

# FRAUDSCAPE

Depicting the UK's fraud landscape

[www.cifas.org.uk](http://www.cifas.org.uk) | March 2013



**C I F A S**

The UK's Fraud Prevention Service

# In this Report . . .

<b>1. Executive Summary</b> . . . . .	<b>4</b>
<b>2. CIFAS National Fraud Database</b> . . . . .	<b>6</b>
2.1 Overview . . . . .	6
2.2 Fraud by Fraud Type . . . . .	7
<b>3. Identity Related Crime</b> . . . . .	<b>9</b>
3.1 Identity Fraud . . . . .	11
3.2 The Geography of Identity Fraud . . . . .	16
3.3 Facility Takeover Fraud . . . . .	19
3.4 Who was Targeted? . . . . .	22
3.5 The Location of Identity Crime. . . . .	26
<b>4. The Fraud Landscape</b> . . . . .	<b>30</b>
<b>5. How Organised is Organised Crime?</b> . . . . .	<b>34</b>
<b>6. First Party Fraud</b> . . . . .	<b>35</b>
6.1 Misuse of Facility Fraud . . . . .	36
6.2 Application Fraud . . . . .	39
6.3 Asset Conversion Fraud . . . . .	44
6.4 False Insurance Claims . . . . .	46
6.5 Who is the First Party Fraudster? . . . . .	47
<b>7. Defeating Fraud: Whose Responsibility is it Anyway?</b> . . . . .	<b>51</b>
<b>Appendix: Fraud by Product Type</b> . . . . .	<b>53</b>

CIFAS is a not-for-profit organisation, concerned solely with the prevention of fraud and funded by subscription. Since February 1991 CIFAS has been an independent Company Limited by Guarantee. CIFAS Members are drawn primarily from the UK financial services industry, but also from telecommunications, insurance, other business sectors and the public sector.

Website: [www.cifas.org.uk](http://www.cifas.org.uk)      [www.identityfraud.org.uk](http://www.identityfraud.org.uk)

CIFAS - A company limited by Guarantee. Registered in England and Wales No.2584687 at  
6th Floor, Lynton House, 7-12 Tavistock Square, London WC1H 9LT



# Introduction

CIFAS is the UK's Fraud Prevention Service, a not-for-profit membership organisation operating in the public interest and dedicated to the prevention of fraud and financial crime. It has 270 Members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring, share dealing and the public sector. Members share information about confirmed frauds in the fight to prevent further fraud.

The CIFAS National Fraud Database contains records of confirmed frauds that have been perpetrated or attempted against CIFAS Member organisations. In order to be recorded on the CIFAS Database a case must satisfy a standard of proof. This means that there must be sufficient evidence to take the case to the police, although it is not mandatory to do so.

Intelligent data sharing allows CIFAS Members to detect, target and prevent fraud and the resulting data contained in this report provides a robust and reliable set of figures for 2012. As Members share information on confirmed frauds only, the frauds recorded to the CIFAS National Fraud Database offer a clear picture of the fraud landscape in the UK. In 2012, fraud rose by 5% compared with the previous year. Following on from the previous high benchmark and 9% increase noted in 2011, this can only be seen as evidence of the challenge posed to the UK economy.

Analysis is presented by the type of fraud being committed (for example, Identity Fraud or Application Fraud), with information contained throughout the report relating to the types of product targeted (e.g. bank accounts or mortgages). An explanation of each fraud type can be found throughout this report, together with definitions of terminology, references to the techniques used by fraudsters and case studies of frauds and fraudsters who have been apprehended or detained.

Frauds are never mutually exclusive, however. For example, Application Fraud can be committed on bank accounts, mortgages or credit cards, among others. Similarly, each product can be attacked in a number of different ways – a bank account could be targeted by fraudsters committing Application Fraud, Identity Fraud or Facility Takeover Fraud.

The motivations to commit fraud, the impact of organised crime, the economic circumstances that organisations and individuals face, and the steps that have or have not been taken are constant themes in this report. We examine what has happened with what needs to happen and look at who is responsible for the frauds, as well as who needs to be responsible for the prevention of it.

Only by analysing fraud in this way, and addressing the issues raised, can organisations and individuals be ready to anticipate, prevent and combat whatever will come next.

# 1. Executive Summary

In the last edition of *Fraudscape*, CIFAS revealed that the frauds recorded during 2011 were at an unprecedented level, and that Identity Related Crimes (frauds that rely on the abuse of identity details) accounted for 58% of all the frauds recorded that year. In 2012, the upward trend continued. The total number of frauds recorded during 2012 now stands at 248,325: a 5% increase. Further analysis reveals that;

- Identity Fraud and Facility (or Account) Takeover Fraud accounted for 65% of all frauds identified. Data has undoubtedly become the key enabler of fraud in the UK, and the links with organised crime cannot be overlooked.
- The economy continued to play a prominent role in the fraud landscape: acting as a likely driver for many frauds, an influence on the types of fraud being committed and – also – a disguise for much fraud that has escaped detection.
- All types of first party fraud (those committed by the named account holder where no proof of compromised identity details existed) decreased in 2012 when compared with the previous year. This cannot be seen as a success in isolation, however, as there were other factors at work which conspired to result in much of it remaining undetected.
- The fraudulent use of a legitimately obtained account (Misuse of Facility Fraud) decreased during 2012 compared with the previous year's figures. It still represented the second most common type of fraud recorded by UK organisations however. Many bore the hallmarks of 'money mule' activity (indicating the presence of organised crime).
- The continued migration of fraudsters to new products, first identified in 2009, continued. Although 2012 revealed that the attention of fraudsters does wander, some products remained key targets.
- 80% of identity related crime was attempted or committed using the internet.
- Men were far more likely to be Victims of Impersonation than women, with over 60% of Victims of Impersonation for the five most commonly targeted products being male. Similarly, Victims of Account Takeover were also more likely to be men, except on mail order accounts – where over 80% were women. Although the ages of victims were more diverse, those in their 40s were the most likely to be targeted by fraudsters.
- Geographical analysis demonstrated that, as with 2011, Victims of Takeover were far more likely to be spread out geographically than Victims of Impersonation who were more concentrated into large urban areas. Numerous fraud hotspots in 2012 were also identified.
- Collaborative research with Ordnance Survey has looked at Victims of Impersonation and the types of property in which they reside. Initial findings (see page 16-17) have dispelled the long-held belief that individuals living in flats are more likely to fall victim to Identity Fraud.

## Data: the fraudster's currency of choice

The abuse of identity details accounted for almost two thirds of all fraud recorded in 2012, confirming that data has become the fraudster's chosen route to financial gain.

The products most commonly targeted by identity fraudsters and account hijackers (such as mail order, bank and plastic card accounts) underlined the severity of the challenge this poses to organisations and individuals. With many larger organisations having refreshed their online security processes during 2012, and with numerous high profile stories about lapses in security, organisations need to become smarter in their real time approach to preventing fraud at the point of application or transaction.

Equally, individuals have their own responsibilities if they are not to bear the brunt of the challenge posed by data enabled crime. They themselves need to keep personal data safe both online and in the real world or face – potentially – an increasing challenge in proving their innocence if they become a victim of fraud.

### Misuse of an account - the money mule issue

In spite of the reported decrease in first party frauds, they are still important. The misuse of bank accounts, especially those bearing the hallmarks of 'money mule' activity (where a person is recruited, knowingly or unknowingly, to allow his/her account to receive and transfer funds as part of a money laundering endeavour), represents a serious challenge to law enforcement, businesses and individuals. The persistence of these frauds demonstrates the need for a more comprehensive, joined up, approach. For example, organisations and others need to educate customers to understand more clearly what constitutes fraud and the possible ramifications, while law enforcement should continue to target the key enablers and methods used by criminals to recruit money mules.

### What remains unseen?

The stark reality is that much fraud simply evades detection as, when applications do not meet an organisation's lending criteria, they often do not get passed to their fraud department. This means that the level of fraud detected was potentially only the tip of the iceberg, which does not bode well for coming years.

### Variety – the spice of the fraudster's life

Some products will always be targets for fraudsters. Trying new targets, however, is also a constant. Plastic card and bank accounts were particularly popular with criminals taking over accounts in 2012, even though cases of Identity Fraud against bank accounts fell by 38% and against plastic card accounts rose by 26%. 45% increases in fraud levels against loans and mail order accounts also demonstrated the dynamism and flexibility of the fraudster. They switch *en masse*: as one door closes, another one opens.

### The constants

There were some constants. The explosion in data driven identity related crime meant that more individuals (across a wider demographic) were targeted than previously, and that the fraudster of today still has some favoured approaches and targets. The internet remained the channel of choice for fraudsters. And while more women, across a more diverse age range, became victims of fraud, the male in his forties

was still, statistically, more likely to be a victim of fraud than any other combination of age range and gender.

### Fraud and organised criminality

Similarly, fraud remained an activity with long-standing links to the world of organised crime. Practically two thirds of all fraud related to the misuse of data (with the obvious links to data hacking and internal compromise of data by staff who were complicit with or had been targeted by criminal gangs). Misuse of Facility Fraud (many of which related to the criminal misuse of accounts in order to launder money) was the second most common fraud. These facts combined provide the clearest indication possible of the deep links between fraud and organised criminal activity. The challenge this poses, particularly to industry, law enforcement and government, is something that will need to be addressed in an equally organised and joined up way.

### Myths: dispelling them

Finally, through data sharing and collaboration, traditional assumptions can be challenged. Initial research by CIFAS and Ordnance Survey has indicated that the long-held belief that those living in flats were more likely to fall victim to Identity Fraud is incorrect. While the area or region may influence a fraudster's approach, it would seem that this myth no longer stands up to scrutiny. •

## 2. CIFAS National Fraud Database

### 2.1 An overview

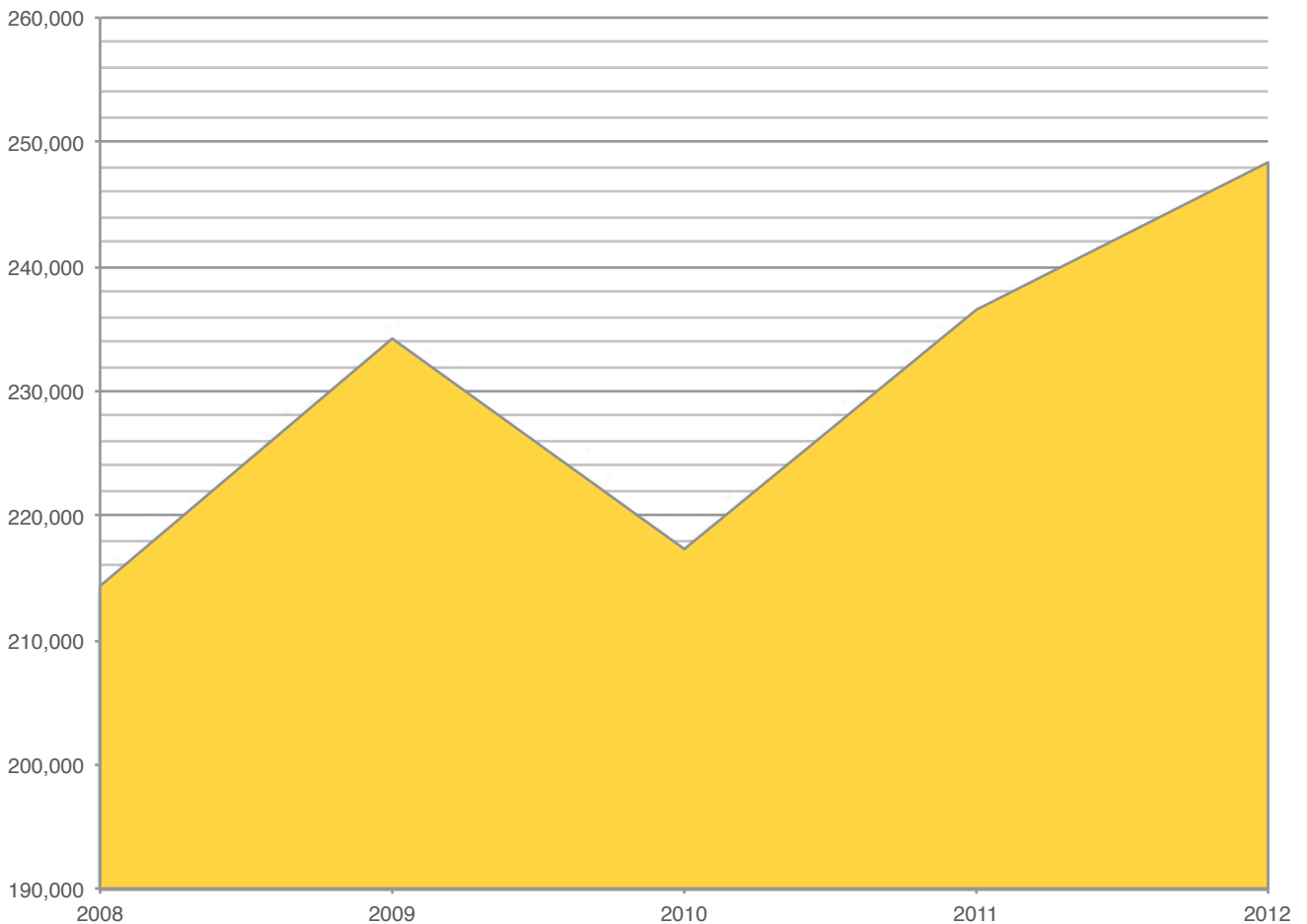
A total of 248,325 frauds were identified by CIFAS Members in 2012. This was an increase of 5% compared with 2011. These frauds were recorded to the National Fraud Database and the following report sets out an overview of the trends identified during recent years.

Figure 2.1.1 shows the number of frauds recorded to the National Fraud Database in the five years to the end of

2012. In the last edition of *Fraudscape* we reported that 2011 witnessed the highest number of frauds recorded by CIFAS Members in any one year. The number recorded in 2012 has surpassed the 2011 total, setting another milestone in the identification and recording of fraud cases by CIFAS Members and nudging a quarter of a million cases. ●

Total Frauds recorded on the National Fraud Database 2008-2012

Figure 2.1.1



## 2.2 Fraud by Fraud Type

Frauds recorded by Fraud Type in 2011-2012

Table 2.2.1

Fraud Type	2011	2012	% change
Asset Conversion Fraud	532	337	-36.7%
Application Fraud	43,263	39,868	-7.8%
False Insurance Claims	396	279	-29.5%
Facility Takeover Fraud	25,070	38,428	+53.3%
Identity Fraud	113,259	123,589	+9.1%
Misuse of Facility Fraud	53,996	45,824	-15.1%
<b>Total</b>	<b>236,516</b>	<b>248,325</b>	<b>+5.0%</b>

The table above shows that, of the six types of fraud identified and recorded by CIFAS Members, only those involving the abuse of identity information have increased. Most evident is the 53% increase in the number of Facility Takeover Frauds recorded in 2012 compared with 2011. Each of these cases represents an instance of a fraudster attempting to gain access to the account of an innocent victim. Disturbingly, this happened over 38,000 times in 2012, putting this type of fraud, volume-wise, on a par with Application Fraud and Misuse of Facility Fraud – two types of first party fraud (fraud committed by the genuine account holder) which have traditionally dwarfed the amount of Facility Takeover Fraud identified. This means that the overall 5% increase in the total number of all frauds recorded in 2012 was driven exclusively by identity crime: signalling louder than ever before the changing landscape of fraud in the modern UK economy and the dominance that organised crime now has in the fraud landscape.

The 53% surge in Facility Takeover Fraud was an area of real concern, but it must also be noted that the number of such frauds was actually less than a third of the number of cases of Identity Fraud. Identity Fraud increased by just over 9% during 2012, bringing the total of recorded cases to over 123,000 for the year.

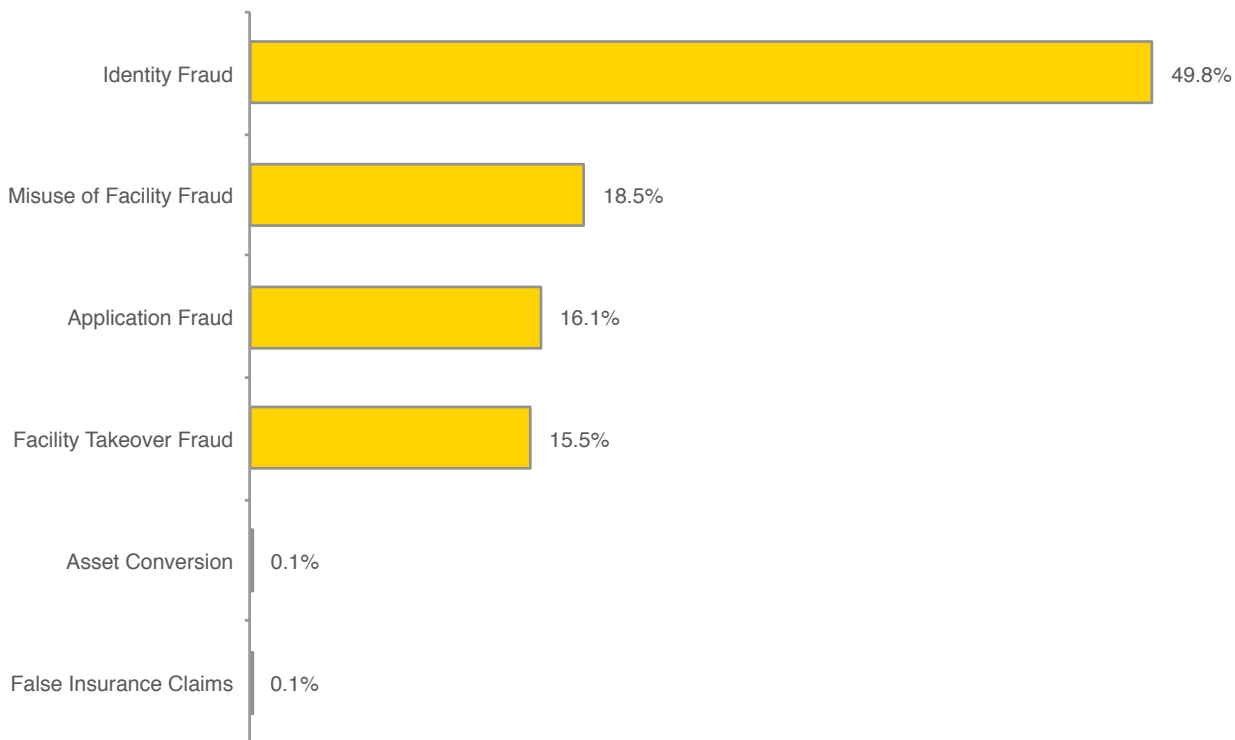
This means that over 162,000 of the frauds that were identified in 2012 involved the abuse of identity information, with the vast majority resulting in an innocent member of the public being adversely affected. This staggering figure represents almost two thirds of all the frauds identified by CIFAS Members, making identity related crime one of the most commonly perpetrated and recorded crimes occurring in the UK at the moment. This can be seen in *Figure 2.2.1*.

2012 witnessed an overall decrease in the number of first party frauds: those frauds committed by the genuine account holder or applicant, in his or her own name. This will include such frauds as telling lies to obtain products and services (Application Fraud), or the fraudulent abuse of the account after it has been legitimately opened (Misuse of Facility Fraud). The decreases seen in Application Fraud, Asset Conversion Fraud (selling an asset – such as a vehicle – that is not theirs to sell) and False Insurance Claims was a continuing trend, but the reduction in Misuse of Facility Fraud was in contrast to the large increase seen in 2011 – although the level recorded in 2012 remained higher than in 2010.

The reasons behind these changing fraud levels included technological, economic and societal factors. These will be examined in more detail throughout this report. •

### Types of Fraud recorded in 2012

Figure 2.2.1



The UK's Fraud Prevention Service

## Protective Registration Service

CIFAS Protective Registration is a service that enables individuals to seek protection against possible impersonation attempts when they have good reason to believe that their details might be used by a fraudster.

As a result of Protective Registration, CIFAS Members will undertake additional checks to make sure that the applicant is genuine and not a fraudster trying to commit Identity Fraud. This offers reassurance that the identity of an individual (who has taken out Protective Registration because they are at heightened risk of Identity Fraud) is protected against fraudulent applications in his or her name.

Visit [www.cifas.org.uk/pr](http://www.cifas.org.uk/pr) for more information about CIFAS Protective Registration.



## 3. Identity Related Crime

This section examines those frauds that involved the abuse of identity details – be that by claiming to be another person to obtain access to their account (Facility or Account Takeover Fraud), or using their name to make new applications for goods or services and/or concocting an entirely fictitious identity (both forms of Identity Fraud).

### What is Identity Fraud?

The concept of identity has evolved over time.

For some people, the argument is that without a system such as a mandatory national identity card, an identity becomes a tapestry of details. These details can take the form of documentation – most obviously a passport or driving licence – but also information: name, address, date of birth and so on. As society has veered away from the ‘traditional’ model of a pre-arranged meeting with a bank manager in order to obtain a loan, so too has the concept of personal information being solely your name, date of birth and address. People have differing opinions as to what constitutes personal information and, as a result, what constitutes the abuse of it. Most people would accept that someone’s name and date of birth identifies them (although maybe not uniquely). There may be more debate, however, about whether a mobile phone number is counted as identity information. To a lot of people it may well not be, but to the mobile phone company whose network that phone uses, the number is a far better personal identifier than the user’s name. This means that while a solitary piece of information may mean nothing to the majority, provided that it means something to someone, then it needs to be protected with the same vigour as someone would protect his or her good name, as to the fraudster it is potentially just as valuable. After all, a fraudster does not necessarily need to know a potential victim’s full name and date of birth if they already have their online banking log-in details and password.

