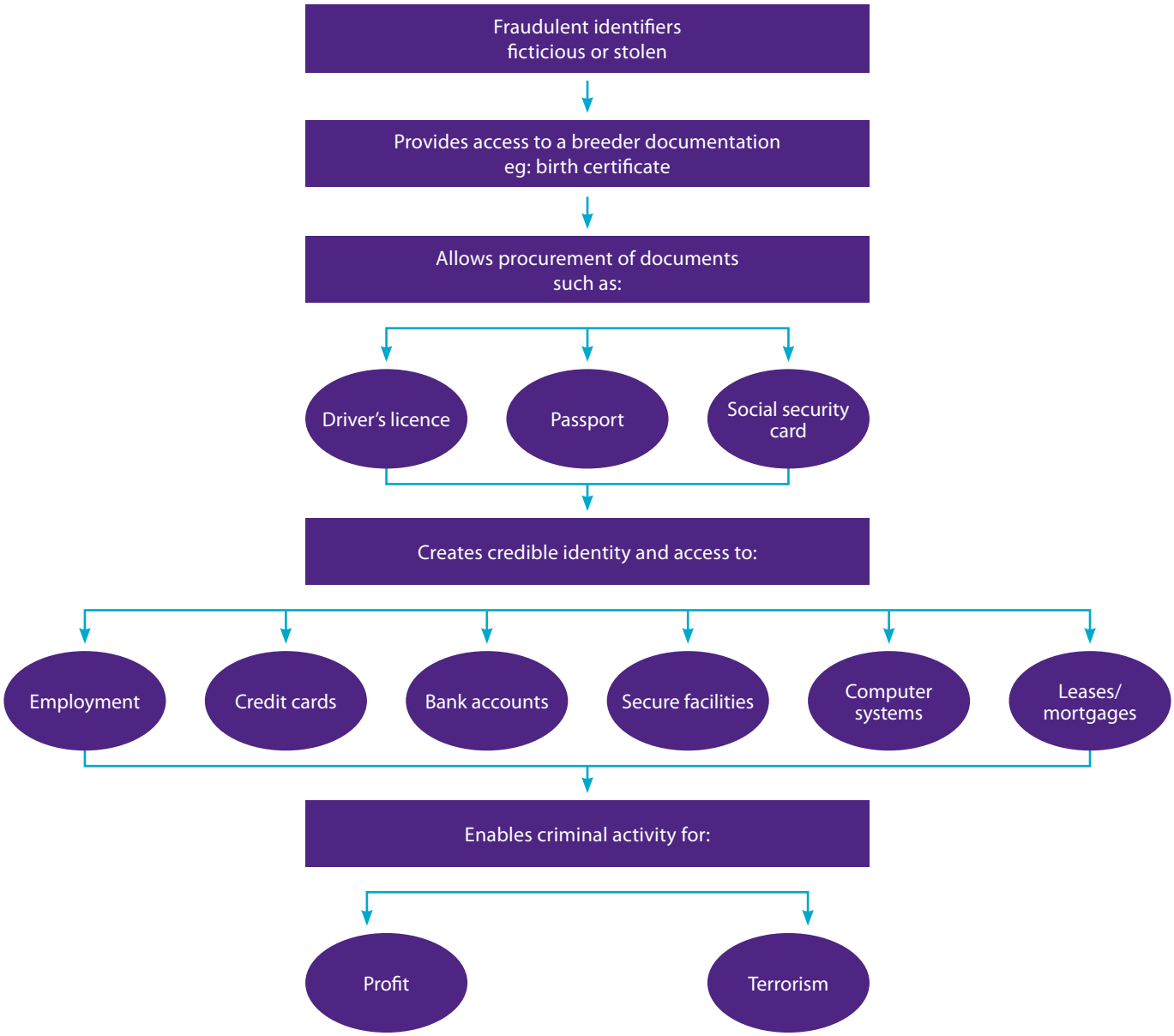
**6. Identity theft**
The fraudster takes on the identity of a person permanently.

The more sophisticated identity frauds are where information is used to secure 'breeder' documents such as birth certificates, driving licences etc. These often lead to multiple applications for store and credit cards, loans, benefits etc to secure credit that is never going to be paid back (Newman and

# The characteristics of frauds

McNally, 2005). These frauds are usually temporary as the real person invariably finds out with bills for goods never received or a failure to secure credit, due to a credit record they are unaware of. The model of the process of identity fraud, set out by Gordon and Wilcox (2003: 19), illustrates how the crime is perpetrated.

**Figure 1**
**The Identity Fraud Process**



# The characteristics of frauds

## Frauds against small businesses

Small businesses face many of the frauds identified above as well as others. They may deal with internal fraud from their employees (Doig, 2006) or external fraud such as long firm frauds perpetrated by other 'firms' (Levi, 2008b). There are also scams particularly targeted upon small businesses. These include false invoices submitted for payment, sales of entries or advertisement in non-existent newsletters or directories. Therefore for the purposes of this review some of the most common frauds perpetrated against small businesses will be reviewed. The Federation of Small Businesses (FSB) has published research illustrating the main fraud risks (2009).

**1. Corporate identity fraud**
The FSB survey found that 6 per cent of their respondents, who were all small businesses, had experienced corporate identity fraud. The common thefts were of IP and e-mail addresses which were then often used to commit frauds. These might be where legitimate clients of the company are redirected to pay funds into alternative accounts or to undertake phishing activities to secure the personal data of clients to undertake frauds against them.

**2. Card-not-present fraud**
A significant problem for many businesses is this type of fraud. Many goods and services are bought over the telephone, via the Internet or fax via the details on the card, rather than presentation of the actual cards themselves. Many fraudsters are able to secure the details on the card, even though they don't have the card itself and use these to order goods and services. Unlike cardholders, businesses can secure all the appropriate numbers from the buyer. However, if it transpires that the buyers details are fraudulent they are still liable to a chargeback, where they lose the money gained, as well as the goods and services sold. The FSB found that 29 per cent of respondents had been a victim of this type of crime. Research on Australian small businesses has also found this to be a major problem (Charlton and Taylor, 2004).

## Perpetrators of frauds

Before some of the techniques used by fraudsters are explored, it would be useful to briefly discuss the literature on the perpetrators of frauds. There is only limited data available. Even the law enforcement community does not always know the background of the perpetrators. There is also an ongoing debate as to the extent of involvement of 'organised criminals' in the various types of fraud explored in this review – not withstanding the challenges of defining this concept (see, Van Duyne, 1996). Levi (2008b: 89) has distinguished a category of fraudsters relating to long firm fraudsters, which can also be applied to other types of fraud (Levi, 2008a). These are:

**Slippery slope**
Individuals who generally have no prior convictions and fall into frauds through pressures combined with identification of opportunities.

**Intermediate long firm fraudsters**
People with prior convictions who started off with legitimate intentions, but eventually turn to fraud.

**Pre-planned long firm fraudsters**
The perpetrators start with the purpose of fraud and generally have past criminal convictions although may use 'front' people without convictions. Some may be involved in organised crime in the 'traditional' sense: ie. drugs, racketeering etc, or links to them or may focus solely on certain types of frauds.

Many of these pre-planned type fraudsters will often use those without traditional criminal backgrounds to perpetrate their frauds. Telemarketing frauds often utilise people with no prior criminal background who have come from white collar jobs. Technological requirements of some internet based frauds may require those with IT backgrounds.