*Figure 3* (page 10) serves to illustrate that the majority of identity related crimes involved Identity Fraud (the use of the identity of an innocent victim, or the use of an entirely fabricated name, to apply for products and services). This is represented by the yellow section in the *Figure* below. It also shows that over the last two years, the volume of cases of Facility Takeover Fraud (represented by >

### Fraudster methods

While data is not exclusively obtained online, there are numerous tactics that fraudsters are known to try in order to harvest personal data using the internet. Some of the most notable include:

**Phishing:** the mass distribution of emails which appear to originate from legitimate sources (e.g. banks, charities, government departments) which direct victims to fake websites, install malware or encourage recipients to reveal personal information which is then collected by the fraudster.

**Malware:** malicious software that infects a victim’s computer. It can capture private information stored on the computer and send it to the fraudsters. Notable types include spyware (a type that collects little bits of information such as websites visited, passwords etc) and trojans (programmes that may appear to be legitimate but act maliciously – often giving fraudsters remote access to your computer).

**Hacking:** a means of attacking the computer systems of organisations or individuals in order to obtain personal details or other sensitive information.

**Social Engineering:** the manipulation of situations, to encourage people to divulge personal or confidential information. Notable examples have included the use of social networking and dating sites: where the fraudster uses an alias to strike up a rapport with the victim before requesting money or details.

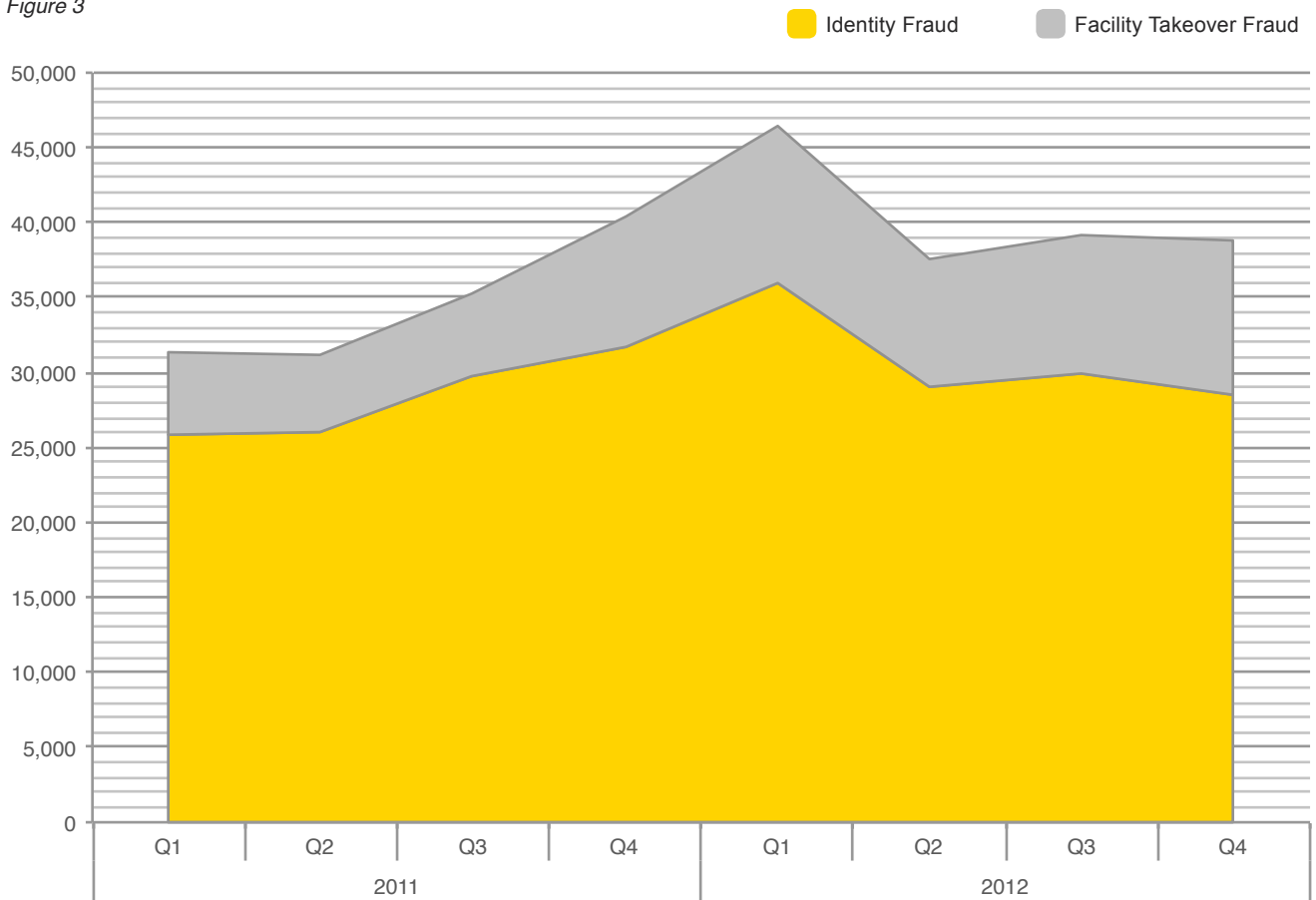
Clearly, anyone employing such tactics to obtain personal data can be considered to be acting in a highly organised manner with clear criminal intent.

the grey section), where the identity details being abused were more likely to be those pieces of less traditional, more organisation specific personal information, have acquired an increasing prominence. The most sobering fact, however, is that – when combined – these two identity crimes accounted for two thirds of all fraud identified during 2012. With these types of fraud being most likely to have been perpetrated by organised criminal elements, the situation becomes more worrying still for individuals, organisations and law enforcement alike (see page 34).

With identity related crimes, the question of ‘how are they perpetrated?’ always arises. The simple and sobering fact is that, of all the identity related crimes recorded in 2012, nearly 80% were attempted or committed online. The impact on the consumer of the internet is something all businesses and individuals have come to appreciate. The ease that it offers individuals, however, is also appreciated by the fraudster – allowing them to attempt fraud on an organised, near industrial scale. This also points towards the internet being the main facilitator for the harvesting of the data which enables such frauds. ●

Identity related crimes recorded in 2011 and 2012

Figure 3



## 3.1 Identity Fraud

Identity Fraud includes cases of false identity (the use of an entirely fictitious identity) or the stolen identity of an innocent victim.

### Identity Fraud cases by product 2011-2012

Table 3.1.1

Product	2011	2012	% change
All-in-one	216	178	-17.6%
Asset Finance	325	282	-13.2%
Bank Account	14,873	9,236	-37.9%
Communications	25,996	18,864	-27.4%
Plastic Card	24,582	30,989	+26.1%
Insurance	27	32	+18.5%
Loan	3,795	7,104	+87.2%
Mail Order	38,336	54,480	+42.1%
Mortgage	68	59	-13.2%
Other	5,041	2,365	-53.1%
<b>Total</b>	<b>113,259</b>	<b>123,589</b>	<b>+9.1%</b>

Table 3.1.1 shows that within the 9% overall increase, four types of product experienced higher levels of Identity Fraud in 2012 than in 2011, while six have experienced a decrease from 2011 levels. By volume, the overall rise is being driven by Identity Fraud against mail order products and plastic cards, although the largest percentage increase was seen against loan products. The increases in Identity Fraud against loans and plastic cards represents an acceleration of a trend that began in 2011. The surge in Identity Fraud against mail order products is a return to an increase, following what would seem to have been a 'blip' of a 14% decrease during 2011. Curiously, two of the groups of products that fuelled the 10% increase in Identity Fraud last year (bank accounts and communications – predominantly mobile phone accounts) experienced quite substantial decreases in 2012. These fluctuations in the numbers of Identity Frauds recorded against the various products can be seen in Figure 3.1.1 (page 12).

### The ever changing choice of products: the return of an old favourite

It is clear from Table 3.1.1 that there was a lack of consistency in levels of change across the range of products in 2012. Evidently, fraudsters continue to adapt to changing circumstances, as do the organisations attempting to counter them. When the credit crunch hit, and credit was hard to obtain, the levels of Identity Fraud against plastic cards, specifically credit cards (historically, the identity fraudster's product of choice) plummeted. This was because it wasn't going to matter which names were used on the applications, it was highly likely that they were going to fail any organisation's credit scoring procedures – and therefore not be subject to fraud investigation before any fraud detection took place.

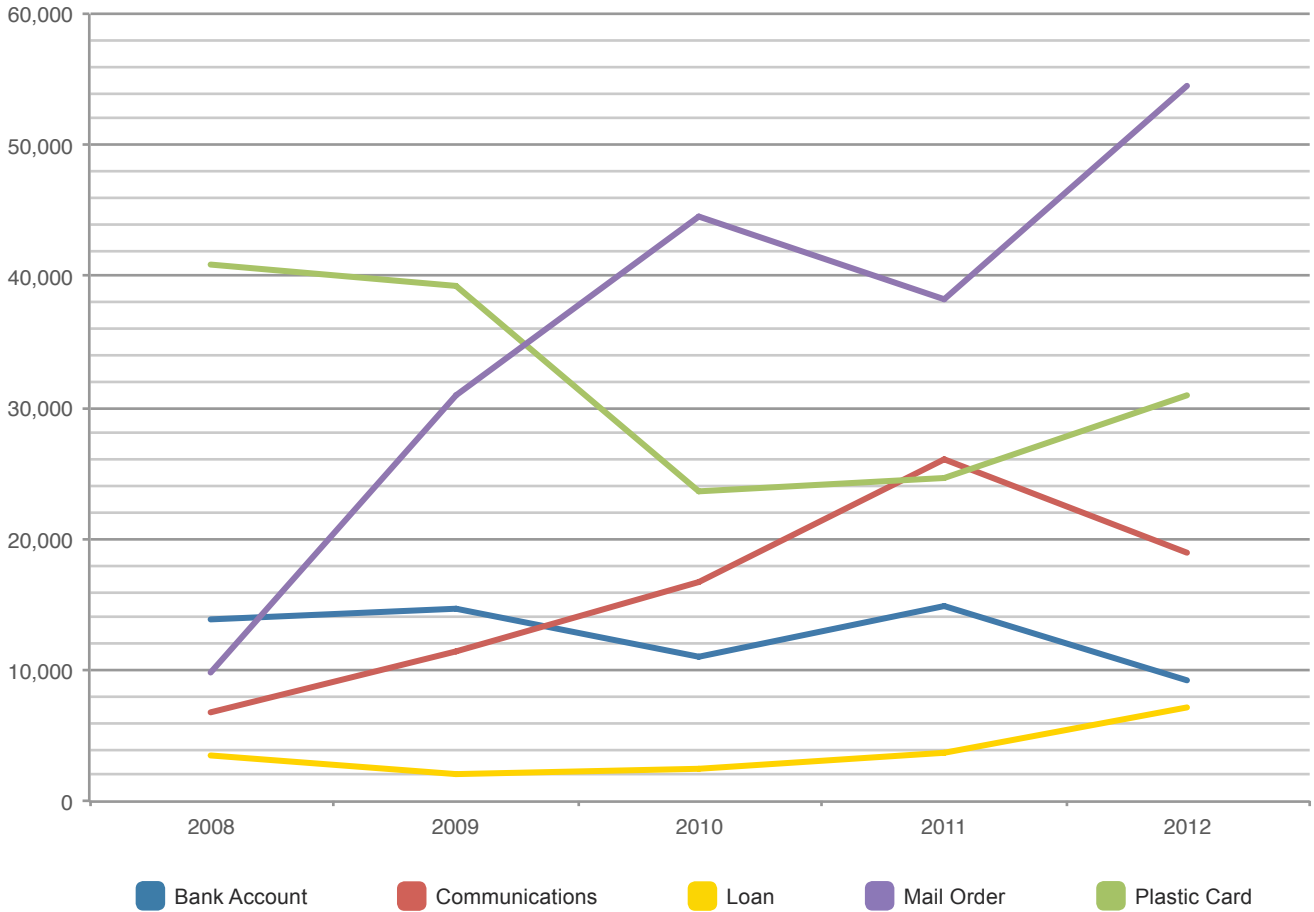
Now that the lending picture is a little bit more optimistic, it is not surprising that fraudsters are turning their attention back to this old favourite. In those credit fallow years, fraudsters looked to other products to fill the void. This was most obviously mail order, where the chances of approval were far greater and the amount of information required at application stage was less. This coincided with a period where there was a substantial expansion in the amount of personal data being captured and traded online – Experian reported that the amount of personal data traded online by fraudsters globally was up to almost 20 million pieces of information in the first six months of 2012\*.

Prior to 2012, this availability of information also fuelled a rise in Identity Fraud to obtain mobile phone contracts, offering the fraudster the chance to obtain high value handsets. As well as more data being available to fraudsters, to enable them to commit these frauds, the market for mobile phone technology and services remained highly competitive. This competition for business meant that the process of applying needed to be kept as attractive (i.e. hassle free) as possible for consumers – and sadly this resulted in it also being easier for the fraudster. The reduction seen in Identity Fraud to obtain mobile phone accounts is a reflection of the tightening up of this sector's application processes to ensure greater security. >

\* <http://press.experian.com/United-Kingdom/Press-Release/illegally-traded-data-soars-fourfold-in-two-years.aspx>

Identity Frauds recorded by product between 2008 and 2012

Figure 3.1.1



**Business innovation provides opportunity**

Product innovation, in particular in relation to loans, has also changed the Identity Fraud arena. The last couple of years have seen an explosion in the different types of loan that are now available. No longer is it simply the case of applying for a secured loan against a property, or a personal loan: the most obvious innovation is the appearance of the ‘payday loan’; where comparatively small amounts of cash are available very quickly, to be repaid over a short period of time. Other examples are peer-to-peer lenders (where an organisation brings together investors and borrowers) and the reappearance of guarantor loans (where the loan is guaranteed by a third party). Some of these products are designed to be easily accessible, but this makes them more susceptible to Identity Fraud attempts. This is largely because these new products are being offered by new entrants to the lending market. Such new entrants will always be a target for fraudsters as they seek to test the level of security and systems that such organisations have in place. In addition, the swift dissemination of information

over the internet means that any weaknesses identified can rapidly be shared among criminal forums – enabling the problem to grow more quickly.

The continuing move to online business has also benefited the fraudster. As more business is carried out online, so more Identity Fraud occurs online. This was again demonstrated in 2012, with an increase in both the number of Identity Fraud cases (up to well over 100,000) and the proportion of Identity Fraud cases occurring over the internet (84% of cases compared with 74% in 2011). The convenience that the internet affords the honest consumer is magnified for the fraudster. Not only do they get the advantages of being able to apply for products from the comfort of their own home (or any other place of their choice with a functioning internet connection – internet cafés being a popular choice), at any time, they can also make multiple applications quickly. In addition, the nature of online applications means that the fraudsters may well *not* have to produce any identity documentation and can perpetrate their

frauds without the inconvenience of anyone actually seeing them. In other words, the very nature of the consumer marketplace becomes a fraud enabler. While this is – perhaps – no surprise to the fraud prevention professional, it is a conundrum that organisations, consumers and society at large will increasingly have to confront. Will there come a point where stricter internet controls are called for? Will there need to be a sacrifice from consumers: a return to the longer waiting times for products and more in-depth, drawn out, application processes (which, of course, neither organisations nor consumers want)? Alternatively, will there be an increased imperative for individuals to protect their own details and data?

### The question of who

There is a lot of emphasis – correctly – being placed on organised fraudsters, or groups, who can be considered to be industrialising the perpetration of Identity Fraud (making large numbers of applications, using data that has been acquired in bulk). But this is not the whole story. The stereotypical ‘hacker’ sat in front of a computer is not the only perpetrator of Identity Fraud. In a minority of cases, the friends or family of the victim increasingly appear to be responsible for a number of the frauds – after all, who knows the victim better? And while the targeting of friends and family may sound unconscionable, the safeguards afforded victims of impersonation by UK regulations mean that the perpetrator can act safe in the knowledge that any ill effects that might be felt by their victim will, at least, not be financial.

It should also not be overlooked that (in *some* instances) the use of the word ‘victim’ may be misleading. ‘Co-conspirator’ may be a better term, or even ‘criminal’. It is a sad fact that some will seek to abuse the safeguards that are in place to protect the innocent by claiming to be just that, or stating that they have no idea who the perpetrator is when they do. This is an area of concern for organisations and police alike, and – soberingly – risks making it more difficult for genuine victims of fraud to prove their innocence. The reasons behind this vary: from an individual simply not wishing to honour the debt that they have incurred, through to a person ‘allowing’ their identity to be used in order to assist a friend or relative who might not be able to obtain credit in their own name. The simple fact is, no matter what the motivation, the net effect poses serious problems for organisations, individuals and the police when investigating cases of genuine impersonation and victimisation.

The overall problem with identity related crime of any kind, of course, is identifying who the fraudster actually is, not

## Case Study Amberhill

The Operation Amberhill team within the Metropolitan Police Service, in collaboration with the Criminal Records Bureau, National Fraud Intelligence Bureau and CIFAS, were able to identify and arrest an identity criminal who had been using a counterfeit French passport to obtain employment as a teacher using the identity of her brother-in-law’s ex-wife.

The Criminal Records Bureau, which works in partnership with the Metropolitan Police, issues vetting certificates for those who wish to take up employment with vulnerable people (young and elderly). Checks revealed that a counterfeit French passport had been used in a teaching application. This led to the Metropolitan Police liaising with the National Fraud Intelligence Bureau and identifying a record on the CIFAS database with a key address link to the person in question. This enabled the true identity of the suspect to be confirmed, facilitating arrest processes and the safeguarding of children.

This demonstrates both the value of data sharing but also the very real situations where stopping identity fraudsters is paramount for a wider good.

least because the details submitted appear to be completely genuine. When all details pertaining to ‘Mr John Smith’ (for example) are correct, and a new product/account is issued, only for it to be identified later as fraud, the organisation and victim are (in the majority of cases) equally left unable to ascertain who precisely was the fraudster.

One argument is that more information on identified frauds needs to be collected, thus identifying common aspects such as shared email addresses, phone numbers or IP addresses that may help to identify those behind prolific cases of Identity Fraud. However, while it might seem like an obvious solution, the ramifications in terms of privacy, data protection and so on are not to be overlooked. This is a debate that will doubtless become more prominent: where does fraud prevention and online security meet the right to privacy\*?

There are other, collaborative, efforts that could be made, however, in addition to sharing more information. Data sharing, of course, is merely one line of defence: without >

\* [www.guardian.co.uk/world/2013/feb/10/software-tracks-social-media-defence](http://www.guardian.co.uk/world/2013/feb/10/software-tracks-social-media-defence)

legal enforcement and punishment, fraudsters will remain free to attempt further frauds with nothing to deter them and, without individuals also taking care of and protecting their own details, any efforts made by organisations to be as secure as possible are undone. A collaborative approach, involving organisations, consumers, police and government, therefore, remains the most reliable option.

### How are Identity Frauds being committed?

So what is it that fraudsters are doing when they perpetrate Identity Fraud?

In the main, they are using the genuine current address of their victim. During 2012, this accounted for 74% of all Identity Frauds, up from 65% in 2011. By using the current address, the application looks 'genuine' to the organisation. They find, for example, that when they check such things as the voters' roll, the person named on the application is indeed recorded at that address. When other details such as date of birth also pass checks, then the application looks – to all intents and purposes – to be completely genuine.

This, however, presents the fraudster with a problem. How does he or she obtain (or intercept) any information that might be mailed out in relation to the application? After all, if the victim receives any mail that relates to an account that they didn't open, then the fraudster cannot achieve his or her aims. The good news for the fraudster is that in an increasing number of cases, the organisations that fraudsters are seeking to defraud are (through changing account management processes) inadvertently helping the fraudster. There has been a general trend for businesses to change from mailing statements or welcome letters, to emailing PDFs to their customers. One can see such electronic channels as a convenience for the consumer, an ecologically sound business practice or a money and time saving measure by business. No matter which way they are viewed, the lack of a paper trail is a bonus for the fraudster because no glaringly obvious giveaway lands on their victim's doormat.

This is not the case for all products, of course. There has been an increase in Identity Fraud to obtain credit cards, and those can't be delivered by email. This is an area where there needs to be a greater level of understanding. Just how does the fraudster ensure that he or she can get access to the documentation that they need, while still perpetrating the type of Identity Fraud that is most likely to be successful?

There are various tactics that fraudsters are known to employ in order to obtain mail relating to their fraud. These

## Case Study Fake Passports\*\*

The issue of the uses of fraudulent identities, and the criminal trade that accompanies it, is also illustrated by the case of a husband and wife from West London who were jailed in January 2013 for making and supplying false passports and identity documents.

Following the interception (in September 2012) of a package containing blank counterfeit Portuguese passports, and counterfeit holographic designs for use in passports at Coventry international postal hub, the couple's house was raided. There officials found further packages containing fake Dutch and French passports, laminated passport pages, counterfeit Schengen zone visas and bogus official stamps.

There was also evidence of money transfers made to Thailand, the source of the packages, and evidence that the counterfeit documents were being sold to illegal immigrants in the UK to make it look as though they had the right to work in the EU.

include using the Royal Mail Redirection service to get their victim's mail sent to an address which the fraudster has access to, or intercepting the postman or postwoman at the front door to trick him or her (using social engineering – see page 9) into handing them the mail. Some identity fraudsters have traditionally been known to target those living in flats where there are communal postal areas, or where post is easier to retrieve. This has led to the perception that living in flats increases the probability that an individual will become a victim of identity fraud. The accuracy of this perception is looked at in more detail on pages 16 and 17.

### Gaps in the fraudsters' knowledge

The proliferation of information on the internet (from legitimate sites, to social networking, through to the criminal marketplaces of the Dark Web), is a fantastic enabler for the skilled fraudster attempting to commit fraud. Sources of information are not always going to be complete, however, and many will only contain partial information. These 'gaps' can help to identify attempted instances of Identity Fraud and ensure that they are not successful.

It is notable that in 2012, there were substantially more cases where the fraudster could not specify accurately the correct amount of time that their victim had lived at their current address (up to almost one in five Identity Frauds in 2012, compared with less than one in ten in 2011). There was also a proportionate increase in false birth dates being given (up to 12% of cases from 9% the previous year). This points towards these frauds largely being perpetrated by those who had acquired incomplete sets of data – forcing them to invent responses for those questions for which they didn't have the correct information. These frauds predominantly took place against products where less information was required during the application process – most commonly mail order. This points towards fraudsters with higher quality datasets choosing to target products with greater potential reward. For instance, very few Identity Frauds for credit cards involved the fraudster getting the time at address or birth date wrong. So, while this does not help us to identify the fraudster, it points towards a methodology.

One of the new types of lending product identified earlier involves the applicant for a loan requiring a third party to guarantee the loan. In the Identity Fraud cases that affected this type of product, it was the guarantor who was being impersonated, not the individual named as the recipient of the loan. The applicant may have had every intention of paying the loan back, but either their choice of guarantor had refused, or the applicant had simply decided not to ask them, but put their name down anyway. Either way, (in almost 1,000 cases) the lender identified that the person who would be responsible in the event of non-repayment had not agreed to take on that role.

#### **Where the person on the form simply did not exist**

There was an overall reduction during 2012 in the number of entirely fictitious identities used to attempt to commit fraud. In 2011, just over 10% of Identity Frauds involved a false identity but, in 2012, this figure decreased to a little over 7%, representing a fall in both the proportion and the actual volume of these frauds. The use of a false identity could indicate that the perpetrator was either very organised (and had meticulously built up a believable electronic history that would stand up to scrutiny), or that he or she was not and had not, and was quite probably a comparative novice. In the latter case, such attempts would fail at the first hurdle.

The building of an entirely fictitious identity is a complex process that might involve the fraudster fraudulently obtaining genuine passports and driving licences. If a fraudster has gone to such lengths, then it becomes

incredibly difficult for an organisation to identify this – even if they are using detection equipment like sophisticated document scanners (as the documents themselves are real, just issued to an individual who doesn't technically exist). However, where this amount of effort and attention to detail is applied to creating a false identity, the purpose behind doing so may not be purely to commit financial crime. Historically, it has been associated with attempts to facilitate, or potentially hide from a past of, other criminal activity.

As a side effect of such individuals starting a new life in a new name, they are going to need certain services to live that new life – and the first of these is going to be a bank account. Bank accounts were one of the few products where applications in entirely fictitious identities increased in 2012. While the overall number of Identity Frauds for bank accounts decreased in 2012 compared with 2011, the volume of Identity Frauds involving a false identity increased. In fact, of all Identity Frauds against bank accounts, almost 30% involved a false identity.

Evidence historically has pointed towards two other main drivers for obtaining a bank account in a false identity. The first is to use that account to facilitate the laundering of funds without it being able to be traced back to any identifiable individual. The second is the 'take that first step to creating a new life in a new name' motivation. This may particularly be the case for those who are new to the UK – especially as this presents a valid reason for having no pre-existing UK financial footprint.

Over the course of 2012, the UK Border Agency has made an extremely valuable contribution to ensuring that the UK is a more hostile place for fraudsters. By sharing the details of those that have no right to remain in the UK on the National Fraud Database, they have helped many other organisations in both the private and public sectors to identify frauds to an estimated value of almost > £12 million. In return, CIFAS Member organisations are able to feed back to UKBA any intelligence they may have relating to the individuals concerned and ensure that those who have no right to be in this country do not have access to services to which they are not entitled.

This mutually beneficial commitment to preventing fraud recognises the importance of collaboration across sectors and industries and marks a key step forward in ensuring a unified approach to tackling all types of fraud across the UK.●

## 3.2 The Geography of Identity Fraud

In order to perpetrate current address fraud, the fraudster needs to access any mail and intercept it physically. For this reason, there has been a long-held belief that those who live in communal buildings (e.g. blocks of flats, converted houses) are more likely to be targeted by identity fraudsters.

As part of a larger piece of work investigating the geography of fraud, Ordnance Survey (in conjunction with CIFAS) has undertaken an investigation into this perception in order to shed light on whether or not someone is more likely to be a Victim of Impersonation because of the type of building in which they live.

### Methodology

CIFAS supplied Ordnance Survey with over 460,000 anonymised records of fraud which were geo-coded (geographically referenced to co-ordinates) and mapped using a Geographical Information System (GIS). Of the 380 Local Authorities responsible for recording building types, however, only one-fifth (76) had undertaken the detailed recording of residential building type for at least 95% of their housing stock. Nevertheless, this still enabled a variety of geographic areas to be analysed (from London Boroughs to sparsely populated rural counties) allowing a variety of communities to be compared. Ordnance Survey is now undertaking an update of property types which should enable access to more complete data in the near future.

Four types of housing (detached, semi-detached, terraced and flats) were analysed in the 76 local authority areas to determine the type of fraud recorded against building type.

### Findings

On average, 0.3% of residential properties involve Victims of Impersonation in Great Britain. This figure is mirrored in the 76 local authority areas examined. *Figure 3.2.1* shows the overall distribution of the residence of Victims of Impersonation, compared with the type of residence in the 76 local authority areas covered.

This also shows that, overall, those living in detached houses were Victims of Impersonation more frequently than would be expected, considering the proportion of residential properties which are detached. Additionally, this shows that flats were under-represented as residences of the Victims

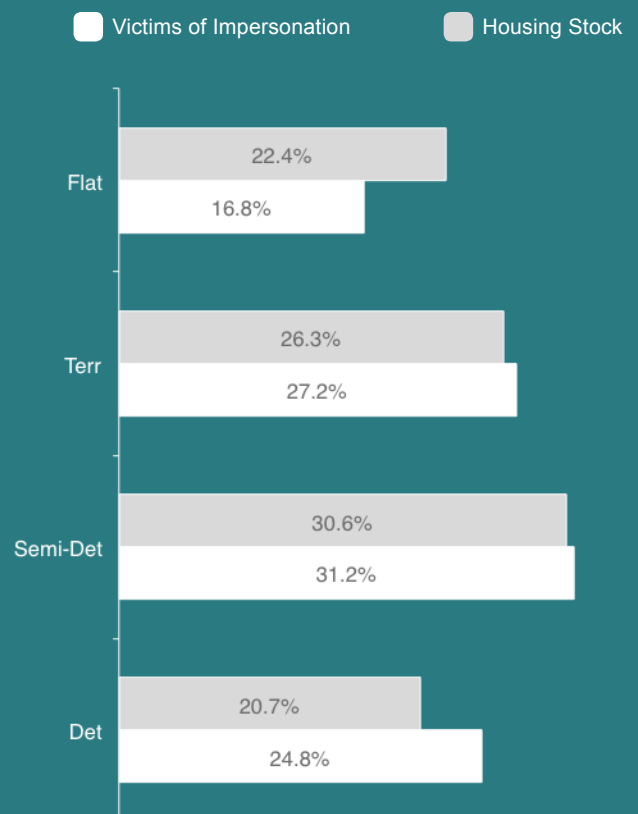
of Impersonation (that is to say, fewer victims lived in flats given the number of properties classified as flats).

This, though, was not uniform across all local authorities considered. Examples included:

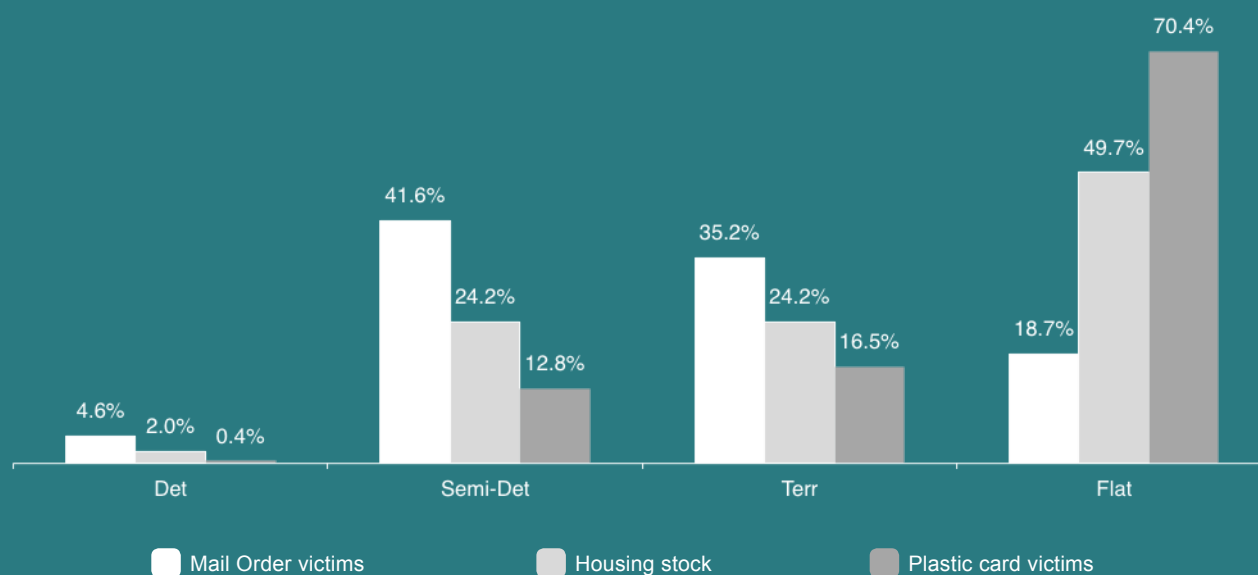
- Kensington and Chelsea, where despite flats making up over 80% of the housing stock, 60% of Victims of Impersonation lived in terraced houses.
- Windsor and Maidenhead, and Solihull, where over 50% of victims lived in detached houses, while the majority of housing stock was semi-detached.

There were also variations across the type of product applied for in the fraud. Frauds targeting mail order accounts had an over-representation of detached housing and an under-representation of flats, for instance. In 21 of the areas examined, detached housing was over-represented by more than 20%, with flats under-

Distribution of Victims of Impersonation by residence  
*Figure 3.2.1*



Distribution of Victims of Identity Fraud in Greenwich by residence  
Figure 3.2.2



represented by over 20% in 13 areas. In total, flats were under-represented in Identity Fraud against mail order accounts in 71 areas. It should be noted that a common *modus operandi* for Identity Fraud against mail order products involves having the goods delivered to a separate delivery address.

Where the product involved was a plastic card, however, the findings were somewhat different. In these cases, flats and semi-detached housing were slightly over-represented: with 10 areas having flats over-represented by more than 20%, and semi-detached over-represented by more than 20% in six areas. Overall, though, there was a greater balance in the proportionality across types of residence.

Within some specific areas, there was an interesting dichotomy. In Greenwich, for example, just under 50% of residences were flats, but only 18.7% of Victims of Impersonation for mail order accounts lived in a flat. That said, over 70% of Victims of Impersonation for plastic cards lived in flats: giving two very different profiles (see Figure 3.2.2).

### Conclusion

Although, at present, this work only covered about one in five local authorities, it does appear to debunk the myth that living in a flat makes you more of a target for identity fraudsters. It would be safe to assume that the property in which the victim resides says something to the fraudsters

about that person's potential for impersonation; but the nature of the property will not be the determining factor.

There were variations according to the local authority areas and products targeted. While, overall, residents of flats were under-represented in the total number of victims, this hid the fact that in some areas, for Victims of Impersonation on plastic card accounts (something requiring physical interception of post) residents of flats were slightly over-represented. The fact that this was not the case everywhere, though, indicates that it was not just living in a flat that makes someone more susceptible to being a Victim of Impersonation for cards, but also where that flat was located. A block of flats that falls within the 'awareness space'\* of an identity fraudster specialising in this type of fraud, therefore, was likely to be a target.

So, while this work might suggest that those living in flats are less likely to be targeted, it would be a mistake to oversimplify the issue. Victims of Impersonation, themselves, are only likely to find out that they have been impersonated after the fact – so it is always important to take care of personal information and postal security. In terms of debunking old myths, however, it is safe to say that the property you live in will not make you more vulnerable to fraud in isolation. Other factors will be as important, if not more so.

Watch out for more in-depth findings from this collaborative research – to be released in June 2013. ●

\* Brantingham and Brantingham's Crime Pattern Theory (1992)

## ENTERPRISE RISK, FRAUD AND COMPLIANCE SOLUTIONS

- Prevent fraud in real-time
- Reduce false positives
- Accelerate investigations
- Support regulatory compliance

Also available as Detica NetReveal® OnDemand

Find out more at [www.deticanetreveal.com](http://www.deticanetreveal.com)

## 3.3 Facility Takeover Fraud

Facility Takeover Fraud, also known as Account Takeover Fraud, occurs where a person (the facility hijacker) unlawfully obtains access to the details of the 'Victim of Takeover', namely an existing account holder or policy holder, and fraudulently operates the account or policy for his or her own (or someone else's) benefit.

### Facility Takeover cases by product 2011-2012

Table 3.3.1

Product	2011	2012	% change
All-in-one	209	583	+178.9%
Bank Account	2,814	4,166	+48.0%
Communications	6,136	6,758	+10.1%
Plastic Card	9,719	13,997	+44.0%
Loan	8	5	-37.5%
Mail Order	5,939	12,889	+117.0%
Mortgage	4	2	-50.0%
Other	241	28	-88.4%
<b>Total</b>	<b>25,070</b>	<b>38,428</b>	<b>+53.3%</b>

#### The data thief: an explanation?

The takeover of an account, while still reliant upon the identity details of a victim, is a different beast from Identity Fraud – due, mainly, to the fact that the account is already in existence and so no 'impersonation' is required. Whereas Identity Fraud requires the fraudster to attempt to impersonate their victim, Facility Takeover Fraud is more akin to stealing someone's keys in order to enter their house. The 53.3% increase, therefore, poses an obvious question: where are fraudsters obtaining the information needed to attempt to take over these accounts? Numerous possibilities are explained in this section, though one possibility must not be overlooked: staff collusion. Members of the CIFAS Staff Fraud Database reported a 20% increase in the theft or disclosure of customer data during 2012\*. Obviously, with an increase in theft or disclosure of data, it is equally unsurprising to see a link in the attempts to take over customer accounts. Whether these two types of fraud are linked – or whether other steps in a criminal chain take place first – is a subject for further study.

#### Some things are better to take over than others

Some types of product naturally experience very low levels of Facility Takeover Fraud, as the fraudster would gain little by having access to that particular account. For instance, there is little advantage to taking over a loan account, as the victim of the takeover already has possession of the funds. It's possible that a fraudster playing the 'long game' *might* try to access such an account in order to gain further information about his or her victim, or to help facilitate other frauds, but there would be little or no direct benefit to be gained by doing so.

For other products, though, there is much to gain. By volume of cases, mail order saw the highest increase in Facility Takeover Fraud (117%). Normally in these cases, the fraudster was looking for goods for their personal use, or to sell on later. Evidence has also pointed towards cases where the fraudster has taken over an account and, instead of taking receipt of the goods (with the accompanying job of trying to sell them on later), they chose not to take delivery of the goods, and then tried to have the value of the goods refunded to a card account that they already controlled. Fraudsters typically look to piggy-back on their victim's existing good relationship with the mail order company in order to reduce the likelihood of the order being identified as potentially fraudulent, and to ensure that the victim is left with the bill.

Plastic cards retained the title of 'most hijacked product', however, increasing by a substantial 44% in 2012 to almost 14,000 instances. While the most common action carried out by the fraudster, once they had hijacked an account, continued to be the issuing of unauthorised payment instructions (e.g. balance transfers), there was a proportionate decrease in the number of such instances: down to 57% of cases from 69% in 2011 (although the absolute number of these cases has increased by 1,000).

The notable increase was in cases where the hijacker attempted to change the address on the account, most likely as a precursor to getting replacement cards >

\* [www.cifas.org.uk/stafffraud\\_annual\\_janhtirteen](http://www.cifas.org.uk/stafffraud_annual_janhtirteen)

delivered. This fraud increased from 23% of plastic card takeovers in 2011, to 36% of cases in 2012. This was a reversal of the trend seen in the previous couple of years where address changes had proportionately decreased as the number of fraudulent transfers increased. This apparent return to the more 'traditional' type of plastic card takeover may suggest that fraudsters value having possession of a physical card. This can be used to take money out of ATMs (if only for a short period of time until the takeover is noticed) as opposed to carrying out transfers (which may be more likely to be flagged by transaction monitoring software and leave a more traceable footprint). Equally, during a year where many plastic card providers stepped up and refreshed their security procedures, this demonstrates that fraudsters have reacted by returning to the more 'old fashioned' preference for a physical card. Only time will tell whether this remains a 'trend'.

#### No news is good news

What was pleasing during 2012 was the increase in the number of attempted takeovers of bank accounts where we have no idea what the fraudsters' intentions were!

This might be seen as a somewhat puzzling statement, but our lack of knowledge here can be considered a good thing because these were cases where the fraudsters' attempts to gain access to the accounts were blocked. This meant that the organisations who hold the accounts are still none-the-wiser about what the fraudster would have done with the accounts if they had been able to access them.

That in itself can be considered a sign of the success of the ever-increasing security measures that banks have put in place to protect their customers' accounts. It is no longer typical for the security question simply to be "what was your mother's maiden name?" or for passwords to be simple. Frequently, the set up on an account now requires more than just one password, and passwords need to be 'complex' (a mix of upper and lower case letters, numerals and symbols) and security questions will be numerous. Furthermore, security (while never the primary selling point) has become an increasingly prominent factor for a potential customer. Therefore, this lack of knowledge of who the fraudster was and what they intended to do can be seen as a positive as the security measures blocked the fraudster at the first opportunity. Conversely, however, some fraudsters were attempting to gain access to accounts by using data which was not up to the task, resulting in 'a swing and a miss' for the fraudster.

#### The incomplete picture

The number of attempts that resulted in a complete failure to take over an account will have been under-reported. This is due largely to the nature of the compromised data. The data that the fraudster had was accurate, but the fraudster was directing it at the wrong institution. A fraudster with personal details can attempt to use them to commit identity fraud and take out accounts and services across many products, and across many providers of those products (although their chances of success will vary depending in the quality of data and the product applied for). A fraudster that has a login name and password, however, can only use that login name and password against the organisations with whom the account is held. While a certain amount of data is obtained through hacking of databases, not all will be, and the trading of compromised data online (through criminal forums or the Dark Web) does not necessarily mean that the fraudster who ends up attempting to use the data will have all of the details that they need to identify the organisation whose account it is. If the fraudster tried to use the details with a different institution, then that institution would not know whose account the fraudster was trying to access, and would (therefore) be unable to record the attempted fraud. In the case of phishing email attacks, while it is common for such emails to purport to come from a specific bank (thus ensuring that the fraudsters know who anyone who responds banks with), if the data is acquired through different means, or through a different phishing method, then this key piece of information may be absent – leading fraudsters to try what they have against a number of different institutions until they get lucky.

#### The differences between bank accounts and plastic card account takeovers

Even with this 'pleasing' increase in the *failure* of account takeover attempts against bank accounts, there was also an increase in the number of instances where access was achieved. In such cases, the fraudster attempted to carry out unauthorised electronic payments – essentially trying to steal the victim's money. Counterbalancing this was a decrease in the proportion of cases where the fraudster attempted to change the address on the account.

As with the takeover of plastic card accounts, this can be considered a precursor to taking receipt of new cards. But the factor that may help to explain why this method saw an increasing prominence in the takeover of plastic card accounts (but decreased in bank account takeovers) is time. For many consumers, it is frequently true that a credit card is used much less frequently than a debit card. Some

people will only use a credit card for 'special purchases' or online transactions, while the debit card may be used daily (especially with the decrease in cash transactions and the increase in usage of such things as contactless payments). This means that a fraudster cancelling debit cards and getting new ones sent to a different address has a very limited window of opportunity to attempt to make use of the cards, as the victim of the takeover is more likely to notice any issues quickly. With reduced use of credit cards\* (and the fact that these accounts tend to be reviewed by account holders on a monthly basis), this means that fraudsters would have days, if not weeks, to make the most of the credit cards before the takeover is detected and shut down.

### The appeal of the mobile device

Something that should now be viewed in conjunction with the increase in attempts to make unauthorised transfers from bank accounts is the increase in the number of takeovers of communications accounts (mostly mobile phone accounts) – up 10% from 2011. Being able to intercept communications from a bank helps to facilitate the takeover of a bank account; and taking over a mobile phone account is one way for a fraudster to do this. A pleasing development is the increase in communication and collaboration between the providers of mobile phones and the banks to ensure that this method of fraud to facilitate fraud is made as unprofitable as possible for fraudsters.