Certain groups have also been identified as associated with particular types of frauds. Nigerians

# The characteristics of frauds

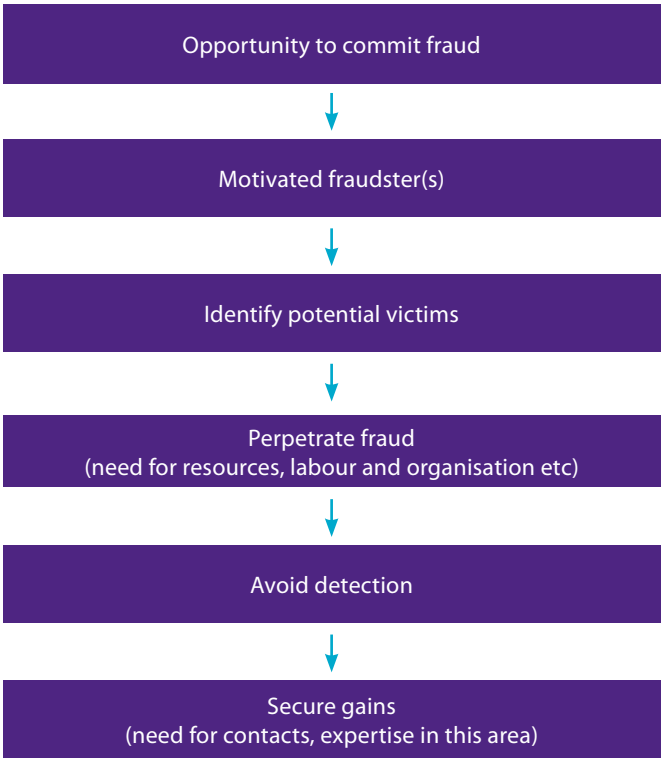
and other West Africans have become associated with the 419 scams, but Smith et al (1999) have also suggested the involvement of Nigerians in credit card fraud, identity card fraud, forgery, immigration fraud as well. Many internet based frauds – often involving phishing – have been linked to Eastern European criminal groups in Russia, Romania, Lithuania to name a few (Levi, 2008a).

## The 'Scampreneur'

The wide range of scams pursued by fraudsters, combined with their innovation in type and techniques used marks many out for their entrepreneurial skill – unfortunately misdirected into fraud. Entrepreneurs have been the subject of much research and some of the characteristics that define them include: risk taking, the need to achieve, the need to be the locus of control, over-optimism and the desire for autonomy (Carter and Jones-Evans, 2006). These traits are central to a successful scammer or 'scampreneur'. Indeed the declining economic conditions from 2008 onwards have already led some to move their operations towards the changing economic conditions, such as fake training opportunities targeted at the unemployed. 'Scampreneur' would therefore seem to be an appropriate title for many of them. Levi (2008b: 392) has sought to outline the process of frauds, which can be adapted utilising the literature on scams to demonstrate their business model.

The model starts with the identification of a potential opportunity. As the earlier section of this review revealed there are a very wide range of different types of fraud that can be pursued by the fraudster. Also, there needs to be a motivated fraudster and this might be a career, organised fraudster or simply a normally law abiding person who has turned to fraud for whatever reason. Once a potential fraud has been found, a potential victim needs to be identified. If the fraud involves mass marketing then the next stage requires the appropriate resources, labour and organisational skills to perpetrate it. The scampreneur also needs to pursue strategies to avoid detection. Finally, any proceeds from the fraud then need to be secured and the money laundered. This will all usually require contacts and expertise.

**Figure 2**
**The 'Scampreneur' business model**




It would now seem appropriate to explore the techniques of fraudsters.

# The characteristics of frauds

## The techniques of fraudsters

The growing literature upon different types of fraud provides much information on the techniques of fraudsters. These diverse range of tactics used will be considered under three sub-headings, victim selection techniques, perpetration strategies and finally detection avoiding strategies. There is also a fourth category of securing the gains, but this is beyond the scope of this paper.

### Victim selection techniques

The earlier section on different types of victims revealed a wide range of strategies fraudsters use to contact their victims. These can range from one-to-one, mail, telephone, e-mail, Internet to advertisements. Some of the methods linked to these will now be explored.

#### 1. Potential victim lists

Mass marketing scams, using addresses (mail and e-mail) and telephone numbers, often use legitimate lists that are available to all businesses. Open source information such as telephone directories, list of shareholders, names of company directors, are used as well as legitimate marketing lists sold to businesses for specific market segments. For example fake lottery scams may make use of known lists of consumers who participate in lotteries. Fraudsters may also purchase so called 'suckers' lists which contain the details of those previously fallen for a scam (Smith et al 1999; Shover et al, 2003). Methods used to generate spam mail that go to multiple e-mail addresses are also used by identity fraudsters undertaking phishing attacks.

Identity fraudsters have also been known to utilise open source information of certain groups of people to perpetrate frauds. For example company directors have to supply a range of personal data, including personal addresses, which is openly available via Companies House. These people are also generally better off in terms of income. Company directors have disproportionately become the victims of identity fraud (Pascoe, et al, 2006; Experian, 2008). Some people also publicise information about themselves on social networking websites such as Facebook, which can then be exploited (Aleem, 2007). Illicit information may also be traded by corrupt employees or persons who have stolen the personal details of potential victims from an organisation.

Thus, to summarise potential victim lists are drawn from the following:

- Open source directories/databases (phone book, lists of directors, shareholders, etc)
- Marketing lists (known purchasers of lotteries, health products etc)
- Illicit lists (suckers, personal information)

#### 2. Affinity groups

A common selection technique of Ponzi schemes is to target affinity groups. These are groups who work together, attend the same place of religious worship, or are members of clubs. The tactic is to get one person hooked who then discusses their above average returns with the aim that they will spread the word leading to further recruits. Evidence from the USA has suggested a disproportionate number of these frauds occur amongst church-affiliated groups (Ganzini et al 1990). The Madoff Ponzi scam was also targeted at the very rich and famous as an affinity group.

#### 3. Targeted advertising

There are a number of scams that simply advertise in appropriate publications encouraging potential victims to respond. For example, bogus tipsters will advertise in the racing press.

# The characteristics of frauds

## Perpetration strategies

This review has demonstrated the diversity of frauds. Therefore, it is also not surprising to find huge variations in the techniques used, once a victim has been identified, to secure their monies. It is useful to divide these between core techniques common to almost every type of scam to more specialised techniques. The latter are mapped in appendix 1 against the different types of frauds considered in this review.

## Core techniques

### 1. Business skills and contacts

Almost all the scams under consideration in this review require the fraudster to have good general business skills and contacts (Levi, 2008). To set up a mass marketing operation using mail, the web or telephones requires good organisational skills. To secure appropriate lists, scripts for scams etc may also require good networks, frequently with criminal groups. Once monies are received skills in laundering it or access to networks that can help are also required.

## Specific techniques

### 1. Use of appropriate and latest technology

A scam artist is committing malpractice if he's not using the Internet (Danner, 2000 cited in Lagenderfer and Shimp, 2001: 764).

Many of the perpetrators make use of the latest technology to undertake their scams. Some of the identity fraudsters use sophisticated software, develop programmes and special gadgets to manufacture and copy cards. Central to many scams is the use of the Internet. It has opened up many traditional small-scale scams to the mass market. There are more mundane technologies used to perpetrate scams, such as the mail and telephones.

### 2. Professional and legitimate appearance

The research by the OFT (2006) on mass marketing scams demonstrates that in many of the frauds a significant factor in their success was the professional and legitimate appearance of what enticed them into the fraud, such as, advertisement, e-mail, letter, brochure, telephone call, presentation etc. Other research has found the credibility of names to be important in investment schemes (Shichor et al, 2001), accents of salesmen/women in telemarketing, quality of documentation/brochures etc (Shichor et al, 2001).

Conversely Grabosky and Duffield (2001) have identified some of the 'red flags' that raise warnings to a potential risk of fraud. Many of these are the opposite of the above in that they convey a lack of professionalism and illegitimacy. They point to factors such as over familiarity, undue pressure to pay, very low prices, very high returns claimed, lack of official documentations/authorisations to name some. Downs et al (2006) have also identified how mistakes in phishing emails can lead to some identifying it as high risk. Although, they also found, people didn't always recognise these clues.

### 3. Illegitimate appearance

The other side of legitimate and professional appearance of some scams are the frauds that, if they had been real, would incite illegal activity. The Nigerian 419 scams are prominent in this category as if the transaction had been real the victim would have been involved in corruption, fraud, money laundering amongst many other potential crimes. Therefore by securing their involvement in what appears to be an illegal activity it makes it more difficult and embarrassing for the victim to report the fraud (Smith et all 1999; Tive, 2006). This is exacerbated when threats of intimidation and violence are added to the combination that by perception or reality the victim is dealing with organised criminals.