Previously (see page 11), this report identified a decrease in the number of Identity Frauds against mobile phones, citing increased security around account opening as a reason. This has not made the handsets any less desirable, however, so this resulted in an increase in 2012 in the number of attempts to take over existing accounts to qualify for upgrades. As previously stated, one of the factors that makes Facility Takeover Fraud more problematic for fraudsters than Identity Fraud, is that the fraudster has to be much more targeted in his or her attempt. The fraudster has to target the organisation holding the account and – should they not know this – then the attempt is likely to fail. The increase in takeover of mobile phone accounts did not completely counterbalance the decrease in impersonations for new accounts. The fraudster has to be much more focussed in their attempts as they need to target the right mobile phone provider, thus making a scattergun, high volume approach unviable. ●

## Case Study Fraud to Perpetuate Fraud

Avon and Somerset Police received reports of a trend, identified by one of the large banks, in the use of stolen and counterfeit cheques where there was distinctive handwriting common to many of them.

This was later identified as a Zimbabwean national living in the Grays area of Essex. He was arrested and his computer equipment revealed numerous templates for the creation of counterfeit bank cheques. Examination of his mobile phones also indicated that he was in contact with several people who were supplying him with confidential bank account information (such as account balances, direct debits, ATM withdrawals, etc).

This led to further arrests of numerous people including staff at two large banks – who were sending copies of cheques and bank details received in their department thus facilitating the creation of counterfeits – along with a third accomplice involved in the use of counterfeit cheques.

The cheques directly connected to them (through handwriting) indicated a conspiracy that succeeded in obtaining, or attempting to obtain, over £150,000. Further examination of the counterfeit cheques being used and the accounts receiving payments revealed that the figure could actually have been in excess of £270,000.

Three of the accused were charged with conspiracy to defraud and pleaded guilty to this, with sentencing occurring at Bristol Crown Court in November 2012. The fourth skipped bail and is still wanted.

As an addendum, two further parties were charged as the result of investigations during this case: one admitted to the use of a number of counterfeit and stolen cheques and the possession of numerous stolen bank cards; with a further party charged with attempting to pay fraudulent cheques into accounts. The former received a suspended sentence while the latter was found not guilty.

\* [www.bba.org.uk/media/article/december-2012-figures-for-the-main-high-street-banks/press-releases/](http://www.bba.org.uk/media/article/december-2012-figures-for-the-main-high-street-banks/press-releases/)

### 3.4 Who was targeted?

In the majority of cases, the Victims of Impersonation were male, although the proportion of female victims crept up over the previous year, reversing the decrease seen in 2011 compared with 2010.

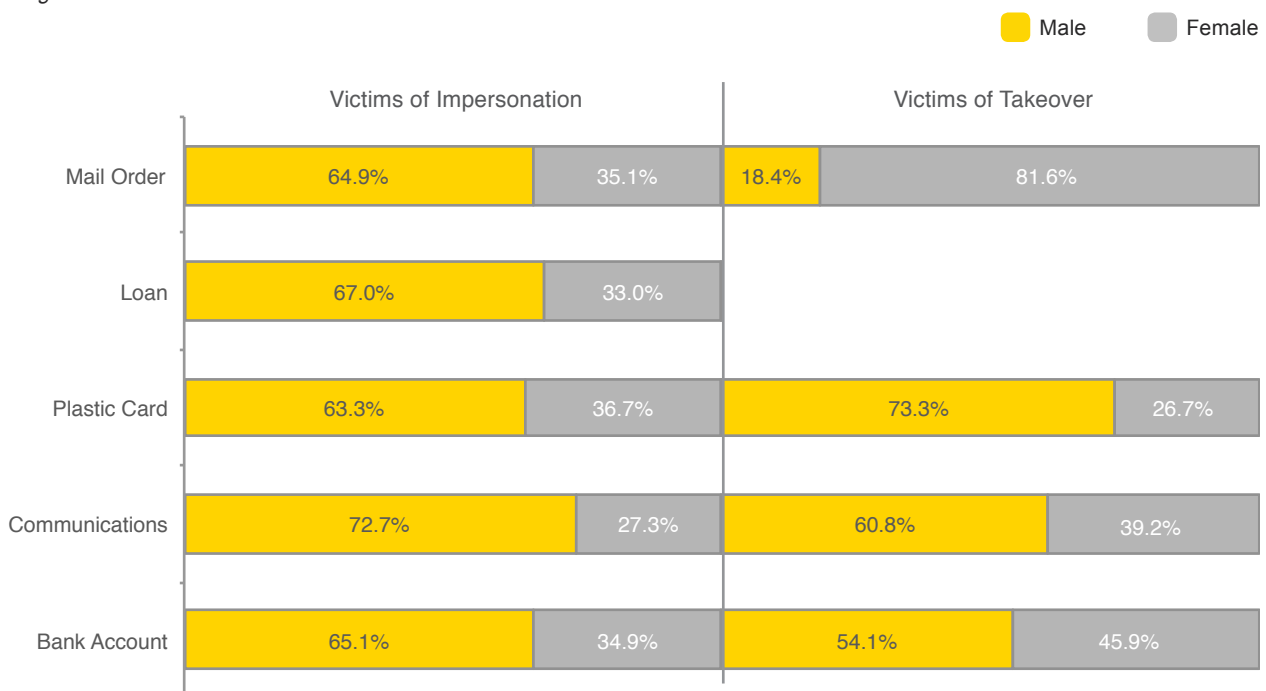
Figure 3.4.1 shows the gender distribution of the Victims of Impersonation for the five most commonly affected products. This reveals that the product which saw the highest proportion of male victims was, as in 2011, communications: predominantly mobile phones. Plastic cards saw the highest proportion of women being impersonated, accounting for almost 37% of victims. Loans saw the highest increase in the proportion of victims that were women, increasing 7% from 26% of victims in 2011 to 33% in 2012.

Figure 3.4.1 also gives this same information for Victims of Takeover (omitting loans, as they were not substantially targeted for this type of fraud).

What is apparent when comparing the two sides of this chart, is that there are some large discrepancies by gender of those who were Victims of Impersonation, and those who were Victims of Takeover, for the same product. This is most clearly seen in mail order, where men accounted for 65% of the Victims of Impersonation, but represented less than 20% of the Victims of Takeover. There is a very obvious explanation for this, which is closely connected to the point made earlier about the necessity to know where an account is held before it can be taken over. Before an account can be taken over, it has to exist. If the majority of account holders are women, then it follows that the majority of Victims of Takeover would be women too. This is not a consideration when it comes to impersonation for a new account, where the gender distribution is more a factor of the nature of the available data, and the preference of the fraudster.

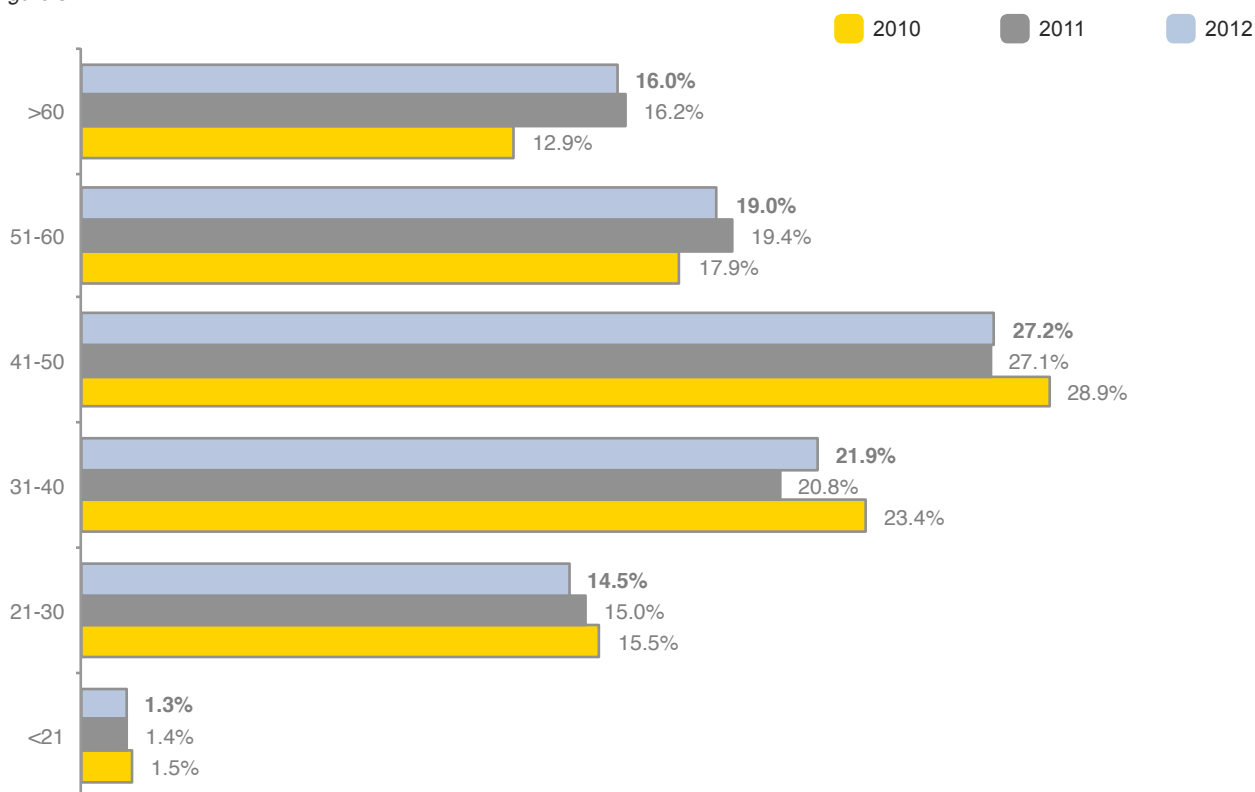
Gender distribution of Victims of Impersonation and Victims of Takeover by product in 2012

Figure 3.4.1



### Age Distribution of Victims of Takeover 2010-2012

Figure 3.4.2



#### Age and product

Last year’s edition of *Fraudscape* identified that, in 2011, there was an increase in the proportion of Victims of Takeover who were towards the higher end of the age spectrum. This posed the question as to whether this was a one-off occurrence or the start of a trend. As *Figure 3.4.2* shows, 2012 has seen an age profile very similar to 2011.

2012 did not see a further bias towards the more mature Victims of Takeover – in fact there was a slight decrease in the proportion of victims who were 51 or over – but the pattern of the previous year does not appear to have been a ‘one-off’. The minimal change that occurred, though, can be accounted for by the change in the distribution of products where an account was taken over. Plastic cards were the most commonly taken over accounts and, as mentioned earlier, the number of cases identified increased by around 4,000 cases. The number of mail order takeovers, however, increased by around 7,000 and the gender and age distributions for those two products were very different.

Male victims of plastic card takeovers tended to be substantially older than their female counterparts and

accounted for almost 75% of victims. For mail order accounts, the average age was lower, but there was little difference in the distribution of male and female victims – even though there were many more female victims than male. It is therefore the numerically greater increase in mail order frauds, with its lower age profile, that ensured that the *status quo* of the age profile of all victims of takeover was maintained.

#### The bad news for men

Looking back at *Figure 3.4.1*, it is noticeable that plastic cards had the lowest percentage of male Victims of Impersonation recorded in 2012, but also had the highest proportion of male Victims of Takeover. Taking into account both this, and the age distribution, what these findings say is that there is a real possibility that fraudsters targeted older men when looking to take over plastic card accounts. Some filtering of bulk record sets that the fraudsters had acquired would, doubtless, have played a part in this, and the idea of ‘spear-phishing’ (where fraudsters specifically target a set demographic) is one that also cannot be discounted. Most worryingly, there is potential for the frauds to have been enabled through insider collusion. This would involve a member of staff within the card company, >

who was identifying specific types of account or victims, before feeding this information to the fraudsters. It is probable that this demographic was being targeted because they were likely to have developed a higher credit limit than younger victims, or that the fraudsters expected those who were older, particularly the over 60s category, to use their cards less frequently than younger people.

### Unnerving repercussions

When talking about the victims of fraud, the question of 'how did they get my details?' always arises. As mentioned previously, if an organisation is dealing with an application or transaction/request (ostensibly from a specific individual), and all the details pass verification, then it is easy to see why the fraud was successful. After all, if a genuine consumer was denied access to his or her account (having passed security) the repercussions are obvious.

The trouble is that the victims of fraud are not just left to deal with the short term damage to his or her financial wellbeing. The victim also has to demonstrate that he or she was a victim of fraud (as opposed to having acted negligently with their details) as well as being left wondering how their details were obtained. It is this uncertainty that is, perhaps, the most lasting consequence of being a victim of fraud. As with many other crimes, the victim is left wondering whether he or she will become a repeat victim.

### Impersonation Targets

*Figure 3.4.3* shows the age distribution of victims of impersonation over the last three years.

This suggests that there was generally little consistency in the minor changes in the proportion of Victims of Impersonation that fell into a given age category between one year and the next. The general pattern remained much the same, with the 41-50 age group the most commonly impersonated, accounting for just over a quarter of victims each year. This lack of any emerging pattern or substantial change would tend to imply that there was a state of 'business as usual' for the fraudster. There may be more and more data available to fraudsters in this data-driven age of impersonation, but the demographics of those to whom the data relates (or, potentially, those that the fraudster picks from the available data as a potential target for impersonation) remains largely unchanged. The same type of person is being impersonated – it's just that the number of such instances is increasing. So, for the fraudster, while more data means more targets, and more fraud has been recorded, these figures demonstrate

that it is still a certain type (male, probably middle-aged, professional and therefore more likely to be financially solvent) who are the most profitable targets for many identity criminals. Therefore, in a data-driven age, where victimisation is more indiscriminate, some individuals and groups are nevertheless likely to be in the fraudsters' sights. ●

## Case Study

### The communications provider scam

Of course it is not just the 'affluent' who will fall victim to identity fraudsters.

National Fraud Intelligence Bureau investigations turned up the case of an organised fraudster who set up a fake company supplying mobile phone contracts. By advertising in the classified sections of local papers and putting leaflets through people's doors in 'run down' areas, the fraudster would target people who found it difficult to obtain credit yet wanted to be able to have a mobile device such as a Blackberry or iPhone.

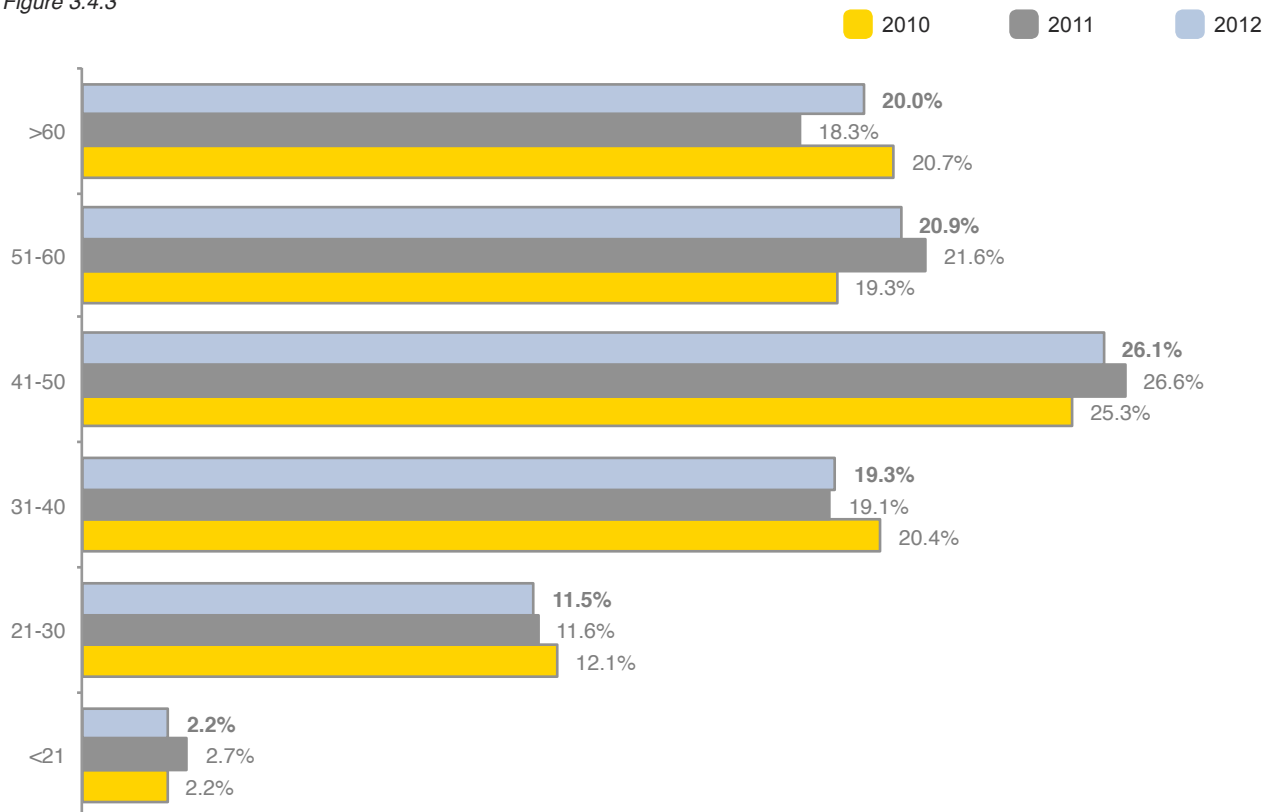
The fraudster would respond to interested parties by telling them that he had to visit their address to make sure that they lived where they said they did, and to take copies of their passports or other identity documents, utility bills and bank statements in order to 'support' the application. As the fraudster later admitted "They would give me anything if it meant they could get a new phone."

Using a laptop and portable scanner, the fraudster was able to capture everything needed. The fraudster also made use of a contact within one of the phone companies who made sure that all the applications were approved: leaving several happy 'customers' who had unwittingly provided the fraudster with all the details needed to open bank accounts in their names.

Making sure that a different address was used to receive correspondence, the fraudster admitted that these accounts were used to "hold my financial proceeds of other crimes. None in my name and none connected to me. Perfect."

## Age Distribution of Victims of Impersonation 2010-2012

Figure 3.4.3



The UK's Fraud Prevention Service

## Fighting Fraud Nationally: Emerging Fraud Threats

CIFAS Conference & Exhibition  
London, Tuesday 4 June 2013

With speakers from a variety of disciplines and backgrounds, this year's CIFAS Fraud Conference and Exhibition will focus on the latest information about emerging threats across the fraud prevention industry. The day will also be a great networking opportunity, giving you a chance to speak to CIFAS Members and staff, to meet representatives from numerous fraud prevention product providers and to catch up with your peers and colleagues from across the public and private sectors.

Visit [www.cifas.org.uk/events](http://www.cifas.org.uk/events) or contact [events@cifas.org.uk](mailto:events@cifas.org.uk) for a full programme and booking details.

## 3.5 The Location of Identity Crime

The following pages contain a range of UK maps which illustrate where the Victims of Impersonation and Facility/Account Takeover Fraud are located.

The first two maps (pages 28 and 29) have been population adjusted, with all boundaries and populations based upon local authority areas, and the shading corresponds to the **number of cases of victimisation per thousand people**. The darker the shade of red, the more victimisation occurred in that area.

### Location matters – in varying ways

*Map A* (page 28) shows the locations for Victims of Impersonation in 2012, with *Map B* (page 29) showing the location of Victims of Takeover.

What these maps comprehensively demonstrate is that, even when population is taken into account, the main fraud victimisation hotspots continue to be the larger areas of more dense, urban population. This is most obviously true in London, but can also be seen clearly in the Midlands and the North West. In addition, in the London areas, victimisation is high throughout. This is consistent with the patterns identified in previous years and demonstrates that little has changed.

In the previous edition of *Fraudscape*, however, some interesting differences were noted when comparing Victims of Impersonation with Victims of Takeover. Put simply, location seemed to matter more in cases of impersonation: with areas where there was a high proportion of Victims of Impersonation per thousand people being far more geographically concentrated into specific areas than the equivalents for Victims of Takeover. This pattern has been repeated, with a greater relative preponderance of Victims of Takeover occurring in areas as diverse as the Orkney Isles, Western Isles, South Lakeland, Melton, Stratford on Avon, Torrington, Mid Devon and South Hams. Considering the lower population levels in these areas, the surprise is that the preponderance of Victims of Takeover was much higher than other areas with similar population levels. Whether this points towards organised criminal activity is – of course – something to be investigated further.

Victims of Impersonation, on the other hand, were far more concentrated within the London and Home Counties regions; with a slightly raised level of occurrence along the M4 and M6/M62 corridors. Other areas with a high preponderance of Victims of Impersonation per thousand people (Bury, Blaby, Kettering, Northampton and Coventry) are closely situated to these corridors, unlike Victims of Takeover whose geographical spread was far wider. This reaffirms the idea that Victims of Impersonation were more likely to be targeted for who they were and where they were than Victims of Takeover. In an age where fraud is largely driven by data, the address of an individual still plays a hugely important role.

As previously explained, to impersonate an individual and open a new account in his/her name, the criminal will need to know his/her address: to take over an account, far less (but very specific) information is usually required. Consequently, for many criminals, the lack of an address in a set of compromised details does not pose a problem: the intended victim may live in the Orkney Isles, but if the data exists to attempt a hijack of an online bank account, then a fraudster based in South London will have no problem.

Furthermore, in densely populated urban areas there is – perhaps obviously – a greater anonymity. Would your local postman/woman notice if you suddenly stopped receiving post (e.g. through a mail redirection) in South London or would he or she be more likely to notice this in a closer-knit community? Put bluntly, the greater the local population, the greater the cloak of anonymity for the identity fraudster. Taking over an account is more likely to be perpetrated remotely – therefore it is distance, rather than headcount, that serves the fraudster. ●

The maps on pages 28-33 contain public sector information licensed under the Open Government Licence v1.0. Contain Ordnance Survey data © Crown copyright and database right 2013. Contain Royal Mail copyright and database right 2013. Source: Office for National Statistics

# We don't just see a landscape of different properties

We see data to validate addresses and reduce fraud

We capture up to 10,000 changes across Great Britain every day, including a property's type. Our database can help validate the existence of single or multiple occupancy properties, by checking that the address actually exists and by tracking the life cycle of an address from planning to demolition. This is especially useful when an individual property is converted into multiple addresses, alerting you to the potential for fraud or financial crime. By using Great Britain's most accurate and up-to-date geographic intelligence you can pinpoint and flag potentially fraudulent activity for further investigation.

[www.seethedetail.co.uk/cifas](http://www.seethedetail.co.uk/cifas)

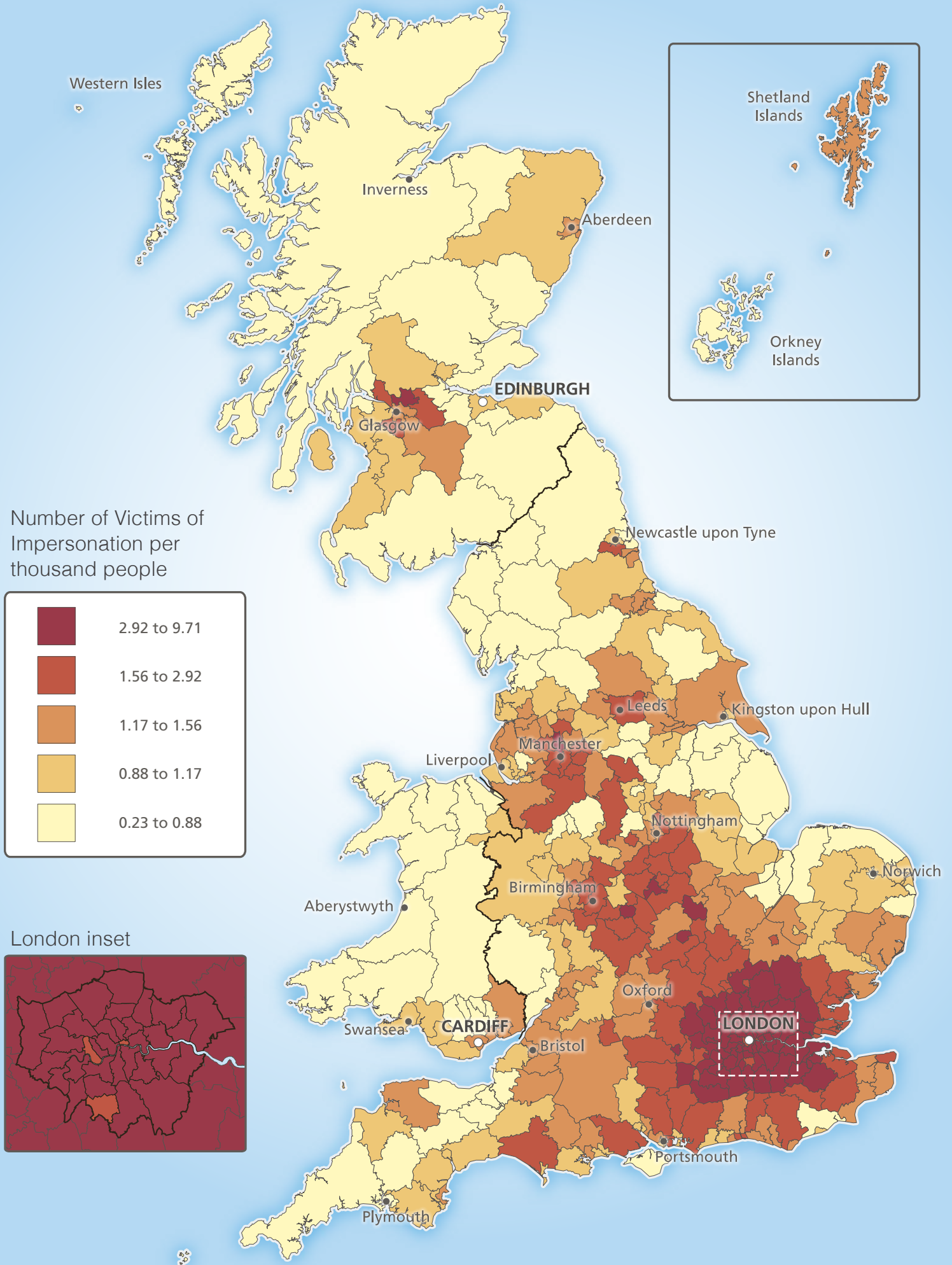


We see the detail  
So you see the bigger picture

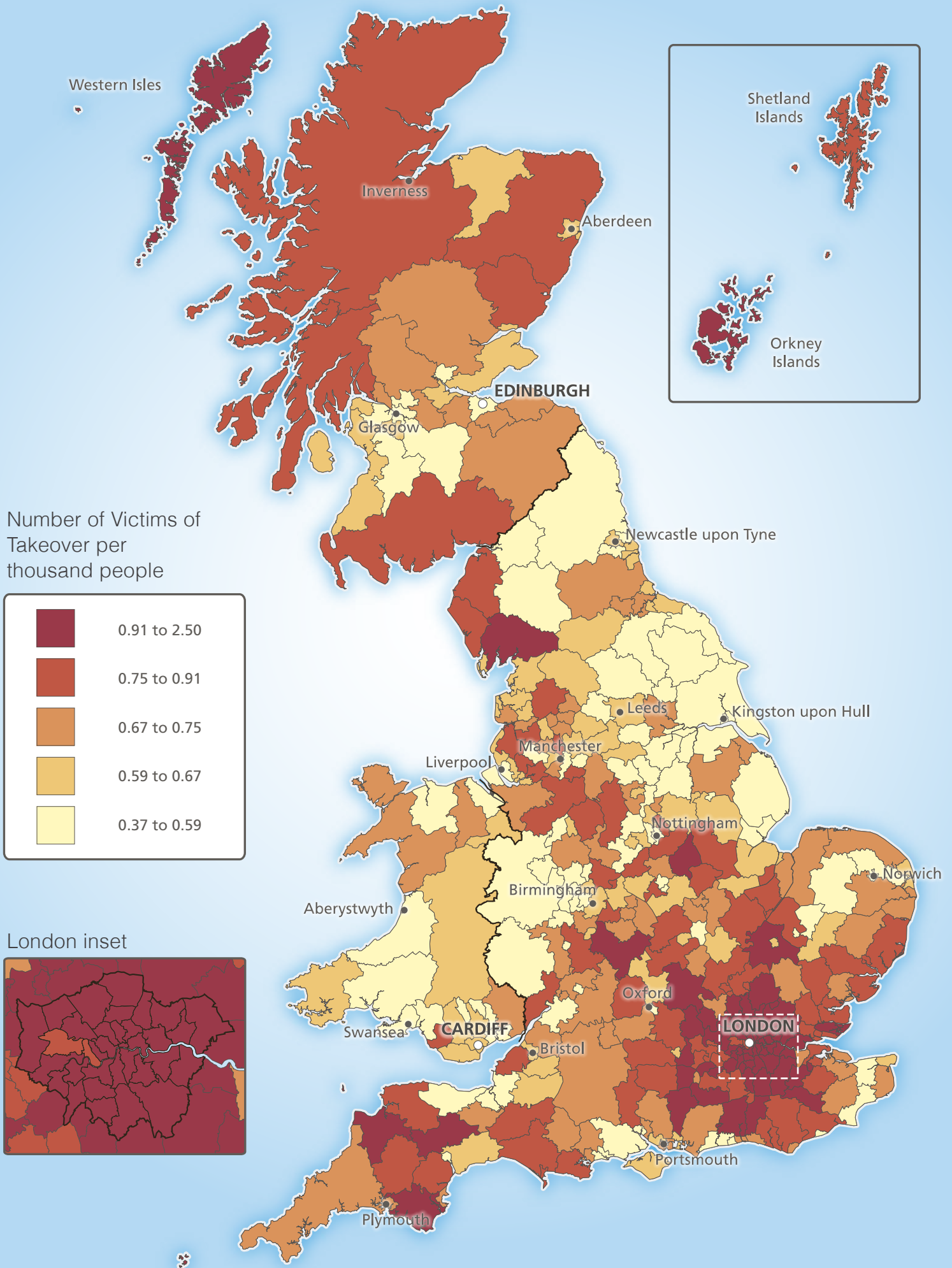


Ordnance  
Survey®

# Map A: Victims of Impersonation in 2012 per thousand people by local authority



# Map B: Victims of Takeover in 2012 per thousand people by local authority



## 4. The Fraud Landscape

Map C shows the total number of all frauds – including those classified as first party frauds (see section 6) – recorded in 2012, per thousand people by local authority area. As with previous years, the clearest finding was that the highest levels of fraud were concentrated in urban areas, most noticeably in and around London. Other ‘urban hotspots’ – where the number of frauds per thousand people was noticeably higher in one area than other geographically close areas – included the Greater Manchester region (comprising Bury, Salford, Oldham and Manchester), and the Wolverhampton/Sandwell/ Birmingham area.

So far, so unsurprising; but there were some other interesting regions. The Gosport and Portsmouth areas, two of the areas with the highest numbers of frauds per thousand people, both displayed similar characteristics; with high levels of Facility Takeover Fraud and frauds targeting mail order products. Similarly, in Middlesbrough (which had a slightly lower number of frauds per thousand people than either Gosport or Portsmouth) mail order accounts were most commonly targeted, though there was a greater relative preponderance of Identity Fraud here than Facility Takeover Fraud. Finally, in most of the fraud hotspots identified on the map, the internet was the channel of choice for the fraudster. Peterborough, however, had very similar levels of internet perpetrated fraud and frauds

attempted on a face-to-face basis. The particular reasons behind such concentration of activity, and the explanations for these types of fraud, product choices or channel are issues impossible to determine from a map alone. Within the sphere of Application Fraud for insurance products there was also a curious finding; namely an increased prevalence for this type of fraud in both Dover and the Malvern Hills areas. It is not immediately obvious why these two distinct and disparate areas should have been targeted in that way: was it the result of an organised multi-party operation, or simply numerous people each trying to manipulate premium prices?

The overall pattern in the rest of the UK, however, showed an overarching pattern of fraud being concentrated in the South East, Thames Valley/Home Counties, and around other areas with urban centres in the Midlands and Northern England. Perhaps most interesting was that, unlike previous years, the concentration of higher levels of fraud along the M4/M5 corridor was far less pronounced than previously seen.

The tables below – for additional interest – show the top ten postal districts for London and the top ten non-London postal districts for total number of frauds recorded in the UK during 2012.

Top Ten London Postal Districts for Fraud

Table 4.1.1

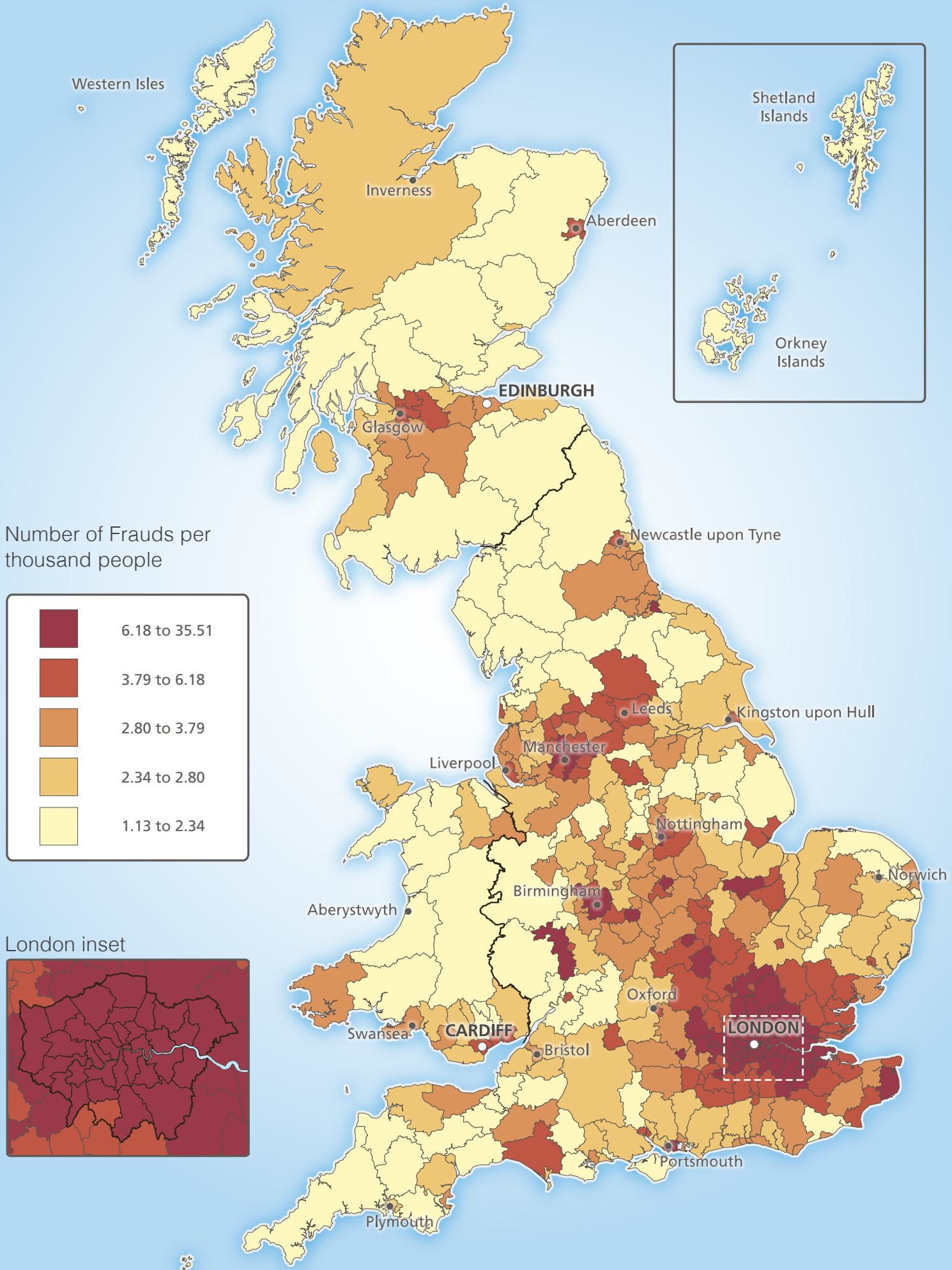
Postal District	Name	Number of times an address used in fraud
E6	East Ham	1,758
SE18	Woolwich	1,709
CR0	Croydon	1,660
SE15	Peckham	1,505
E17	Walthamstow	1,488
IG11	Barking	1,467
SE28	Thamesmead	1,387
NW10	Willesden	1,351
E7	Forest Gate	1,212
IG1	Ilford	1,173

Top Ten non-London Postal Districts for Fraud

Table 4.1.2

Postal District	Name	Number of times an address used in fraud
PE1	Peterborough	814
SL1	Slough	785
LE4	Leicester	760
LU1	Luton	735
M8	Manchester	719
LE3	Leicester	710
LE2	Leicester	649
CV6	Coventry	647
LE5	Leicester	568
NG7	Nottingham	563

# Map C: Total number of Frauds in 2012 per thousand people by local authority



**Regional Focus**

Maps D, E and F (while using different geographical scales) are constructed using the same scales for fraud density and clearly demonstrate the localised patterns in three of the UK's densest fraud hotspots.

In terms of the traditional centre for fraudulent activity, the map of the Greater London region demonstrates a consistency with previous analysis: with fraud clearly having been at its most concentrated in areas of high population.

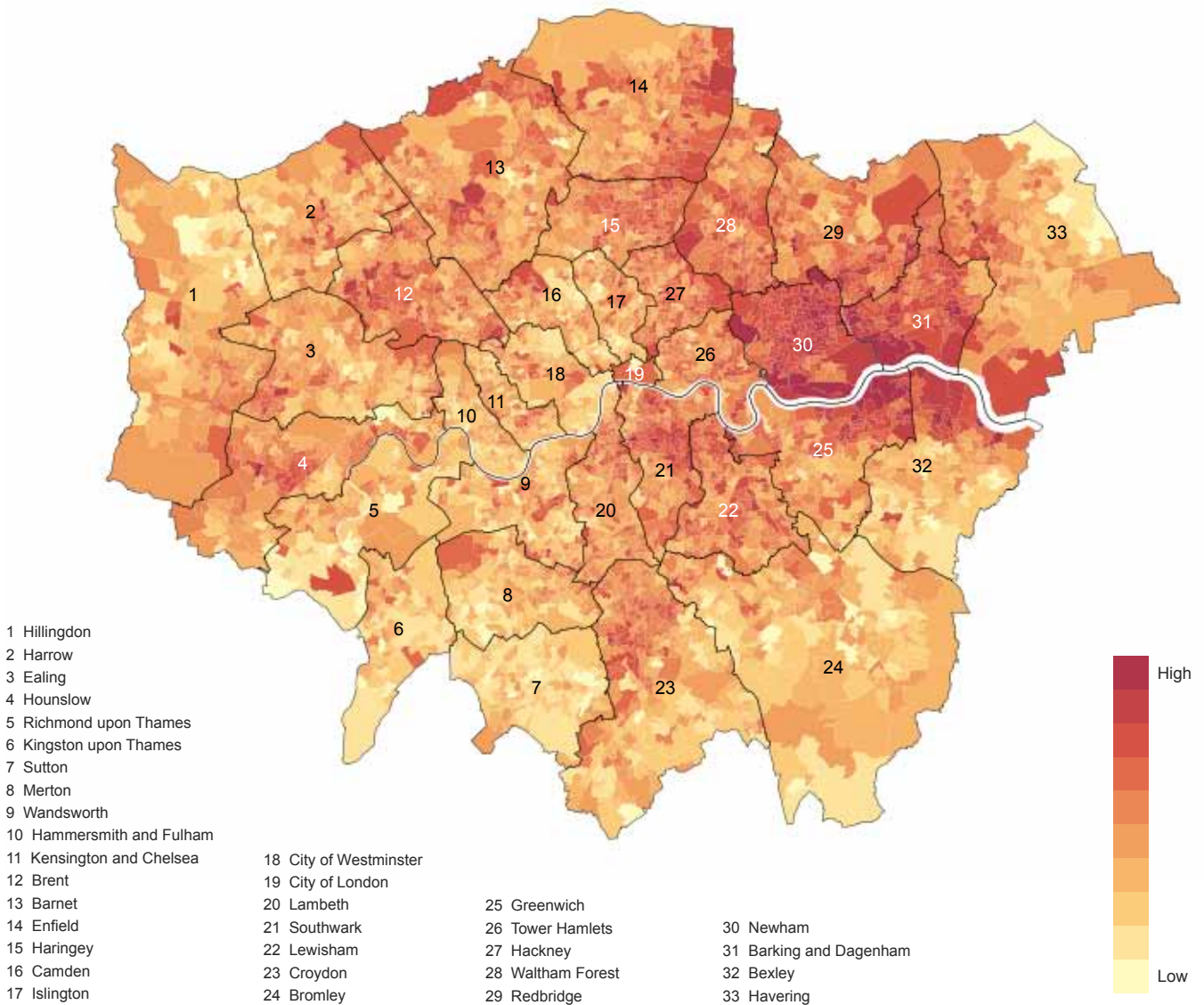
In Greater London (Map D), the East London Boroughs of Newham, Barking and Dagenham, Greenwich and Bexley remained the long standing 'fraud epicentres'. However,

other clusters of fraudulent activity were also seen in the outer regions of North London (especially in the Boroughs of Redbridge, Enfield and Waltham Forest).

Lesser populations will appear to give the Greater Manchester and West Midlands regions a lesser overall density of fraud, but this therefore shows up particular hotspots in Manchester, Bury and Salford (Map E) and Birmingham, Coventry and Wolverhampton (Map F).