# The characteristics of frauds

### 4. Small sums of money sought

The OFT (2006) research illustrates that in many of the frauds relatively small sums of money are lost – frequently less than £100. The tactic of the fraudster is to secure such a sum of money that the victim will be less bothered to report the fraud (Langenderfer and Shimp, 2001).

### 5. Good sales techniques

Central to many scams of this type are very good sales skills (Levi, 2008b). Many of the 'boiler rooms' also take on the structures of legitimate call centres that deploy sales expertise according to skill. For example Shover et al (2003) drawing upon interviews with 47 criminal telemarketers in the USA found three key types of roles:

- Sales agents: who make the first calls with a scripted pitch and identify potential victims.
- Closers: who are more experienced, and then take on the role.
- Reloaders: who are the most experienced and maintain contact with those already defrauded to secure more monies from them.

Sometimes the victims, who are often vulnerable, are also subjected to high pressure sales where they are contacted multiple times with the purpose of signing them up (Shichor et al, 2001). An American survey found some victims 'besieged by telemarketers' (AARP, 1996 cited in Titus and Gover, 2001: 143). Further, Schichor et al (2001) in a survey of victims of one investment scam, found that 82.3 per cent had reservations about the scheme when contacted, but such was the persuasiveness of the sales agents they still participated.

### 6. Selling a dream

Central to sales based frauds is 'selling a dream'. The fraudster offers something someone wants at a low price or something that promises to make the victim above average returns. As Titus (1999: 4) argues, 'The lure of something free, absurdly cheap or unrealistically lucrative, is integral to many fraud "come ons"'. For example, fraudsters offer work with few skills that pay above average, loans to persons who would never secure one from a bona fide provider, investment returns fund managers could only dream of. They play on the needs of certain groups of individuals and with their slick sales skills sell them the dream.

Lagenderfer and Shimp (2001) argue that many scammers play on the visceral influences. That is, those desires that have a hedonistic impact such as sexual desire, greed, fear etc. Many decisions based upon these needs are often made with limited or no cognitive deliberation, but after time these desires often wane. This is why many scammers often seek instant responses.

### 7. Operating in legal hinterland

Many of the frauds operate in a legal hinterland where the tactics they use make it difficult to unambiguously identify it as fraud. This makes some 'victims' adamant that they are not victims of fraud; others, even though they recognise it probably was a fraud, are less likely to report it because of the perceived ambiguity; and another group who may be conscious it is a fraud, want to report it, but because of the ambiguity face a law enforcement community unwilling to take it on or passing it on to other agencies. For example, some lotteries do pay out prizes and consequently the reaction of many police forces who receive complaints is that it is a 'civil matter' between the victim and lottery. Some scams also have very small print contradicting the main message of the scam. Fraudsters play on this and even if the law enforcement community does become interested they claim the dispute is a civil matter and of no interest to the police (Shover et al, 2003).

# The characteristics of frauds

### 8. Intimidation and threats of violence

Most mass marketing and investment scams take place with no threats of violence or intimidation. However, there are a few exceptions. The Nigerian advanced fee frauds in some cases, once a victim is drawn in, sometimes deploy threats of violence and intimidation to ensure their continued participation. For example, Smith et al (1999: 3) found evidence of one fax to a victim:

> "… to inform you to produce a mandatory sum of US$35,000 only, into our account given below in Switzerland within ninety six hours, alternatively you will kidnapped and forced to commit suicide during the period of our on-coming anniversary of fifty years [sic]."

Some of the clairvoyant and psychic mailing scams also play on fear, by threatening bad luck, health problems etc on those (or their families and friends) who refuse to participate.

### 9. Identity fraud techniques

There are a wide range of techniques used by identity fraudsters that deserve consideration in their own right. The fraudster requires either genuine identity documents, such as a passport, driver's licence, credit card or selective personal information such as name, address, date of birth, bank account numbers, national insurance number to name the most prominent. Depending upon the fraud the fraudster might hijack the victims account and/or apply for credit cards, loans etc.

### 9.1. Redirection of mail

One of the most common techniques used in identity fraud is the redirection of the mail of a victim to an alternative address. This accounts for 36 per cent of identity fraud (Experian, 2008). Using this technique requires careful planning. There are also more opportunistic fraudsters who simply steal mail by acquiring the mail of a housemate or a previous occupier of an address. As soon as they are able to control the mail they can then use the victim's identity to apply for credit cards, order mail order goods etc.

### 9.2. 'Jackal' fraud

In this type of fraud a deceased person's identity is used to secure credit, goods and services (Experian, 2008). It is known as 'Jackal' fraud from the film 'The Day of the Jackal' where the assassin assumes the identity of a long deceased child to apply for a passport.

### 9.3. Theft of personal information

Some identity frauds are based upon much more basic strategies. For example a wallet or purse stolen in a burglary, theft, or some other crime might contain official documents that are sold to a fraudster or used by the original criminal to assume the identity of the victim, for the purposes of securing credit, goods and/or services (Allison et al, 2005).

### 9.4. Dumpster diving

Another relatively simple approach – although slightly messier method – is simply stealing a person's rubbish with the hope they have left personal information in it such as bank statements, utility bills, etc which can then be used to assume that person's identity for the purpose of fraud (Allison et al, 2005).

### 9.5. 'Skimming'

'Skimming' is a more sophisticated means of stealing a person's identity. It is when a person presents a credit or debit card to a corrupt cashier who also swipes the card to copy the data on it. That can then be used to make a copy. Ideally for the fraudster there will also be some means to identify what the person's PIN number is although this is not essential (Allison et al, 2005).

# The characteristics of frauds

### 9.6. Pretext calling (social engineering)

Some fraudsters will pretend to be someone they are not, to secure bank account and other personal data. This often is known as pretext calling or social engineering. It can be done in person, over the telephone or most commonly through e-mail. The most common approach are the so called phishing emails, where a person receives an e-mail from what looks to be their bank or some other official body that seeks the personal information of the person. Some of the emails use the logos of the financial institutions and look very professional. At a less sophisticated level the fraudster might just telephone potential victims pretending to be a financial institution to secure the information they require.

### 9.7. Trojans

The more sophisticated identity fraudsters sometimes send out 'trojans', so called because what may seem like a legitimate e-mail, website, pop-up box actually hides a computer virus. Once the virus is installed via opening a mail, clicking on a pop up or downloading a site, it sends data to the fraudster on login names, passwords etc which are then used to target legitimate accounts (Bank Safe Online, 2009).

### 9.8 Hackers

Some of the more sophisticated fraudsters may also have the capacity to 'hack' into certain organisation's computers which then gives them access to the personal data they need to commit fraud (Newman and McNally, 2005).

### 9.9 Corruption and incompetence

Personal information on individuals and businesses is also sometimes secured through a corrupt employee passing the information on or occasionally sheer incompetence (Newman and McNally, 2005). There have been a number of high profile losses of personal data in the UK through incompetence such as the personal details of all child benefit claimants in the UK.

## Detection avoidance strategies

Fraudsters also use a wide range of techniques to minimize the risk of getting caught. Some of the strategies used will now be considered.

### 1. 'Rip and tear'

Many boiler room based fraudsters are mobile and do not stay in a location very long (Hines, 2001). They will set up in a place for a period of time and initiate intensive targeting of potential victims and then move on before the local law enforcement community become alerted to their operation. This tactic is often called 'rip and tear' (Shover et al, 2003). In some cases 'boiler rooms' will bring in local sales staff – who may not even know it is a scam (Stevenson, 1998) – and frequently these are the only staff left when the law enforcement community turn up, not the organisers (Hines, 2001).

### 2. Operation from regimes with limited police interest/weak sentencing

Many of the mass marketing scams operate in countries where there is limited police interest or if caught the sentencing regime is light. Spain is commonly cited as a source of many boiler room scams. This is often put down to a lack of interest by the Spanish authorities given that the fraudsters do not attack Spanish citizens on their own doorstep. In Canada the reason is often laid at the feet of what some believe are light sentencing laws should a fraudster be caught, compared to the neighbouring USA where sentences, if caught, are very harsh.

# The characteristics of frauds

### 3. Making reporting unlikely

Fraudsters often pursue frauds for low sums of money that make reporting to the authorities unlikely by the victim (Hines, 2001). They also operate scams so they are or are perceived to be in legal hinterlands making reports less likely and law enforcement involvement less likely if contacted. Some frauds also pose jurisdictional challenges, meaning it is unclear where a victim should report or who has responsibility for investigating it. As Starnes (1996: 2006) argues:

> "… many operators of fraudulent schemes slip through the cracks in state or federal statutes, or create new schemes to fall outside the scope of statutes."

Now the nature and techniques of frauds have been considered it would be appropriate to examine the research on victims.

# The characteristics of victims of fraud

**Victims of fraud have been largely neglected by the broader community of scholars studying victimology (Shichor et al, 2001). This is despite evidence of the widespread risk of fraud. In the USA, for example, a nationwide survey for the National Institute of Justice found 58 per cent have been a victim of a fraud or attempted fraud (cited by Deem, 2000: 34). In the UK the OFT (2006) have estimated 48 per cent of the population have been targeted with a scam and 8 per cent would admit to being a victim of one. With the growth of phishing emails and other scam e-mail it would be fair to assume that these figures – at least in attempts – are much higher.**

There has, however, been some research on the victims of fraud in recent years in North America and Australia, as well as the UK. Much of the research has highlighted the parallels of the perception and treatment of fraud victims to rape victims – as the victims are often thought by legal authorities to be partly to blame (Shichor et al 2001; Levi, 2008a). There is often a view of victims of fraud that they are partly to blame and that you can't con an honest man (or woman) (Van Wyk and Benson, 1997). Indeed, Delord-Raynal (1983, cited in Titus and Gover, 2001) goes as far as arguing some victims are co-conspirators in the crime.

## Victim typologies

There are a diverse range of issues covered vis-à-vis the research on victims of fraud. Before some of it is considered it would be useful to make one major observation on fraud victims. As the earlier part of this review demonstrated there are numerous types of frauds. Similarly there are a wide range of different types of victims, therefore it is difficult to generalise. A good analogy is the case of cancer victims. There are a large number of cancers affecting a wide range of different groups. They are all called cancer but the victims and how they became victims are very diverse. The following section will illustrate the wide diversity of fraud victims. However, like cancer victims, when it is broken down into distinct frauds and scams some patterns become more observable.

### Profile by Knowledge

**Figure 3**
**Profile of victims by knowledge**

The first observation of note is that there are many 'unknowing' victims of fraud. Such is the nature of some frauds many fall for them and unless contacted by a law enforcement agency would never know they have been defrauded. The best examples of these are some of the lottery and fake charity scams. Many people enter lotteries knowing winning is unlikely. Therefore, not receiving a prize is not an indication of fraud to them. Similarly, some people who give to charities may never learn it was in fact a scam (Fraud Advisory Panel, 2006).

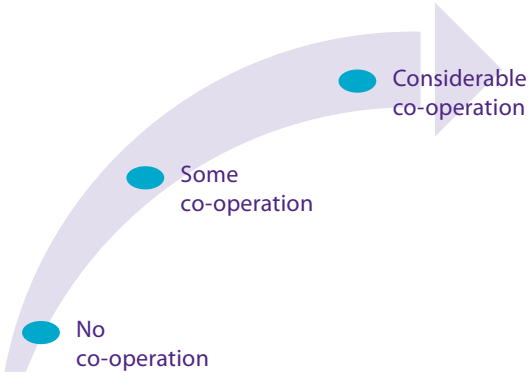
# The characteristics of victims of fraud

Most scams, however, do eventually result in the victim finding out and 'knowing'. These can be divided between those who report and those who don't. Some of the reasons for non-reporting will be considered later in this section. There are also, however, the 'unbelieving' victims who are so taken in by a scam they will not believe it is one. For example the researchers were informed of some victims of investment frauds who were told at the point of payment by their financial institutions that it was a scam, but who thought they were merely frustrating their chances of making a 'killing' on an investment. These and many victims of mass marketing fraud have been termed what is known as 'chronic victims', responding to multiple requests by the scammers.

## Profile by co-operation

Some researchers have also sought to profile the degree of co-operation in carrying out the fraud (Titus, 1999; and Titus and Gover, 2001). There is also what could be described as the 'careless' victim. For example some identity fraud victims who exhibit a degree of carelessness by throwing away bank statements also put too much personal information on a social networking website or fail to update the security on their personal computer. There are also some victims warned by financial institutions that the transaction they are about to pay for is a scam, however they ignore the advice.

**Figure 4**
**The range of involvement of the victim in the fraud**




The involvement of the victim can be distinguished according to the degree of co-operation as set out in Figure 4 below. Drawing upon Titus (1999) Figure 4 shows the range of involvement by victims distinguished according to the degree of cooperation. At one end is the completely random victim, where there is no co-operation in the fraud whatsoever. This could be a company director whose personal details are used to make fraudulent loan applications.

At the next level of involvement is 'some co-operation', where the victim does play a part but is generally more 'passive' in orientation. For example, someone responds to a phishing e-mail who is tricked into giving their bank account and other personal details or a person cold called by a boiler room and persuaded to purchase worthless shares. This could also cover a victim of identity fraud who has thrown away their bank statements. They have played a role in the fraud, but have been unlucky that their rubbish has been targeted by a fraudster.

Finally there is 'considerable co-operation' where the victim is more involved in the fraud and may even show a degree of pro-active involvement. For example, responding to an advertisement or actually seeking out an investment scheme. Some of the victims of home working scams, racing tipsters would fit this category. The figure above demonstrates these three categories of involvement.

Some of the types of co-operation have been identified by Titus (1999: 2):

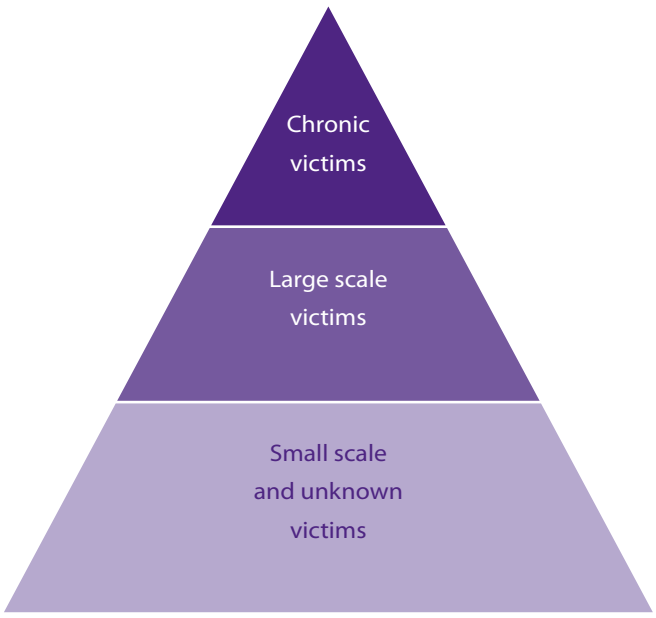
- Victim making contact with offender (responding to advert, visiting website etc);
- Victim providing information about him/herself;
- Victim allowing offender to turn business relationship into a personal one;
- Victim allows offender to create false perception of situation which can then be exploited (believing the lottery has been won);
- Victim reveals personal financial information to offender.

# The characteristics of victims of fraud

The general typology of victims can also be mapped according to losses and repeat victimisation. In many ways it resembles an iceberg. There are a small number of so called 'chronic' victims, largely succumbing to mass marketing scams above the surface at the top, few in number but often losing large proportions of their income/ savings (although often in multiples of relatively small sums of money) (Shichor et al, 2001; OFT, 2006). Once a victim responds to a scam they are likely to be put on the 'suckers' lists and face a barrage of further scams. The Fraud Advisory Panel (2006) highlighted the case of Lillian Lazonby who had been targeted by junk mail scammers and after her death, relatives found over 10,000 letters and losses of £20k.