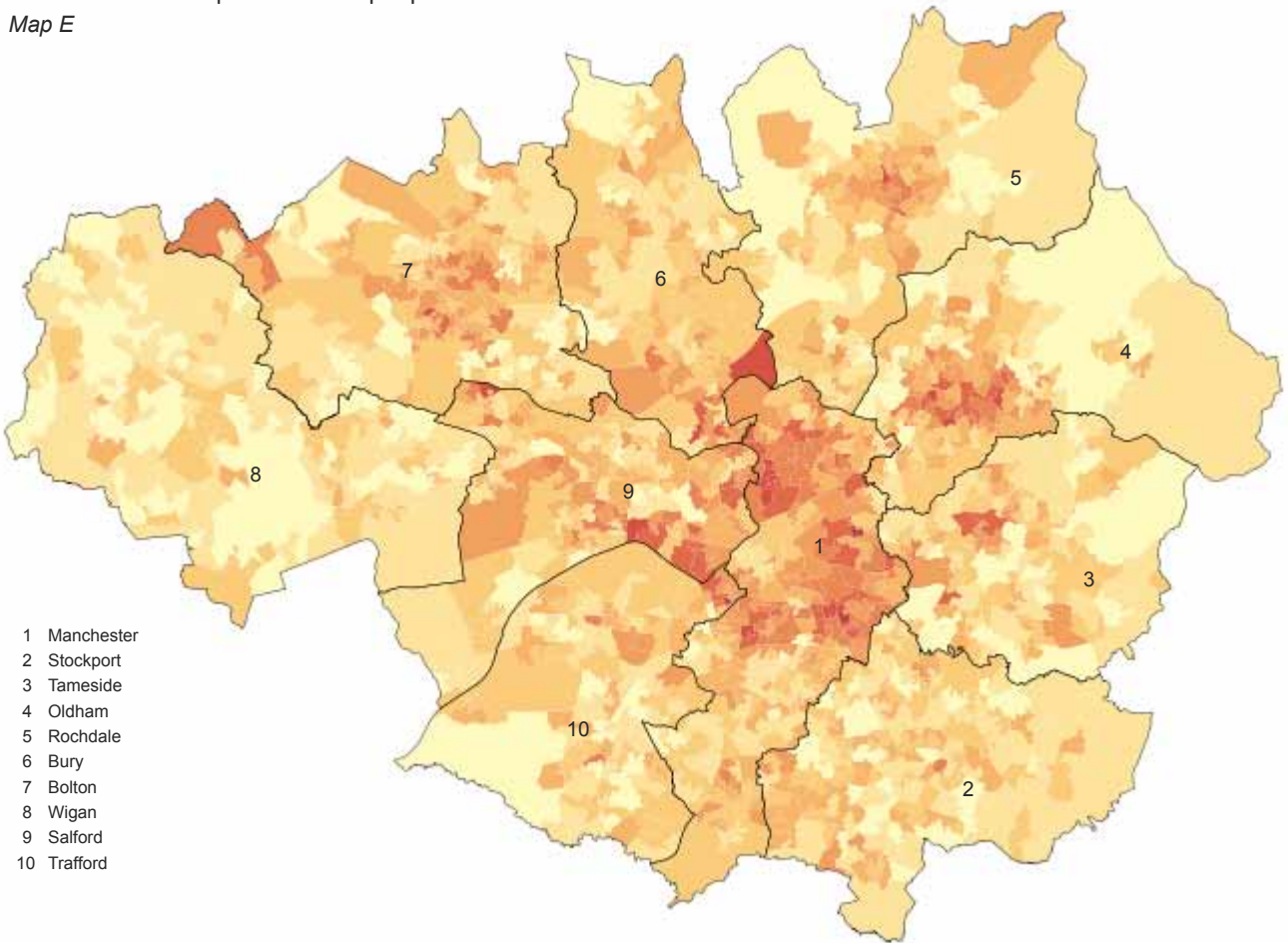
Analysis of this kind can play an instrumental role in the identification of criminal networks operating within specific areas and such analysis will feature further (for specific areas) in future collaborative work between CIFAS and Ordnance Survey. ●

Number of Frauds per thousand people in Greater London  
Map D



Number of Frauds per thousand people in Greater Manchester

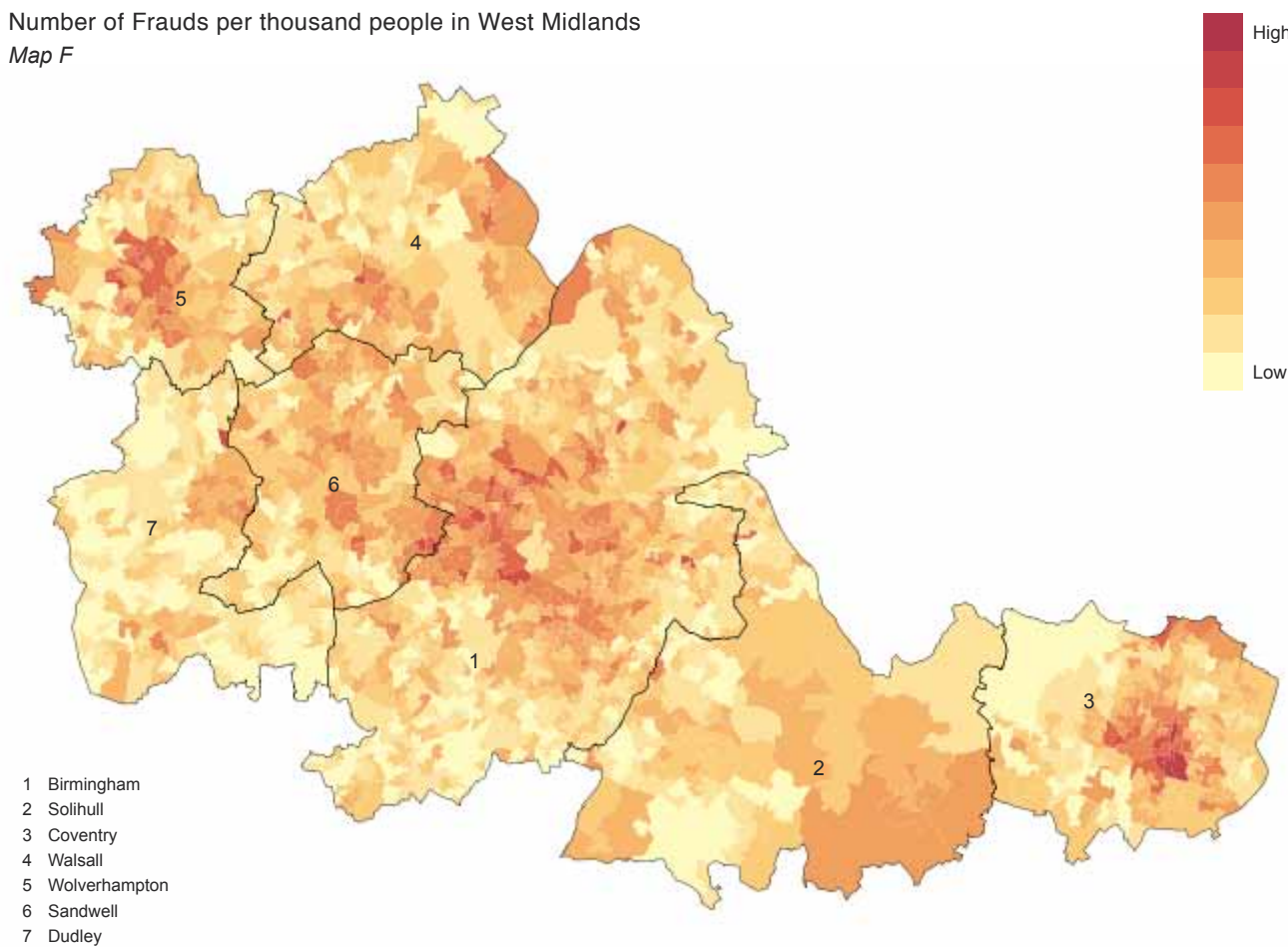
Map E



- 1 Manchester
- 2 Stockport
- 3 Tameside
- 4 Oldham
- 5 Rochdale
- 6 Bury
- 7 Bolton
- 8 Wigan
- 9 Salford
- 10 Trafford

Number of Frauds per thousand people in West Midlands

Map F



- 1 Birmingham
- 2 Solihull
- 3 Coventry
- 4 Walsall
- 5 Wolverhampton
- 6 Sandwell
- 7 Dudley

## 5. How Organised is Organised Crime?

For most people, the term ‘organised crime’ will conjure up images of the Corleones in *The Godfather* films, or the Krays in the East End of London. Rarely does it evoke the image of a spotty teenager in his bedroom. But developments in criminal techniques, and in criminal relationships, mean that the concept of what constitutes organised crime has been reassessed.

Definitions of ‘organised crime’ historically tended to place an emphasis on the established structure of the group or the number of people involved. More recently, there has been a move away from specifically defining the term, to giving some indication of the sort of criminal activity covered by it. The SOCA website, for example, states that serious organised crime “includes Class A drugs, people smuggling, human trafficking, major gun crime, fraud, computer crime and money laundering.” The Home Office paper *Local to Global: Reducing the Risk from Organised Crime* says that “Organised crime involves individuals, normally working with others, with the capacity and capability to commit serious crime on a continuing basis, which includes elements of planning, control and co-ordination, and benefits those involved.”

It is clear from this that there has been an acknowledgment from government and law enforcement that finding a precise definition is less important than actually getting a handle on the crimes.

From an organised fraud perspective, the perpetrators can be thought of as fitting somewhere on a continuous scale between what is, essentially, the traditional idea of organised crime, to an individual working alone, but in a methodical, industrialised manner.

**The organised crime gang:** this is the end of the spectrum that most fits with the traditional view of organised crime, involving structured groups (possibly based on familial, cultural or ethnic grounds) and which may well be involved in other forms of socially damaging criminality. An example would be crime groups originating from Eastern Europe, or Western Africa, some of which are known to traffic people in to the UK to use them for a variety of criminal activities. These include duping them into committing fraud and money laundering offences. It is thought that a lot

of the frauds that fit the profile of ‘money muling’ will be orchestrated by these organised criminal gangs (see page 36).

**The dynamic network - trusted community:** this describes a much looser network, based on a largely commercial interaction between the participants. Essentially, one member of the network will purchase expertise or a product from another member which will allow them, in turn, to perpetrate their own crime. Those involved in the network will change as the needs of the individual change. A prime example of this would be the identity fraudster purchasing personal information from another criminal in order to commit Identity Fraud *en masse*. These relationships largely happen online, through such things as the Dark/Deep Web (internet content not accessible by normal search engines), but also have an element of trust involved. A large proportion of the data-driven crimes discussed in this report originate from people forming part of one of these networks.

It must be acknowledged that these groups do not just exist in the virtual world. They also include real world transactions between a company insider compromising data and a fraudster, to cash-for-crash scams where groups of people are involved in staged accidents for the purpose of making fraudulent insurance claims.

**The lone wolf:** the fraudster who acts alone, but in a highly organised, methodical manner. It could be that this is an individual who has sufficient skills and experience without needing ‘buy-in’ from anyone else or, equally, to a staff insider who steals customer data for personal use. The more ‘traditional’ identity fraudster (who will target a victim such as a company director, develop that identity and then carry out multiple frauds in that name) might also fall into this category.

### Should the punishment fit the crime?

So, if the definition of organised crime can be seen as fluid, this then raises an intriguing question: if the damage is the same, should the categorisation of the perpetrator affect the attention that the perpetrator receives from law enforcement, or the punishment resulting from any prosecution? ●

## 6. First Party Fraud

‘First Party Fraud’ is a term used to categorise any fraud where there is no proof that an account has been subject to Identity Fraud or an attempted takeover by a third party – and, therefore, the fraud is being committed by the named account holder or applicant.

Although the motivation behind the vast majority of identity related crimes is simply to secure money, goods or services without paying, the motivations behind first party fraud can be far more complex. They range from coercion by organised criminals (in the case of some Misuse of Facility Frauds), to a sense of entitlement that the proceeds of the fraud are their due (in the case of some inflated insurance claims), and the belief that they are actually going to pay back what they owe (in the case of some Application Frauds). But let’s not forget simple greed, in cases where the applicant has not the slightest intention of repaying what he or she owes, or has become accustomed to a lifestyle that he/she does not wish to give up.

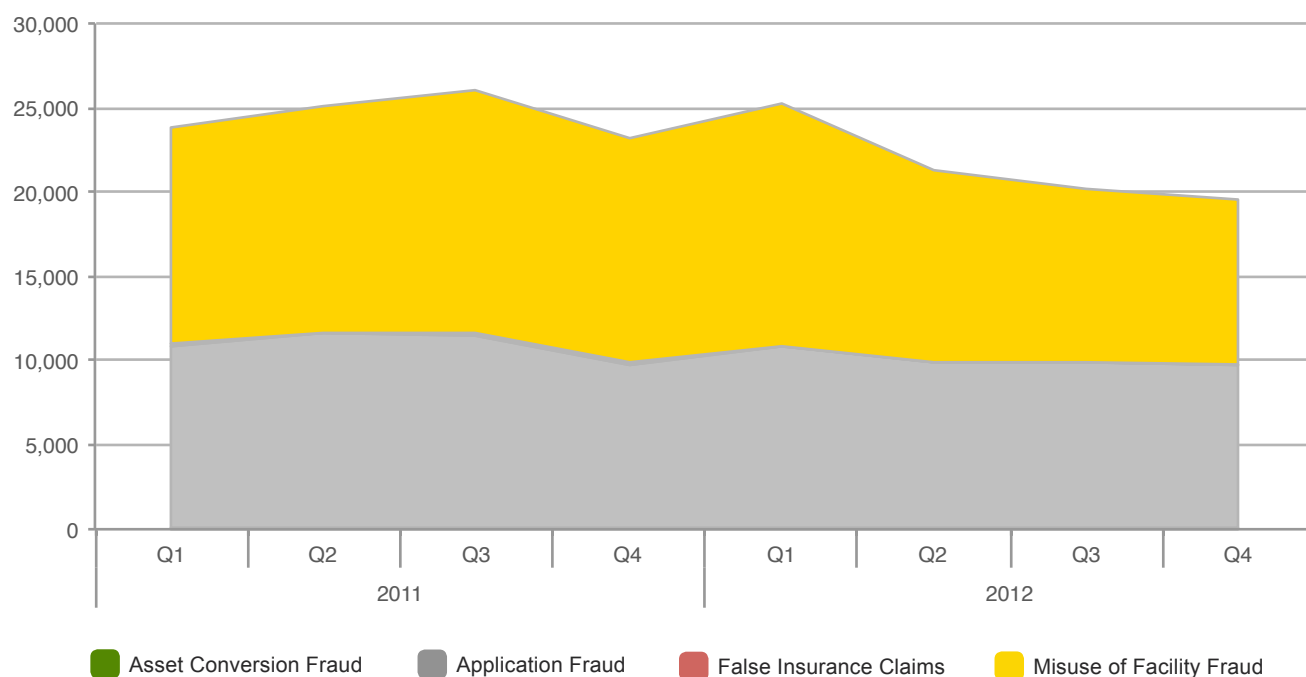
This is against a background of what is currently described as a potential (at the time of writing) triple dip recession. A range of economists give, at times, conflicting messages.

Unemployment is down, as are the levels of average household debt. On the other hand, the cost of living has increased and wages have not. Numerous high profile cases of companies entering administration, public sector job cuts and financial warnings from long established high street names create a confusing picture where the man in the street can be forgiven for wondering whether – since 2008 – the economic situation has got better or worse or not changed. This is an important consideration when examining first party frauds, where the nature of the frauds attempted are not necessarily associated with organised criminal endeavours which themselves are less influenced by the recession.

Figure 6 shows the number of first party frauds recorded in 2011 and 2012, by quarter, and split by the type of first party fraud. This shows that over the last couple of years the number of Application Frauds recorded each quarter has remained remarkably stable. The number of Misuse of Facility Frauds has varied much more, with the last three quarters of 2012 showing a steady decline following a peak in the first.

First Party Fraud cases recorded by case type 2011-2012

Figure 6



## 6.1 Misuse of Facility Fraud

Misuse of Facility Fraud occurs when an account, policy or some other facility is used fraudulently, e.g paying in an altered cheque or knowingly making a payment that is going to bounce/be declined.

### Misuse of Facility Frauds recorded by product 2011-2012

Table 6.1.1

Product	2011	2012	% change
All-in-one	107	128	+19.6%
Asset Finance	433	607	+40.2%
Bank Account	41,018	35,801	-12.7%
Communications	5,477	3,897	-28.8%
Plastic Card	3,471	3,557	+2.5%
Insurance	90	61	-32.2%
Loan	334	341	+2.1%
Mail Order	2,952	1,278	-56.7%
Mortgage	87	123	+41.4%
Other	27	31	+14.8%
<b>Total</b>	<b>53,996</b>	<b>45,824</b>	<b>-15.1%</b>

#### The bank account and money mule issue

While *Table 6.1.1* shows that there was a bit of a mixed bag (in terms of which type of products were misused more and which were misused less) in 2012 compared with 2011, the key driver in the 15% reduction was the 13% fall in the number of Misuse of Facility Frauds against bank accounts. The majority of these frauds (65% of Misuse of Facility Frauds against bank accounts in 2012 compared with 63% in 2011) involved false instruments being paid into the account. In some cases, these would have been false or altered cheques which, while possibly perpetrated by organised criminals, would not necessarily be indicative of organised crime. A large proportion of the cases where the false instrument was an electronic transfer, however, would be. Many such cases will have been situations where the person who held the account acted as a 'money mule', receiving and possibly laundering money obtained through other criminal enterprises. These other criminal enterprises will vary: from receipt of funds obtained fraudulently from the benefits system through to far more socially damaging crimes such as human trafficking and the funding of other sinister causes or groups.

One of the reasons for the decline in Misuse of Facility Frauds recorded to the National Fraud Database is not that such frauds were occurring less, but that the banks are not recording those who had been duped into facilitating money laundering. Such instances often involve those who have fallen prey to employment scams: where the victim has (in good faith) accepted a job as a 'Financial Officer' or 'Payments Administrator'. One of the duties of this new 'job' typically involves moving payments through their own bank account. While it may be considered naïve for people to believe that any job that involved moving corporate funds through their own personal bank account was legitimate, being naïve does not make the individual guilty. Furthermore, in cases of coercion or where the account holder was him or herself a victim of a con, then (legally) that person cannot be considered guilty of fraud.

Finally, it must be noted that – over recent years – much media attention has been paid to the role of banks in how they treat these cases, with a few stories appearing in the public domain about organisations closing accounts erroneously for what had appeared to them to be 'fraudulent activity' without establishing that a full, legal, standard of proof existed. Much work has taken place within the industry – examining best practice and seeking more proactively to educate consumers about the dangers. The fall in Misuse of Facility Fraud, therefore, could be seen as a sign that such work is beginning to take effect; but the simple fact remains that Misuse of Facility Fraud was the second most common type of fraud recorded in 2012. It is worth noting too that, in some quarters, the question is being asked 'what is the responsibility of the citizen and where does it begin and/or end?'. We expect to see this issue become a far more prominent debate – legally and financially – before long.

Financial desperation may well have resulted in a number of people choosing not to look too closely at what the job entailed or, indeed (if there was one), any official 'job offer'. While it is pleasing that the numbers of unemployed have started to reduce (at time of writing), with the Office of National Statistics stating that the jobless total has fallen to its lowest level for 18 months at the end of November 2012 (down to 2.49m), that is still around a million more people out of work than there were in 2005. There will,

## Case Study

### Conspiracy to Launder Money

In 2010, a personal banker at a high street bank used his position to open a number of fraudulent personal bank accounts. Numerous high value business cheques (from several businesses that had experienced the theft of cheques) were then paid into these accounts. The fraudulently set up accounts all used names that were simple variations of the names on the cheques.

The value of the funds credited to the fraudulently opened accounts was then transferred by the bank insider through other “money mule” bank accounts from which the money was then withdrawn. These account holders were also arrested. Investigations indicated that the ‘money mules’ had been recruited specifically for the purpose by two organisers of the scheme – both operating together, although keeping their distance from the ‘running’ of any of the accounts involved.

The value of the cheques misused was in excess of £250,000.

One of these organisers was also linked to another investigation, with another suspect who was also a ‘money mule’ specifically recruited to operate an account into which (again) stolen company cheques were being paid.

The two organisers were identified through a series of links, following the arrests of the ‘money mules’. On arrest, one of the organisers’ homes was searched and further cheques (related either to fraudulently opened accounts or genuine accounts – all of which had had similar stolen business cheques paid into them) were found. These cheques had a total value of £196,000.

In total 11 individuals were charged with conspiracy to launder money.

also, be many people who are not claiming unemployment benefit (and therefore are not registered as unemployed) but who are facing a very tight economic squeeze. The challenge for organisations, therefore, is twofold. Legally, they are required to freeze accounts that have been used fraudulently for the laundering of funds. Equally, and publicly, they have a responsibility to educate their customers about what fraud is, what the dangers are, what the consequences would be, and – therefore – offer assistance to those naïve customers who might fall (or have fallen) prey to the criminals responsible for such scams.

It will not be just those who were duped who carry out ‘money mule’ activities, however. Some know that what they are doing is a crime and that they are accepting payment to launder money (although a proportion of these may not have thought through the implications of their actions). Worryingly, there are organised criminal gangs that use coercion to ensure that they have a ready supply of money mules – in some cases going as far as to take their victims into a branch to oversee the (legitimate) opening

of the account in the first place. This is a method known to have been used by groups that traffic people into the UK.

Much more, therefore, remains to be done.

Whether periods of economic recession cause fraud to occur or increase is a subject that has received academic attention and the opinions vary. The simple fact is, however, that while economic circumstance might not lead a career fraudster or organised criminal to attempt to commit more or less fraud than at any other time, for many others there may be a far greater ‘grey area’ in terms of what is right and what is wrong. Misusing an account that has been held for many years (for example, to receive payments and make payments on someone else’s behalf for a fee) might seem peculiar to an individual as a proposition. But, if that individual is having real financial difficulty, it is easy to see why they might choose to allow their account to be used in this way when, in other circumstances, they would have refused. This is, of course, one thing that many organised criminal gangs involved in the laundering of money >

rely on when attempting to recruit people to act as money mules.

The fact that the identification of Misuse of Facility Frauds against bank accounts decreased in 2012 is good news. But this does not mean that the problem has disappeared, or that organisations can in any way be complacent. ‘Money mule’ activity, has become an issue that organisations, individuals, law enforcement and society at large will have to work together to examine in order to tackle the root causes that lead to people becoming vulnerable to it.

### **Small increase in plastic card fraud hides more sinister events**

The small increase in the misuse of plastic card accounts, in percentage terms, disguised some more substantial changes in how these accounts were misused. There were far fewer cases where people attempted to pay their bill with false instruments – such as cheques that they knew would bounce (34% reduction in these frauds) – but there was a 24% increase in the number of cases where people set up regular payments from someone else’s account. There was also an increase in individuals fraudulently evading payment, which accounted for over 14% of misuse of plastic card account frauds in 2012 compared with a remarkably low 5% in 2011. What these frauds have in common is that they are all ways of someone deliberately trying to avoid paying their debts. As the average household debt (excluding mortgages) has reduced by over £2,000 in the 12 months to the end of October 2012\* this increase in those who feel the need deliberately to evade their payments seems counter intuitive. The change in the way that individuals are attempting escape payment, however, by trying to get someone else to foot their credit card bill, may well indicate that this is less to do with stretched individuals trying to keep their heads above water, and more about greed and malice.

In addition, the increase in attempting to use someone else’s account to pay a plastic card debt must also be viewed in conjunction with the increase in Facility Takeover Fraud. This is an example of someone who would not be viewed as an organised criminal actually using organised criminal methods and using one type of fraud (Facility Takeover Fraud) in order to perpetrate another (Misuse of Facility Fraud).

### **Other products, other explanations**

It remains possible that the reduction in average household debt, and the indication that there might be a light at the end of the financial darkness for the consumer, partially explained the reduction in the number of cases where a communications account was misused. In this instance, the communications product involved was typically home media. There was no change in the way that people tried to dodge paying for these services – there were just fewer instances.

This same principle applied to the reduction in the number of attempts to avoid paying for goods that were bought on mail order. Equally, the reported reduction in household debts may indicate that people were not purchasing goods that they could not immediately afford.

There was an increase in the number of cases of Misuse of Facility Frauds against asset finance agreements, however: up 40% in 2012 from 2011’s levels to over 600 cases. 87% of these cases involved the individual having fraudulently evaded making payments. More peculiarly and more interestingly, there were instances of people buying vehicles under a finance agreement, then sub-hiring those vehicles to a third party; either purely as a money-making enterprise or essentially ‘fronting’ the finance agreement for someone who would not have been able to get credit themselves. This is prohibited under the terms of an agreement as the ‘sub-hirer’ may not keep up payments or use the vehicle in line with the agreement and, therefore, counts as fraud.

2012 also saw an increase in the number of misuse of mortgage agreements. While the numbers were lower than for other products, there was a 41% increase in the number of cases identified in 2012 compared with 2011. Most of these cases involved the misuse of a mortgaged property – or, more simply, renting out a property which was subject to a residential mortgage without changing the terms of the mortgage agreement. This is likely to indicate that there were a number of people seeking to take advantage of the present rental market, and the shortage of rental properties, but who were not notifying their mortgage lender. This exposes the mortgage lender to greater financial risk, and presents another challenge to organisations in terms of their need and responsibility to educate customers in what constitutes fraud. ●

## 6.2 Application Fraud

Application Fraud relates to applications with material falsehoods (lies) or false supporting documentation (where the name provided has not been identified as false).

Application Frauds recorded by product 2011-2012

Table 6.2.1

Product	2011	2012	% change
All-in-one	86	27	-68.6%
Asset Finance	6,945	6,632	-4.5%
Bank Account	12,039	9,277	-22.9%
Communications	5,118	3,281	-35.9%
Plastic Card	4,378	4,483	+2.4%
Insurance	7,426	8,292	+11.7%
Loan	3,958	4,355	+10.0%
Mail Order	174	93	-46.6%
Mortgage	2,994	3,142	+4.9%
Other	145	286	+97.2%
<b>Total</b>	<b>43,263</b>	<b>39,868</b>	<b>-7.8%</b>

2012 saw yet another decrease in the number of Application Frauds identified by CIFAS Members. These have been declining, year on year, since 2008. It was thought that the very small drop seen in 2011 compared with 2010 (only 3%) might indicate the beginning of the end in terms of falling numbers of Application Frauds. Evidently, this was not the case, with the rate of decline increasing again in 2012 compared with 2011.

Application Fraud, after all, is probably the easiest fraud type for a layperson to comprehend: it involves making false declarations in order to obtain a product (e.g. inflating annual income by £10,000 in order to obtain a mortgage).

The overall decline in Application Fraud must be taken in context of the current, squeezed, economic climate. If it is reasonable to assume that many individuals might perceive the need to make fraudulent declarations in order to obtain products and services that they need or want, it is also reasonable to accept that organisations will have more

strict criteria in place (in terms of affordability for instance). This will continue to mean that many attempted frauds will simply not meet an organisation's more stringent criteria and will not reach the organisation's fraud department. No fraud checks will therefore, take place, no frauds will be recorded, and the Application Fraud figures will appear to be fewer. It is important to bear in mind that – because of this – there is potentially a large amount of attempted Application Fraud that has escaped detection.

The simple matter is that a steeper drop in Application Fraud numbers does not mean that fewer frauds are being attempted: to argue this oversimplifies the picture.

As with some of the other types of fraud already examined in this report, however, an overall drop of 8% disguises some interesting changes in the number of frauds identified which have affected the different products.

### In an ideal world

Most of the decrease in Application Fraud came from a 23% drop in the number of fraudulent applications for bank accounts, although they remained the product most targeted in Application Frauds. There are various explanations for this. First, a number of fraudulent applications are failing to pass credit scoring, resulting in the application being declined before fraud can be identified. In an ideal world, these applications would be passed to the bank's fraud prevention teams for further investigation, and, if fraud is confirmed, recorded to the National Fraud Database. The reality though, is that pressure on resource within these units mean that they are required to focus their attention on those cases where the facility could be granted and, therefore, where the bank would be exposed to risk.

The exception – especially in the light of the figures presented in section 3 – remains cases of impersonation (Identity Fraud), where further investigation is required to protect an innocent victim's identity from further abuse. Another factor may also be that some bank accounts, the basic bank accounts, are designed to be accessible to all: including those who have a poor credit history. >

So, where someone applying for a mainstream bank account may have thought they had to hide the fact that they had a County Court Judgment (CCJ), this is not material to the decision as to whether to offer a basic bank account, and therefore no requirement to hide it. This again poses questions to organisations, concerning consumer education: do organisations have a responsibility to explain, more clearly, eligibility requirements for different types of account? And what – therefore – would constitute fraud should an applicant attempt to make fraudulent declarations?

### **The economy as motivation: is it really that simple?**

Partially counterbalancing the decline in Application Frauds against bank accounts was an increase in those against plastic cards and loans - up 6% across both products from 2011. Both of these products experienced an increase (in terms of volume and the percentage of cases) in people failing to disclose addresses where they have adverse credit information. There was, however, a decrease (again, both by volume and percentage) of cases of people giving false employment details. The logical conclusion is that there were more people with adverse credit information who thought that they needed to hide this in order to get the loan or credit card that they wanted.

Considering the reduction in average household debts, however, and taking CCJs as one representation of the level of adverse credit in the consumer marketplace, then the situation was not as clear cut as it might have seemed initially. According to Registry Trust\*, the number of CCJs issued to consumers reduced meaning that the argument concerning economic pressures seems less persuasive. Why, then, the increase in the number of people fraudulently hiding information? Oddly enough, this is likely to have been due to the reappearance of some appetite for less risk averse lending practices, more in line with those seen before the onset of the global financial crisis. As mentioned earlier, in many sectors, an array of Application Frauds will not have been identified due to credit scoring or lending criteria meaning that the application was screened out before any fraud checks could take place. Conversely, as criteria becomes less strict, more applications will be fraud checked and – therefore – an increase in fraud is identified. This, of course, assumes that these frauds originate from applicants who intend to honour any debts, which will not always be the case. So, it must be acknowledged that the growth is equally likely to be driven by an increase in people who just want to take the money and run.

The decrease in the number of people providing false employment details makes sense in light of the increasing levels of employment in the UK. The decrease in such cases, however, was substantially greater than the decrease in the unemployment rate: cases for plastic cards decreased from 24% of Application Frauds in 2011 to only 10%, and for loans this dropped from 10% of cases to 6%.

### **How fraud works and how it can be prevented**

Another aspect of the increase in loan fraud cases was the increased prevalence of less mainstream lenders. The nature of fraud is that fraudsters will not just target one organisation. This is part of the reason for the success of CIFAS' data sharing system, as it brings multiple organisations together from numerous sectors. When new organisations appear in the marketplace, it is inevitable that fraudsters will target these new organisations in the hope that their fraud defences will be deficient.

A real cause for optimism in the increase of recorded cases of Application Fraud for loans was that a substantial proportion of the increase was a result of the Student Loans Company recording the cases that they identify to the National Fraud Database. This helped other participating organisations to prevent those same fraudsters from attacking them – and of course, the Student Loans Company was able to use the fraud information recorded by other Members to prevent individuals from obtaining a student loan to which they were not entitled. This sends a clear message that fraud against the public sector is unacceptable and is an excellent example of the benefits of public/private data sharing.

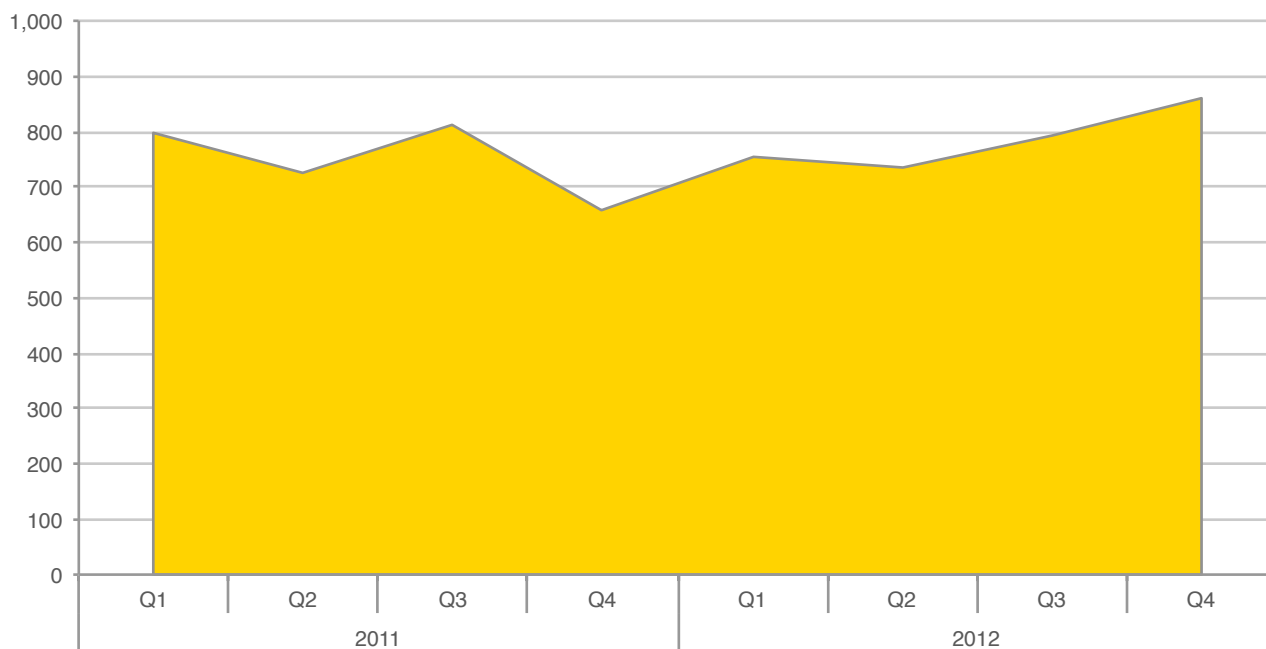
### **Fraud – when trying to buy a house**

Mortgage Application Fraud increased in 2012 compared with 2011 by almost 5%, reversing an 11% decline in 2011 compared with 2010. As can be seen from *Figure 6.2.1* on page 41, there has been a relatively steady increase since the number of mortgage Application Frauds bottomed out in the fourth quarter of 2011.

What was interesting was the change in the nature of the mortgage-related frauds which were being identified within Application Frauds. First, there were fewer cases of false employment details being provided. This was down from 17% of cases in 2011 to 14% in 2012 and could be seen as a reflection of the overall drop in unemployment in the UK. Aligned to this was a decrease in the type of fraud carried out to try to make it appear that the applicant earned more than they did (like providing false or altered

## Mortgage Application Fraud cases recorded 2011-2012

Figure 6.2.1



documents to prove income). This type of fraud accounted for 45% of cases in 2011, but dropped to 33% in 2012.

Conversely, hiding adverse credit information (most commonly hiding the address where the adverse information was registered, but also just failing to disclose the adverse information) increased from 34% of cases in 2011 to 43% in 2012. While this finding flies in the face of the reported decrease in average household debt, it may have been that some considered that 2012 was the year to get on the housing ladder, or that it was time to move home. In a year where total mortgage lending was marginally up from levels recorded in 2011\*, but where house prices in some areas of the country were still beyond the reach of many potential buyers, this increase probably indicated the desire of many to try to take advantage of an opportunity rather than a reflection of a greater number of people with adverse credit information against them.

#### Trying to ensure that the price is right

Application Frauds for insurance increased again in 2012 compared with the previous year, consolidating the position of insurance as the second most commonly targeted product by application fraudsters. These frauds have seen an upward trend over the last two years.

On the face of it, there appeared to be two main reasons for committing Application Fraud to obtain insurance

– to procure a lower quote and/or to avoid paying the premium altogether. While neither can be condoned, the first is perhaps the more understandable of the offences. Insurance, especially for the young, can be prohibitively expensive – and it is something that anyone with a car has no option but to purchase. It was therefore not surprising to see an increase in people providing a false address. This was people claiming to live in a better neighbourhood than they actually did in order to give the impression that the vehicle was at less risk and therefore to reduce the premium – most probably involving people still claiming to live with their parents when they had moved out. This accounted for 18% of Application Frauds for insurance, up from less than 16% in 2011.

An emerging fraud, probably committed for similar reasons, was the fronting of an insurance policy. This was where someone else took out insurance, stating that a third party was a named driver, when in reality that named driver was the primary driver of the vehicle. Again, this was generally likely to be a parent taking out insurance on behalf of a child. While some might not see this in the same way as something more blatant (like failing to disclose previous claims or criminal convictions), the upshot is the same: by claiming that someone may only occasionally drive a vehicle, they are understating the risk of that vehicle being involved in a situation that would result in a claim. >

\* [www.bbc.co.uk/news/business-21119628](http://www.bbc.co.uk/news/business-21119628)

Historically, it has been young men who have borne the brunt of insurers' pricing policies. They were more likely to be involved in accidents, so they were asked to pay higher premiums. This, of course, meant that they were more likely to commit fraud in an attempt to reduce the premium. It remains to be seen whether the European Court of Justice ruling that insurance pricing must become gender neutral will result in lower premiums for men, and therefore fewer men will feel the need to commit fraud to reduce the premium, or whether (instead) it results in higher premiums for women, and lead more women to commit fraud as a result.

#### Other rogue elements

The number of cases where false payment details of some description were provided increased in 2012 compared with 2011 – up to 57% of cases from 42% in 2011. This type of Application Fraud, involving attempts to avoid payment completely, has a number of very serious implications. Many of these frauds were perpetrated by an individual acting as 'broker' for a client. They took the money from their client, applied on their behalf, but provided false payment details. These may have been false bank account details, false card details or compromised card details. The policy documentation would have been issued at the point of application, but the policy voided when the payment subsequently failed to be processed, or was claimed back. In the meantime, the unwitting client would have been presented with the paperwork on their 'policy': meaning that they would be driving on UK roads, believing that they were covered, but were actually uninsured drivers. Of course, a number of these cases of false payment details did not involve someone being 'duped'. They may have been perfectly aware that they did not have a valid policy but, provided they had the necessary paperwork with which to tax their car, they were not worried.

More serious than those who believed they were covered by an insurance policy when they were not, was where these frauds were used to facilitate 'cash-for-crash' cases on British roads. Whether these staged accidents involved an innocent member of the public being induced to crash into another, or where the event involved two or more complicit drivers, these attempts to submit false claims for financial gain presented a very real risk of physical harm to other road users and pedestrians alike. ●

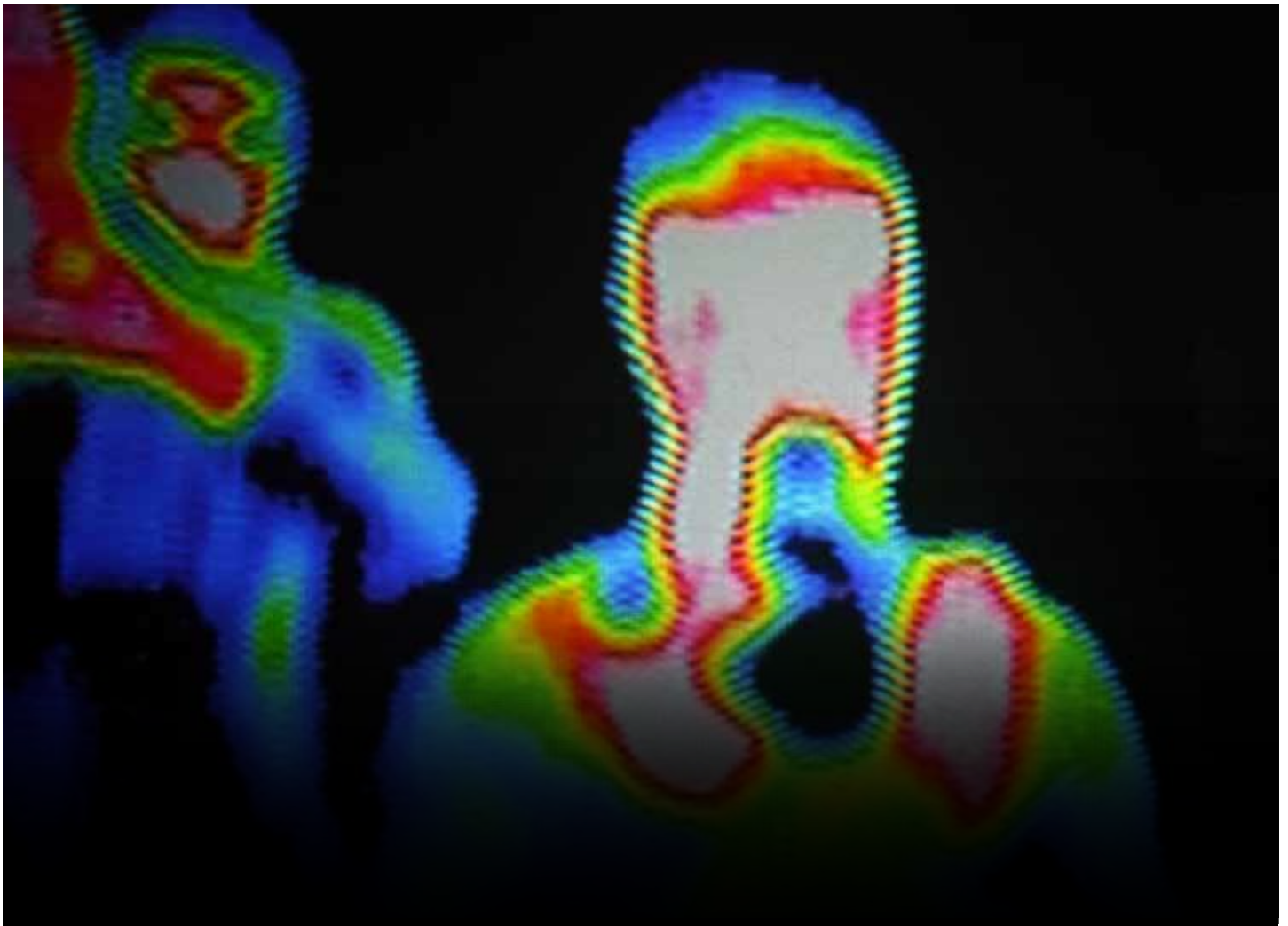
## Case Study

### Teen 'ghost broker'

A teenager who attempted to sell worthless vehicle insurance online was handed a 12-month conditional discharge in January 2013, after admitting to posting four adverts in a bid to dupe drivers into paying out for bogus policies.

In February 2012, the 19-year-old failed to persuade anyone to invest in his fraudulent scheme but one suspicious internet user reported the adverts to the Insurance Fraud Enforcement Department (IFED). IFED detectives arrested the teenager in May 2012 and seized a computer on which they found falsified insurance certificates.

Head of IFED, DCI Dave Wood, said: "Illegal insurance advisers, known as ghost brokers, are costing the industry millions and casting thousands of drivers unknowingly into the role of law breakers as soon as they get behind the wheel with no insurance."



# Use a comprehensive tool kit to hunt down fraudsters

- Investigate and record fraud at application through anomaly detection with current and previous applications.
- Check anomalies against Experian's extensive data assets to identify inconsistencies.
- Analyse your current customer file and screen against multiple data sources to identify possible 'Bust out' or 'Sleeper fraud'.
- Uncover fraud network links to prevent organised fraud groups attacking your organisation.
- Combine data about individuals and households at any point in the credit life-cycle to assess propensity of fraud occurring at that address.
- Use device reputation technology to offer a global fraud prevention service that reduces cyber crime.