Then there are a large number of victims who may have been victims of fraud once or a few occasions, but have lost substantial sums of money. Some of these may or may not report the fraud. Finally there are an even larger number who may or may not know they have been a victim, as the sum of money lost is very small.

**Figure 5**
**Typology of victims by loss**




## Profile of victims

The analogy of cancer victims was used to describe fraud victims. To gain a deeper insight into the victims of fraud it is therefore necessary to delve further into the profile of specific types of fraud. Appendix 2 highlights some of the research on the main profiles of victims to different types of frauds. Some of those findings will be explored according to the different types of frauds. Before this is considered, however, it would be useful to examine some key issues related to victimisation which can be applied generally.

There is a common perception, particularly in the media, that older people are more likely to be the victim of a fraud (Titus, 1999). Indeed, the profiles of some victims in appendix 2 show higher proportions of victims coming from older age groups. However, it is important to distinguish between who the fraudsters are targeting, who succumb and the actual number of victims across different demographic groups. If a fraudster is solely targeting older age groups then they are of course likely to form the greater number of victims.

There have been a number of studies in other countries that have shown that rather than older people, the most likely victims of consumer frauds is in fact younger people. Titus et al (1995) in a national survey of fraud victims in the USA found older people were three times less likely to be victims of fraud. Another smaller scale study in the USA also found that the younger were more likely to become victims of fraud (Van Wyk and Benson, 1997). In Australia Muscat et al (2002) drawing upon data from the Australian Crime Victims survey found younger people to be at greater risk of fraud, with 9.3 per 100 persons of 16-64 years compared to 3.9 for 65 years and over victims of consumer fraud. They found lifestyle factors such as an active social life and working to be more important, as they exposed individuals to greater risk of fraudulent transactions. However, compared to other crimes, consumer fraud is a much higher risk than other crimes for the elderly: 2.2 times more

# The characteristics of victims of fraud

frequent than assault, 2.4 more times than theft and 13 times more than robbery (Caracach et al, 2001).

Research has also shown that those who have a positive attitude to financial risk taking are more likely to be targeted as victims of fraud (Van Wyk and Benson, 1997). There is also evidence that persons with low self-control – who are often prepared to engage in a range of risky behaviours to seek instant gratification - are also more prone to victimisation (Holtfreter et al, 2008).

## Mass marketing and investment frauds

Appendix 2 illustrates the profile of the different types of victims to a range of scams, and their median losses (largely drawn from OFT, 2006). However, it is challenging to ascertain the numbers and range of individuals targeted by the fraudster. This makes it difficult to determine whether specific groups are more susceptible to fraud.

**1. Scams which men tend to fall for:**
African advanced fee frauds, internet dialler scams, high risk investments, and property investment.

**2. Scams which women tend to fall for:**
Internet matrix, Miracle health and slimming cure scams, clairvoyant and psychic scams, and career opportunity scams.

**3. Scams the old tend to fall for:**
High risk investments and doorstep service providers.

**4. Scams the young tend to fall for:**
Work at home and business opportunities, clairvoyant and psychic scams, and Internet dialler scams.

**5. The biggest scams (costs to society):**
Bogus holiday clubs scams, high risk investments, pyramid selling and chain letters, and foreign lottery scams (as identified in appendix 2 according to the total costs to society estimated by OFT, 2006).

**6. The biggest scams (by individual median loss)**
African advanced fee, high risk investments (there are some chronic victims who large sums by responding to multiple scams.

What is striking about of the scams is that the profiles cover almost everybody; hence almost anyone could become the victim of a scam.

## Identity fraud

There have been several studies that have sought to measure the impact of identity fraud and profile their victims. Research by the Home Office has estimated it costs the UK economy over £1.2 billion and there are over 100,000 victims costing every adult £25 per year (cited in Pascoe et al, 2006; and Identity Fraud Steering Group, 2008). This illustrates that anyone can become the victim of identity fraud, but there are certain groups who appear to be more at risk than others.

Research for CIFAS based upon all 55,548 victims of impersonation on their records as well as a survey of some of them revealed some of the following key findings.

- 67 per cent male, 32 per cent female
- 31-40 years old 28 per cent
- 41-50 years old 23 per cent
- 64+ years old 13 per cent
- Largest number of victims living in London, but higher per capita rates in Manchester and Nottingham.

# The characteristics of victims of fraud

A survey was also carried out resulting in some key findings:

- **Three-quarters of victims had been the victim of more than one offence**
- **Victims in the 31-40 age bracket were most likely to be repeat victims**
- **51 per cent didn't know how the fraudster obtained their documents.**

Experian (2008) has conducted a much deeper analysis into some of the 10,000+ victims of identity fraud. It found the typical victim of identity fraud was:

- **26-45 years old**
- **Working in a professional occupation**
- **Owner/occupier (usually in a detached house)**
- **Earning over £50,000 (these are 3 times more likely to be victims)**
- **Directors of companies.**

The evidence would suggest that fraudsters tend to target – for obvious reasons – those likely to have higher credit ratings, where their chances of both rewards and success are greater. Targeting those on lower salaries runs the risk that the application might be rejected and second that the potential credit offered may be lower.

Using their client classification system, the 'corporate top dogs', those running businesses, high up in large organisations were the most at risk group. Directors of companies are also at high risk of becoming victims of fraud; with those from large companies becoming five and a half times more likely and those in organisations with less than 50 employees, two and a half times more likely.

They were also able to profile the most at risk locations, all of which were desirable locations in London:

- **Kensington, Richmond-upon-Thames, Putney, Wimbledon and Kings Road (Chelsea).**

This was believed to be due to the large number of affluent people who frequent restaurants, clubs, and other services, providing opportunities for fraudsters to gain appropriate information. Outside of the M25 the 10 most at risk locations were:

- **St Albans, Guildford, Windsor, Woking, Camberley, Maidenhead, Redhill, Bracknell, Bishops Storford and Horsham.**

Experian also offered analysis of the average costs of each fraud. In these types of fraud it is generally the corporate body that faces the financial loss, rather than the victim. Although there are a number of ways they lose out for example, in time lost and credit rating, to name a few. The average loss for all was £1,303, but this did vary with mail order companies £219, higher purchase £28,424, loan providers £7,556 and credit and store cards £1,365.

## Low reporting of frauds

Virtually all identity frauds are reported, it is more a question of how soon they are reported. This is because actual attacks on the victims' accounts or attempts at securing credit trigger an enquiry that leads to the discovery. Thus someone who rarely seeks credit who has not had their own accounts targeted might take some time to discover they are a victim. For mass marketing and investment frauds, however, reporting is generally very low – approximately 1 to 3 per cent report.

Appendix 2 also highlights some of the statistics on the reporting of frauds. It shows that although there is a variation in mass marketing frauds, levels of reporting are generally very low. The literature on fraud victimisation offers a number of reasons for low reporting.

# The characteristics of victims of fraud

## Don't know

Some victims don't know they are victims of fraud thus don't report them.

## Perception partly responsible

Many victims hold themselves partly or solely to blame and as a consequence are reluctant to report it. Indeed Mason and Benson (1996) found those victims who blamed themselves or the offender and themselves, were much less likely to report.

## Embarrassment

Linked to perceptions of responsibility some victims feel embarrassed and do not want family members and outsiders to know of their loss.

## Low financial Loss

Several researchers have found that relatively small fraud losses make reporting less likely (Mason and Benson, 1996; Copes et al, 2001).

## Ambiguity of fraud

Some frauds are designed to be legally ambiguous. This means once the victim realises it is a scam, it may be difficult to secure the interest of the law enforcement community. Some scams, such as investment frauds, are ambiguous in the sense some victims think it was just a bad investment rather than a scam.

## The criminal justice process

A common perception for victims' low reporting of fraud is the perception that criminal justice agencies do not take them seriously (Mason and Benson, 1996; Titus, 1999). There has been rigorous evidence to support this perception. A study of consumer fraud victims in Florida found that one of the most significant reasons for low reporting was low confidence in the ability of legal bodies to respond to victimisation. Less than half of those surveyed had either 'a great deal' or 'quite a bit' of confidence in legal authorities to deal with fraud victimisation (Reisig and Holtfreter, 2007). This compares to other studies on the police which tend to show around three-quarters have confidence in their ability to solve and prevent crime. There is also evidence in the USA of the unequal treatment of victims enshrined in law with lesser opportunities to outline the impact of the fraud in court proceedings as well as access to restitution (Dee, 2000).

## Confusion

Some victims are confused over to whom to report the fraud. This might be made worse if they go to the police and are told it is a 'civil matter' or to speak to another agency, who in turn then may refer them elsewhere or to another body.

## Social networks

Another important factor in whether a victim reports their fraud is related to the social networks they belong to and their attitudes towards the fraud. Mason and Benson (1996) in a survey of residents in Knox County, Tennessee found as a significant factor in whether a person reported a fraud, was whether their social network (family, friends) encouraged them to do so or not.

## Engaging with the Law

In one study in the USA an attempt was made at linking 'Black's theory of law' to reporting behaviour for fraud (Copes et al, 2001). This theory holds there are a series of factors which make individuals more

# The characteristics of victims of fraud

likely to invoke the law in an activity they are pursuing. These include factors such as:

- **Strata: those in higher strata use the law more than those in lower.**
- **Morphology: strangers are more likely to use the law than intimates.**
- **Culture: where there is more culture there is more law involved (more education, literacy etc).**
- **Organisation: greater organisation leads to greater use of the law.**
- **Social control: if certain measures used to secure social control will have an impact on others, thus more custom will mean less law, and vice versa.**

The researchers treated reporting fraud as equivalent to engaging the law and found morphology and culture to be significant predictors of fraud reporting. They also found the size of the fraud a factor; the greater the size of the loss, the more likely a report. Interestingly, they found income earned was not a significant predictor.

## Impact upon the victim

In this section of the review the impact of fraud upon the victim will be considered. The literature on fraud highlights some of the devastating consequences some frauds have on the victim. Such is the impact some have claimed they actually feel like they have been raped (Deem, 2000: 37).

### Financial

The most obvious consequence is a financial loss. For some victims of fraud such is the loss that it results in them having to sell assets (often their home), to go back to work (if they were retired), or not being able to secure credit. In the worst cases victims even become bankrupt. The National Institute of Justice research on victims of fraud in the USA found 20 per cent suffered financial or credit problems as a direct result of the fraud (cited by Deem, 2000).

It is not just the actual financial loss that may have an impact upon the victim, it is also the time taken to deal with it. It has been estimated it takes 48 hours on average for the typical victim of identity fraud to clear their name (cited in Fraud Advisory Panel, 2006). Research by Pascoe et al has suggested that for most victims they can spend between 3 and 48 hours rectifying their situation (actual time taken which might be over a longer period of days/weeks). Appendix 2 highlights the median losses across a range of mass marketing, investment and identity frauds. It must be noted the low figures hide some victims who have lost substantial sums of money.

### Employment

For some victims who are self-employed, the consequences of fraud against their business might result in it failing and consequent loss of employment.

### Emotional impact

A study of the impact of identity fraud found some victim's emotions were affected. Some became worried about someone accessing their personal details. Others became agitated and distressed. For some this led to feelings of violation, stress and anger (Pascoe et al, 2006). Research on mass marketing scams has also found some victims suffer stress, anxiety and loss of self-esteem (OFT, 2006).

# The characteristics of victims of fraud

## Health problems

The impact of fraud can also lead to a range of health problems, both physical and mental. Spalek (1999) in a study on the victims of the Maxwell pension fraud found that 'anger' was a common emotional impact of the fraud. She also found they suffered stress, anxiety and fear as a result of their loss. A study of victims of a Ponzi scheme found many were afflicted with depression (Ganzini et al, 1990). These conditions often then feed into an impact upon the physical health of the victims. Spalek (1999) also found that some of the victims of the Maxwell fraud felt their husband's deaths were accelerated as a result of the scam. Such is the consequences for some victims they attempt to actually commit suicide.

## Social disintegration of family

The loss of wealth and sometimes the way in which the money has been lost (ie often hidden from partners) can often lead to the breaking up of marriages and relationships. Such is the nature of some chronic scams and their effect on victims. When family members try to intervene to stop them from engaging with the fraudster it leads to a disintegration of their relationships.

## Self-blame

A common theme amongst some victims of rape and other violence is that the victims partly blame themselves. There is evidence for this amongst fraud victims as well (Titus and Gover, 2001).

## Behavioural changes

For some victims the impact of the crime changes their behaviour. Spalek (1999) found victims of the Maxwell pension fraud changed their perceptions on activities to which they previously felt they were invulnerable. She found some victims changed their behaviour as to where they might place their money. The OFT study of mass marketing fraud found over half the scam victims studied had changed their purchasing and payment behaviour (OFT, 2006). There is also evidence of some victims less likely to make use of the internet for purchases. Some of these changes could be seen as positive in terms of reducing the risk of fraud, but if some changes become too widespread this may have an impact on legitimate business.

## Impact on wider business community

Another wider consequence of many frauds is it undermines trust in certain business practices. Internet fraud may make people reluctant to use it to purchase goods (Fraud Advisory Panel, 2006). Many people may become less likely to engage with legitimate telemarketers and mass marketing mail, penalizing the legitimate companies (OFT, 2006).

# Plural provision

This review has illustrated the diverse nature of fraud. The diversity is also reflected in the plurality of organisations involved with helping victims from both the public, private and third sectors. This presents challenges in both victims finding the best place to report to and organisations in supplying the appropriate service without duplication.

# The characteristics of victims of fraud

## Impact on wider business community

There are certain crimes whereby the sensitivity of their nature can often prevent the victim from reporting it to the authorities. It was not so long ago that those who suffered at the hands of domestic violence faced a similar scenario - domestic violence was something that occurred 'behind closed doors'. There was simply no encouragement to report such matters and therefore victims were entirely dissuaded from doing so and made to feel that they shouldn't. However, recognition of domestic violence as a serious criminal act now ensures that its victims are no longer overlooked by the enforcement and support communities. The same cannot currently be said for fraud victims. The embarrassment that is attached to 'falling for a scam' is a key reason that prevents many victims from reporting. Moreover, if someone does choose to report a fraud committed against them. Who do they report it to? The police, OFT, CAB, FSA, Consumer Direct to name some. Once they decide who to approach one of them they then might face a response such as, 'this is not our responsibility' (particularly from the police outside the City of London and London) or be referred elsewhere. They might also receive an unsympathetic response or worse even blamed. They are also reporting in an environment where there has until the formation of the NFA, been little interest in the standards of provision for fraud victims or pressure to enhance performance. There are also no clear national standards or protocols applied to fraud. Thus in an area where there are challenges to deal with victims for fraud the environment is much harder.

It is also worth illustrating the plurality of provision by highlighting the wide range of organisations that can become involved with victims of fraud.

**Figure 6**
**Providers of support to victims**

| Identity | Mass marketing/ investment |
|---|---|
| Company (bank, credit card, mobile phone, UK Payments, etc) | Statutory (police, SFO, FSA, OFT, Consumer Direct, local authority |
| Credit agency | Private (CAB, trade association, etc) |
| CIFAS | Victim Support, Help the Aged |
| Statutory (police, SFO, FSA) | (Specialist: ThinkJessica) |
| Victim Support, Help the Aged | CPS |
| (Specialist: Ecrime.org) | |
| CPS | |

# The characteristics of victims of fraud

## What do victims want?

The limited research that has been undertaken on victims has provided some analysis of what victims of fraud actually want. Some of the most common issues will now be explored.

### Individual case worker

Pascoe et al (2006) in a review of victims of identity fraud have suggested many victims want an individual case worker to deal with their case from when a report is filed, through to court (should it reach that far). Added to this is the complication of multiple agencies involved in the process, which makes it even more difficult for victims to comprehend the process, particularly the more vulnerable.

### Kept up-to-date on the progress of the case

A common theme amongst victims of almost any crime is a desire to be kept up-to-date with the progress of the case. Victims want to know if its been investigated if the culprits have been identified, have they been charged, were they found guilty and if so what was their sentence (Pascoe et al 2006).

### Service providers to adopt a more sympathetic approach

The section above demonstrated that many victims of fraud do not report. For some of them, it is because of the attitudes they face when they attempt to report. The nature of some frauds lead to questions concerning whether the case is actually a crime, if it is the responsibility of another agency. Thus for many victims simply been treated with sympathy is important (Pascoe et al, 2006).

### Staff better trained in how to deal with victims

There are many people dealing with fraud victims who have no specialist knowledge of fraud. Frauds are complex and diverse and it is not possible to create a 'one size fits all' fix for fraud, which meets the needs of all victims. For example, a person who has been subjected to an identity fraud, not only has needs related to the emotional impact, but also specialist needs of restoring credit ratings and avoiding further victimisation. A victim of chronic scams who is elderly and convinced the lotteries entered are real, thus denying they are even a victim, and who as a consequence has fallen out with family members. Trying to stop them has a completely different set of needs. Staff involved in this area therefore need to be trained in general principles of victim support, as well as more specialist areas, particularly if they are looking to provide services to all types of fraud victims (Pascoe et al, 2006).

### Better and clearer information

There are some victims who report who may receive no information. On the other hand, there are others who will be provided with extensive resources. There is lots of guidance available to victims of fraud in the forms of leaflets, websites, DVDs etc produced by some of the wide range of bodies involved. Many examples of best practice can be found by utilising the best resources with the clearest messages, which would be advantageous for many victims (Pascoe et al, 2006).

# The characteristics of victims of fraud

## Restitution and compensation

For victims of identity fraud, once fraud has been proven and there is no evidence of negligence funds are usually restored if they have been stolen. There may, however, be other costs that are borne by the victim, for which individuals would like compensation. For many of the other types of fraud restitution is not only difficult but very unlikely (Fraud Review Team, 2006; and Pascoe et al, 2006).

## Not to be victimised

A priority for many victims is not to be targeted again by fraudsters. Clearly the evidence from the criminals is that once a person has become a victim of fraud they are at high risk of being victimised again. Therefore measures that can be taken to make this less likely are also important for victims (Fraud Review Team, 2006).

## Offender punished

A simple desire for many victims is for the person who committed the fraud to be brought to justice and punished (Fraud Review Team, 2006). As has already been alluded to, for many frauds, investigation is unlikely, let alone a successful investigation, verdict and punishment.

# Conclusion

**This review has illustrated the diversity of frauds that affect individuals and small businesses. Some of the frauds and scams that are used by fraudsters were considered, along with the techniques they use to perpetrate them.**

A brief overview of those who commit the frauds was provided and a description of them as 'scampreneurs' established. The review then went on to examine the victims, providing some of the different typologies that have been developed. Analysis was provided drawing upon the research of a range of studies, profiling the different types of fraud victims. The review then went on to explore why some do not report frauds, along with the impact of them upon the individual. Finally, the review assessed the current infrastructure for victims of fraud, illustrating the plural provisions and ending with an overview of what victims want.

# Glossary

**Boiler Rooms** – a term used to describe a hub of sales-persons usually engaging in high pressure selling of worthless investments or other items. 'Boiler' is used because of the high pressure.

**Phishing** – emails sent out with the purpose of tricking the target into revealing personal data which can then be used by the fraudster.

**419 Scams** – scams where the person is tricked into engaging in what seems like an illegitimate scam by a corrupt official in another country to launder money for which they will receive a share. An advanced fee needs to be paid to start the process and the victim never sees that or the loot.

# References


Aleem, A (2007)
**Social Engineering: A Threat to Corporate Security**
**SMT Online**
Retrieved, 20 March, 2009 from http://www.info4security.com/story.asp?sectioncode=10&storycode=4113958

Allison, S F, Schuck, A M and Lersch, M (2005)
**Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/Offender Characteristics**
**Journal of Criminal Justice** 33, pp 19-29.

**Bank Safe Online (2009) Trojans Explained**
Retrieved on 18 March, 2009 from http://www.banksafeonline.org.uk/trojans_explained.html

Carach, C, Graycar, A and Muscat, G (2001)
**The Victimisation of Older Australians. No 212**
Canberra: Australian Institute of Criminology.

Carter, S and Jones-Evans, D (2006)
**Enterprise and Small Business**
London: Prentice Hall.

Charlton, K and Taylor, N (2005)
**Online Credit Card Fraud Against Small Businesses**
Canberra: Australian Institute of Criminology.

Consumer Direct (n.d.)
**Watch Out Online Dating Scams**
Retrieved on March 20, 2009 from http://www.consumerdirect.gov.uk

Copes, H, Kerley, KR, Mason, KA. and Wyk, JV (2001)
**Reporting Behavior of Fraud Victims and Black's Theory of Law: An Empirical Assessment**
**Justice Quarterly** 18, pp 343-363.

Deem, DL (2000)
**Notes from the field: Observations in Working with the Forgotten Victims of Financial Crimes**
**Journal of Elder Abuse and Neglect** 12, pp 33-48.

Doig, A (2006)
**Fraud**
Cullompton: Willan.

Downs, J S, Holbrook, MB and Cranor, LF (2006)
**Decision Strategies and Susceptibility to Phishing**
Retrieved on 20 March, 2009 from http://cups.cs.cmu.edu/soups/2006/proceedings/p79_downs.pdf

Experian (2008)
**Victims of Fraud Dossier: Part IV**
London: Experian.

Federation of Small Businesses (2009)
**Inhibiting Enterprise Fraud and Online Crime Against Small Business**
London: FSB.

Fraud Advisory Panel (2006)
**Victims of Fraud**
London: Fraud Advisory Panel.

Fraud Review Team (2006)
**Final Report**
London: The Legal Secretariat to the Law Offices Annex D.

Ganzini, L, McFarland, B and Bloom, J (1990)
**Victims of Fraud: Comparing Victims of White collar and Violent Crime**
**Bulletin of the American Academy of Psychiatry and Law** 18, pp 55-63.

Grabosky, P and Duffield, G (2001)
**Red Flags of Fraud. No 200**
Canberra: Australian Institute of Criminology.

# References


Hines, J (2001)
**Telemarketing Fraud Upon the Elderly: Minimizing its Effects through Legislation, Law Enforcement and Education**
**Albany Law Journal of Science and Technology** 12, pp 839-862.

Holtfreter, K, Reisig, MD. and Pratt, TC (2008)
**Low Self control, Routine Activities and Fraud Victimisation**
**Criminology** 46, pp 189-220.

Home Office Identity Fraud Steering Committee (n.d.)
**What is Identity Fraud**
Retrieved on 5 August, 2009 from http://www.identitytheft.org.uk/identity-crime-definitions.asp

Identity Fraud Steering Group (2008)
**New Estimate on the Cost of Identity Fraud to the UK Economy**
Retrieved on the 22 April, 2009 from http://www.identitytheft.org.uk/cms/assets/Cost_of_Identity_Fraud_to_the_UK_Economy_2006-07.pdf

Langenderfer, J and Shimp, TA (2001)
**Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion**
**Psychology and Marketing** 18, pp 763-783.

Levi, M (2008a)
**Organized Frauds and Organising Frauds: Unpacking the Research on Networks and Organisation**
**Criminology and Criminal Justice** 8, pp 389-419.

Levi, M. (2008b)
**The Phantom Capitalists**
Revised Edition. Aldershot: Ashgate.

Mason, KA and Benson, ML (1996)
**The Effects of Social Support on Fraud Victims' Reporting Behaviour: A Research Note**
**Justice Quarterly** 13, pp 511-524.

Morton, J and Bateson, H (2007)
**Conned: Scams, frauds and Swindles**
London: Portrait Books.

Muscat, G, James, M and Graycar, A (2002)
**Older People and Consumer Fraud Number 220**
Canberra: Australian Institute of Criminology.

Newman, GR and McNally, M (2005)
**Identity Theft: Literature Review**
Washington DC: US Department of Justice.

Office of Fair Trading (2006)
**Research on Impact of Mass Marketed Scams**
London: Office of Fair Trading.

Pascoe, T, Owen, K, Keats, G and Gill, M (2006)
**Identity Fraud: What About the Victim**
Leicester: Perpetuity Research and Consultancy International.

Reisig, MD and Holtfreter, K.(2007)
**Fraud Victimisation and Confidence in Florida's Legal Authorities**
**Journal of Financial Crime** 14, pp 113-126.

Semmens, N (1999)
**When the World Knows Your Name: Identity Theft and Fraud in the UK**
**Scottish Journal of Criminal Justice Studies** 7, pp 80-91.

Shichor, D, Sechrest, D and Doocy, J (2001)
**Victims of Investment Fraud**
In, Pontell, HN and Shichor, D (eds)
**Contemporary Issues in Crime and Criminal Justice: Essays in Honour of Gilbert Geis**
Upper Saddle River (USA): Prentice Hall.

# References


Shover, N, Coffey, GS and Hobbs, D (2003)
**Crime on the Line**
**British Journal of Criminology** 43, pp 489-505.

Smith, R.G, Holmes, MN and Kaufmann, RG (1999)
**Nigerian Advanced Fee Fraud. No 121**
Canberra: Australian Institute of Criminology.

Spalek, B. (1999)
**Exploring the Impact of Financial Crime: A Study Looking into the Effects of the Maxwell Scandal upon the Maxwell Pensioners**
**International Review of Victimology**
6, pp 213-230.

Starnes, RA (1996)
**Consumer Fraud and the Elderly: The Need for a Uniform System of Enforcement and Increased Civil and Criminal Penalties**
**Elder Law Journal** 4, pp 201-224.

Stevenson, R.J (1998)
**The Boiler Room and Other Telephone Sales Scams**
Chicago: University of Illinois Press.

Titus, RM (1999)
**The Victimology of Fraud**
Paper presented to the Restoration of Victims of Crime Conference, Melbourne, Australia, September 1999.

Titus, RM and Gover, AR (2001)
**Personal Fraud: The Victims and the Scams**
**Crime Prevention Studies** 12, pp 133-151.

Titus, RM, Heinzelman, F and Boyle, JM (1995)
**Victimisation of Persons by Fraud**
**Crime and Delinquency** 41, pp 54-72.

Tive, C (2006)
**419 Scam**
Lincoln (USA): iUniverse.

Van Duyne, PC. (1996)
**Organised Crime in Europe**
New York: Commack.

Van Wyk, J and Benson, ML (1997)
**Fraud Victimisation: Risky Business or Just Bad Luck**
**American Journal of Criminal Justice**
21, pp 163-179.

Vaughan, D and Carlo, G (1975)
**The Appliance Repairman A Study of Victim-Responsiveness and Fraud**
**Journal of Research in Crime and Delinquency**
2, pp 153-161.

Walker, RH and Levine, DM (2001)
**"You've Got Jail": Current Trends in Civil and Criminal Enforcement of Internet Securities Fraud American Criminal Law Review**
38, pp 405-429.

# Appendices

## Appendix 1. The techniques of fraudsters

| Type of scam | Use of latest technology | Professional and legitimate appearance | Illegitimate appearance | Small print | Good sales pitch | Selling dream | Legal hinterland | Intimidation and violence |
|---|---|---|---|---|---|---|---|---|
| **Gambling** | | | | | | | | |
| Prizedraw and sweepstake scams | | ✓ | | ✓ | | ✓ | ✓ | |
| Foreign lottery scams | | ✓ | | ✓ | | ✓ | ✓ | |
| Bogus tipsters | | ✓ | | ✓ | | ✓ | ✓ | |
| **Money making** | | | | | | | | |
| Pyramid selling and chain letter scams | | ✓ | | ✓ | | | ✓ | |
| Internet matrix scams | | | | ✓ | | | ✓ | |
| **Bogus products and services** | | | | | | | | |
| Miracle health and slimming cure scams | | ✓ | | ✓ | | ✓ | ✓ | |
| Premium rate and telephone prize scams | | | | ✓ | | | ✓ | |
| Clairvoyant and psychic mailing scams | | | | ✓ | | ✓ | ✓ | ✓ |
| Career opportunity scams | | ✓ | | | | ✓ | ✓ | |
| Loan scams | | ✓ | | | | | ✓ | |
| **Illicit scams** | | | | | | | | |
| African advanced fee frauds/foreign making scams | | | ✓ | | | | | ✓ |
| **Technological trick scams** | | | | | | | | |
| Internet dialler scams | ✓ | | | | | | | |
| High risk | | ✓ | | | ✓ | ✓ | | |
| Property investment | | ✓ | | | ✓ | ✓ | | |
| **Identity** | | | | | | | | |
| Identity fraud | ✓ | | | | | | | |

Source: OFT (2006), Pascoe et al (2006), Experian (2008).

# Appendices

## Appendix 2. Victim profiles

| Type of scam | Victim profile | Report | Number of victims | Financial impact individual | Total financial impact annually |
|---|---|---|---|---|---|
| **Gambling** | | | | | |
| Prizedraw and sweepstake scams | Female (57%)<br>35-64 (66%) | Low reporting to police (2%) | 380,000 | £33 median | £60 million |
| Foreign lottery scams | Male (53%)<br>35-64 (58%)<br>65+ (24%) | Low reporting to police (3%) or to local authority (2%) | 140,000 | £42 median | £260 million |
| Bogus tipsters | | | | | £5 million |
| **Money making** | | | | | |
| Work at home and business opportunity scams | Female (53%)<br>35-64 (61%)<br>under 34 (29%) | Low reporting to OFT/ local authority (2%) or to police (1%) | 330,000 | £43 median | £70 million |
| Internet matrix scams | Female (61%)<br>35-64 (70%) | No reports to authorities | 70,000 | £53 median | £10 million |
| **Bogus products and services** | | | | | |
| Miracle health and slimming cure scams | Female (78%)<br>35-64 (70%) | Low reporting to any statutory body (1%) | 200,000 | £46 median | £20 million |
| Premium rate and telephone prize scams | Male (53%)<br>35-64 (68%) | Low reporting to BT (2%) and police (1%) | 1.08 million | £14 median | £80 million |
| Clairvoyant and psychic mailing scams | Female (70%)<br>34 and younger (31%) | Low reporting to statutory agency (1%) | 170,000 | £36 median | £40 million |
| Career opportunity scams | Female (65%)<br>35-64 (65%)<br>under 34 (26%) | No reporting to authorities | 70,000 | £155 median | £30 million |
| Loan scams | Female (53%)<br>35-64 (66%)<br>65+ (18%) | Low reporting to police (3%), CAB (3%), Bank (2%) and DTI (1%) | 110,000 | £376 median | £190 million |
| **Illicit scams** | | | | | |
| African advanced fee frauds/foreign making scams | Male (64%)<br>35-64 (69%) | Low reporting, but higher than average to police (9%) | 70,000 | £2858 median | £340 million |
| **Investment frauds** | | | | | |
| High risk | Male (71%)<br>65+ (34%) | Medium 9% to police and 5% to OFT | 90,000 | £2751 median | £490 million |
| Property investment | Male (65%)<br>35-64 (76%)<br>London (25%) | Very low 45 to police | 40,000 | £251 median<br>(but 4,240 mean) | £160 million |
| **Identity** | | | | | |
| Identity fraud | Male 26-45<br>Professional director | Very high | 100,000 | £1303 | £1.2 billion |

Source: OFT (2006), Pascoe et al (2006), Experian (2008), Identity Fraud Steering Group (2008)
Note: Where there are gaps, there was no information available of sufficient quality to enter.

National Fraud Authority

National Fraud Authority
PO Box 64170
London WC1A 9BP

www.attorneygeneral.gov.uk
T 020 3356 1000