Experian Identity and Fraud provides a complete Fraud service to help you target fraudsters effectively. Used as separate solutions or combined for more in-depth searches, Experian can help you find the right fraud prevention strategy to suit your organisation.

For further information, contact

**0845 266 6604**

**Request a call back**

**Or visit our website**



## 6.3 Asset Conversion Fraud

Asset Conversion Fraud relates to the unlawful sale of assets subject to a credit agreement where the lender retains ownership of the asset (for example, a car or lorry).

Asset Conversion Fraud recorded 2011-2012

Table 6.3.1

	2011	2012	% change
Asset Finance	532	337	-36.7%

The number of these cases decreased abruptly between 2011 and 2012. *Figure 6.3.1* shows when this happened in more detail.

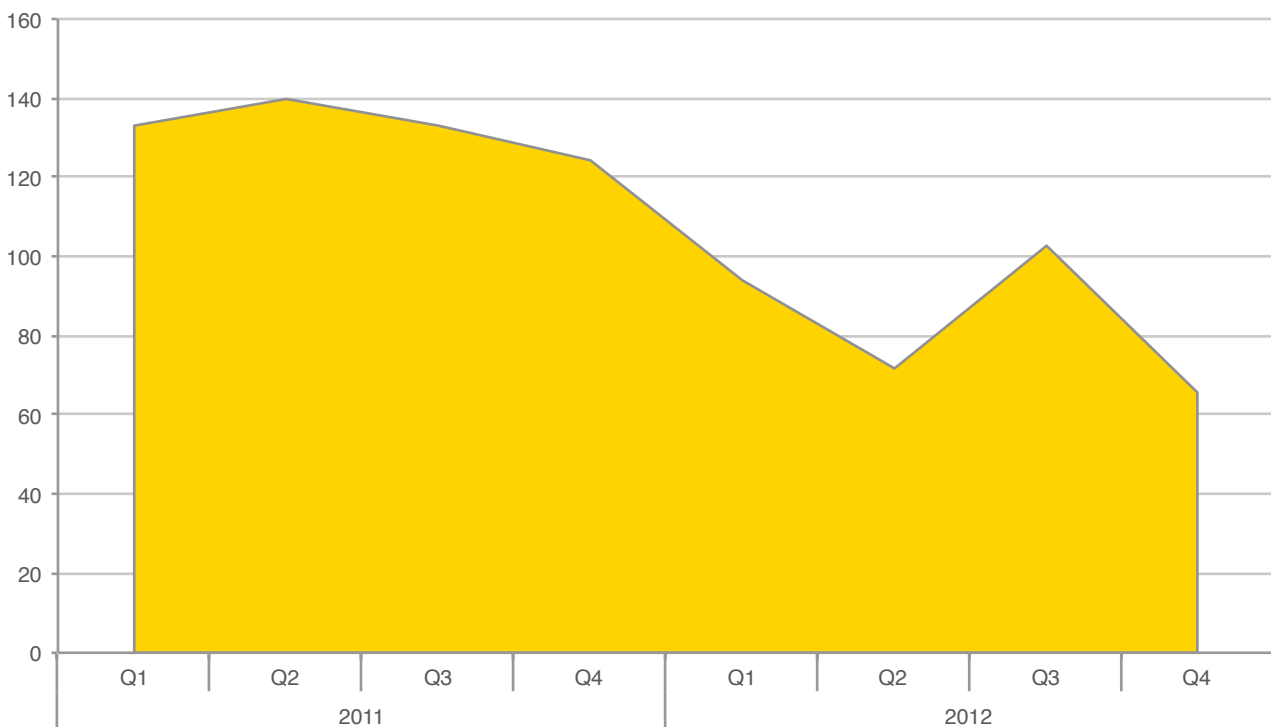
### A question of resource?

Asset Conversion is a type of fraud specific to asset finance companies, but it is by no means the most common fraud suffered by them (see Appendices). There were over 6,500 cases of Application Fraud for asset finance accounts recorded in 2012, compared with 337 Asset Conversion Frauds. Every Asset Conversion Fraud, however, carried

the potential to be more financially damaging to the organisation than other fraud types. Most Application Fraud cases were identified prior to finance being approved, thus nullifying most of the risk. Asset Conversion Frauds are identified only *after* the metaphorical horse has bolted, leaving the finance house out of pocket. Fewer of these cases were identified and recorded to the National Fraud Database – which implies that asset finance companies are incurring the associated costs less often, which would be a good thing. The reality, though, may not be that simple. If cases of Asset Conversion Fraud were actually written off

Asset Conversion Frauds recorded 2011-2012

Figure 6.3.1



as bad debt, without further investigation, then the frauds would not have been recorded, thereby losing valuable insight and prevention opportunities. Where resourcing within asset finance companies is tight, there will be a need to prioritise cases depending on the outstanding value of the asset. If an asset is of lower value, or the fraud occurs later in the life of the finance agreement, then the investigation of the fraud is likely to be a much lower priority than tracing an asset of greater value or which has a far higher outstanding value. It may, therefore, be that such lower value frauds were not identified and recorded to the database.

#### The financial 'need': has it reduced?

Another possible contributory factor was the previously high credit limits that affected credit granting over recent years. It is possible that those who may have been prepared to convert an asset further down the line, were actually declined credit in the first place: thereby meaning that the individuals who would have gone on to commit Asset Conversion Fraud were not in a position to do so. Looking at the situation more positively, however, the previously mentioned reduction in average household debt may mean that the number of people selling a vehicle that they did not actually own as a viable way of easing some of their financial pressures has actually reduced. ●

**SIRA** Syndicated Intelligence  
for Risk Avoidance

## Revolutionary solutions for fraud and risk management

- ▲ Advanced application fraud prevention solution
- ▲ Transactional monitoring for effective fraud detection
- ▲ Integrated case management system
- ▲ Automated fraud network & data mining modules
- ▲ Risk ranking & sophisticated scoring capability
- ▲ Employee fraud screening
- ▲ Procurement fraud identification
- ▲ Real-time and batch infrastructure

**01782 664000**

**[sirasales@synectics-solutions.com](mailto:sirasales@synectics-solutions.com)**



## 6.4 False Insurance Claims

False Insurance Claims occur when an insurance claim, or supporting documentation, contains material falsehoods (lies).

### False Insurance Claims recorded 2011-2012

Table 6.4.1

	2011	2012	% change
False Insurance Claims	396	279	-29.5%

The number of these cases decreased sharply between 2011 and 2012.

#### Understanding the insurance figures

Not all UK insurers are Members of CIFAS, and the requirement that each fraud recorded to the National Fraud Database should be backed by sufficient evidence to support a report to the police means that only a percentage of False Insurance Claims are recorded. In many instances, attempts by the insurer to verify a claim (seeking further detail or supporting evidence) results in claimants withdrawing their claim and walking away when they realise that their attempt to defraud the insurer will be unsuccessful. This often leaves the insurer with insufficient evidence to prove a case of fraud. The Association of British Insurers reported that false claims in 2011 numbered 138,814 and were valued at nearly £1billion\*.

#### Claiming for events that did not happen (or did not happen quite as the claim indicated)

So, bearing in mind that the number of confirmed false claims recorded to the National Fraud Database is very understated, what can be learnt? First, the majority of the decline in 2012 compared with 2011 was due to a reduction of false claims in motor insurance. These reduced by 43% compared with a 2% reduction in false household insurance claims. The most substantial reduction within false motor insurance claims was for staged accidents which accounted for 59% of claims in 2011, but was down to 42% in 2012.

Claims for events that did not take place also reduced by number, but increased as a percentage of the total, from 16% of false motor insurance claims in 2011 to 25% in 2012. On the face of it, from a public safety angle, this is encouraging as the implication is that there were fewer cash-for-crash events (endangering other road users and pedestrians) and a greater emphasis on events that

didn't happen at all – which clearly endanger no-one, but still result in a possible fraud loss to the insurer. What did increase, by volume of claims, was the number of instances where it was claimed that a vehicle had been stolen. Again, this is a type of fraud that has contributed to an extra £50 per year being paid by every UK policyholder – the figure that the Association of British Insurers quotes as the cost of fraud.

Within claims on household insurance, the most common offences were (as in 2011) claiming for events that were not covered by the policy. This included claiming for damage that had taken place before insurance was taken out and claiming for an event that took place outside the cover period – 34% of claims. This type of fraud can be seen as opportunistic but also, to a certain extent, the product of desperation. Damage has occurred, and in many cases the individual has paid for insurance over a prolonged period, so this could be seen as the individual trying to find some way to make those two factors tally. There were proportionally fewer instances of inflating a claim (down to 8% of claims from 14% in 2011), implying that there were less instances of people trying to get more from a claim than they were owed but, in contradiction to this, there were numerically more cases where the event was staged: so the individual was claiming when they were owed nothing at all. ●

## 6.5 Who is the first party fraudster?

In contrast to identity crimes, it is possible to draw conclusions about fraudsters by examining the details of those submitting and committing first party frauds. The details provided in these cases relate to the individual who has committed the fraud, and therefore some assessment can be made as to the demographics of those who commit fraud in their own name.

The gender of the subjects involved in first party fraud was recorded 94% of the time. The gender distribution for each of the first party fraud types can be seen in *Figure 6.5.1* below.

### Fraud: a male game?

It can be seen from *Figure 6.5.1* that men were disproportionately involved in first party fraud. They accounted for more than 70% of subjects in all fraud types with the exception of Application Fraud, where the proportion of male subjects increased to 69% of subjects (compared with 67% in 2011).

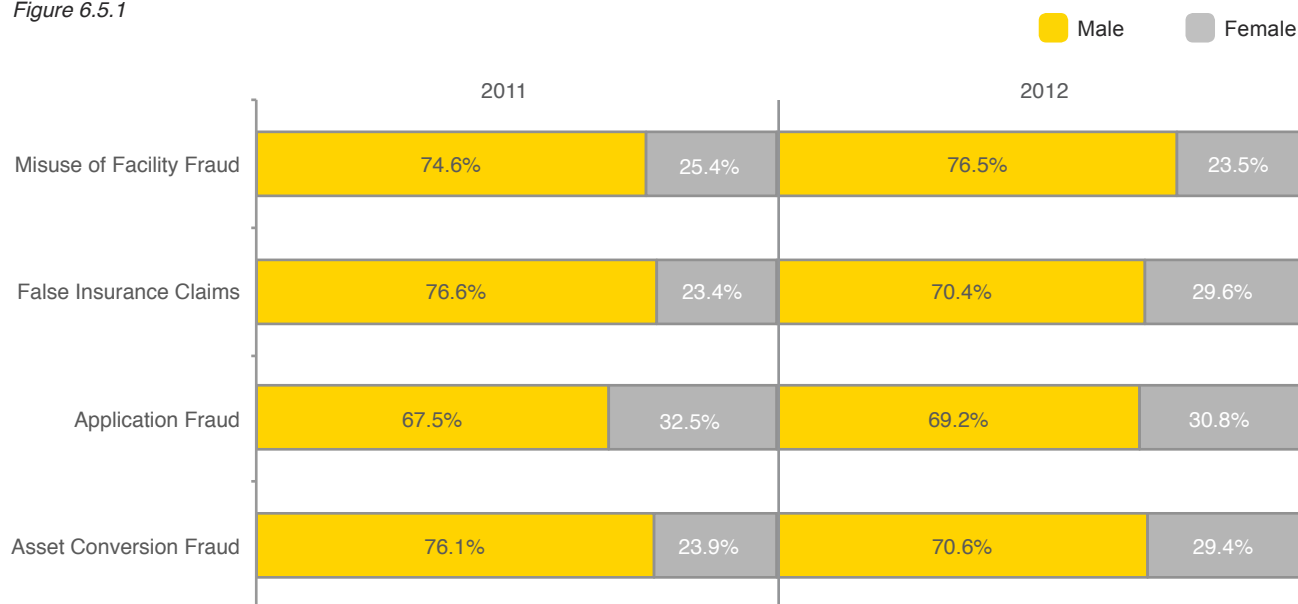
The proportion of men involved has increased in two of the four first party fraud types, and the proportion of women

increased in the other two. There was a higher proportion of women involved in False Insurance Claims, with variations depending on the nature of the claims. Men were more associated with motor insurance claims, while women (although still in the minority) were proportionally more likely to be involved in home insurance claims. The decrease in motor insurance claims recorded in 2012 therefore resulted in an increased proportion of women involved in False Insurance Claims as a whole. There was also a higher proportion of women involved in Asset Conversion Fraud. This, again, as a fraud type that typically involves a car, has traditionally been very male dominated, with over 75% of subjects involved in this type of fraud in 2011 being men. In 2012, this figure dropped to 71%. There was, however, a relatively low number of such cases recorded in 2012, so a small change by number of subjects makes a more substantial proportional change.

Comparatively, more men were involved in Application Fraud in 2012 than in 2011 and, again, this change had its roots in fraud against insurers. Men were more likely to be involved in motor insurance Application Fraud, and this was the type of Application Fraud that saw the >

Gender Distribution of First Party Frauds recorded 2011-2012

Figure 6.5.1



highest numerical increase – pushing up the proportion of male subjects involved in Application Fraud generally. Those involved in Misuse of Facility Fraud also increased slightly. This change was mostly driven by the change in gender distribution of those who misused their bank account. The numbers of these frauds decreased in 2012 compared with 2011, but there was a greater proportionate reduction in women misusing their bank account than men. As the majority of these frauds bore the hallmark of money muling, and it was only the complicit who were being recorded to the National Fraud Database, this suggests that men were more willing to get involved in this type of criminality for financial gain than women.

**Fraud: a young person’s trade?**

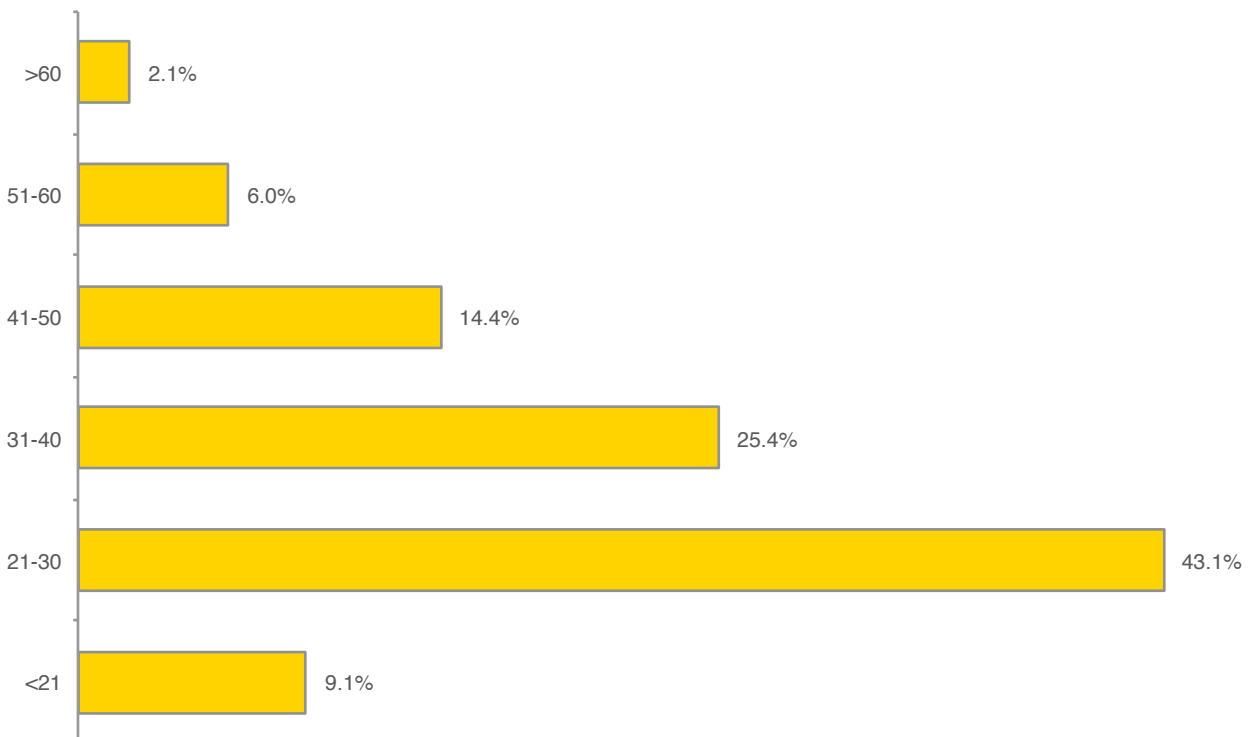
By far the most common age group involved in committing first party fraud in 2012 was between 21 and 30. They accounted for 43% of subjects. A quarter of subjects were 31-40 years of age. The age distribution of first party fraudsters in 2012 can be seen in *Figure 6.5.2* below. This distribution changed only minimally in 2012 compared with 2011.

*Figure 6.5.3* (page 49) shows the proportion of those in different age ranges committing different types of fraud. These figures present the data for 2011 and 2012.

The most obvious finding is that there was little change in the distribution of fraud types across the age ranges. It was clear that the younger a subject was, the more likely he or she was to be involved in Misuse of Facility Fraud. Over 65% of subjects involved in Misuse of Facility Fraud were less than 31 years of age and nearly 90% of the subjects under 21 years of age had been involved in this type of fraud. This finding was unsurprising as it is well-known that criminal gangs attempting to recruit money mules target students. They do so because they are confident that their target will be looking for some extra cash (and what student isn’t?) and that either they will be willing to overlook the criminality that they would be getting involved in, or be naïve enough not to realise that what they are being asked to do amounts to money laundering.

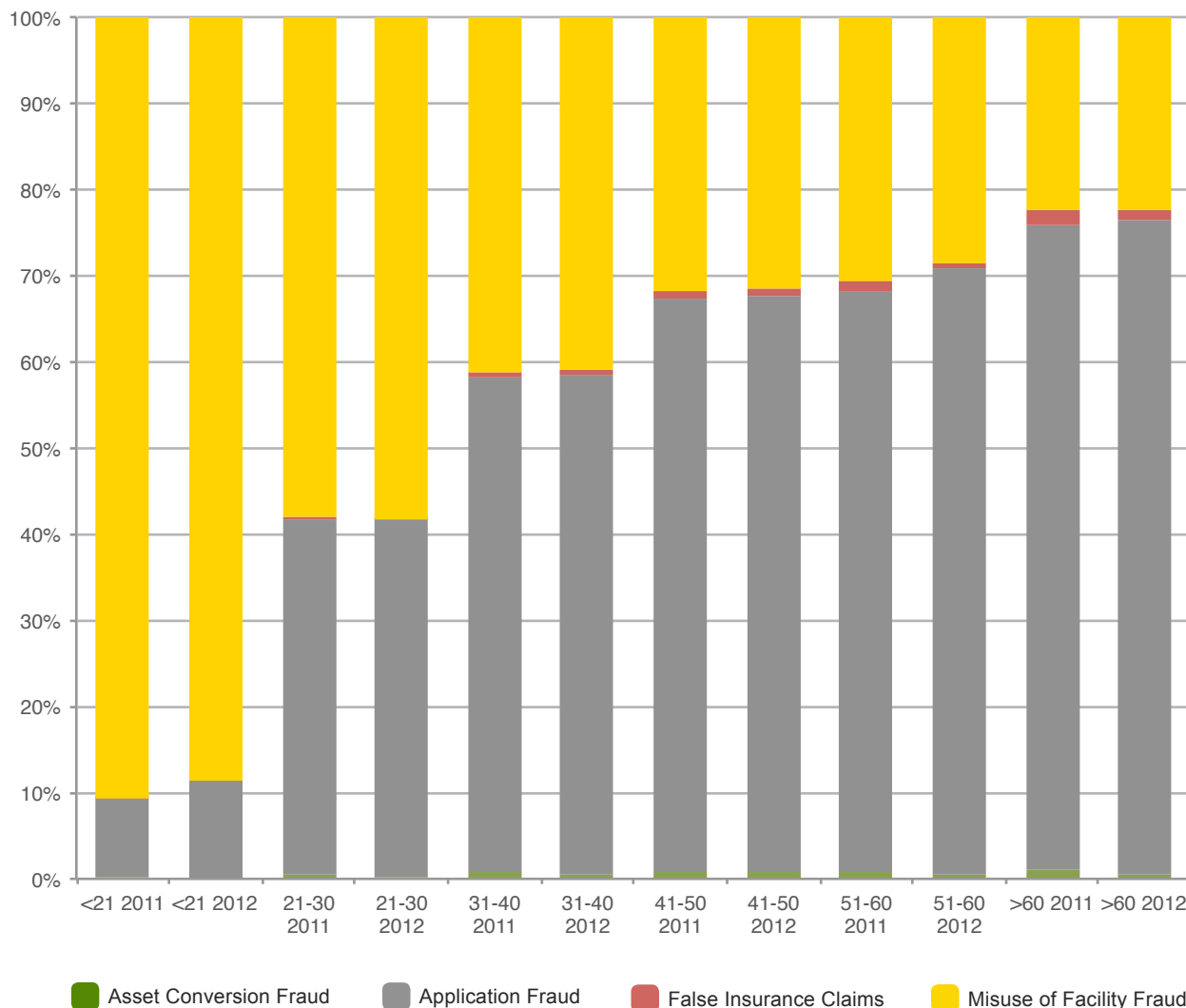
Fewer young people were involved in Asset Conversion cases. It may be that, with the previously stringent lending conditions, younger people had struggled to obtain finance

Age Distribution of First Party Frauds recorded 2011-2012  
*Figure 6.5.2*



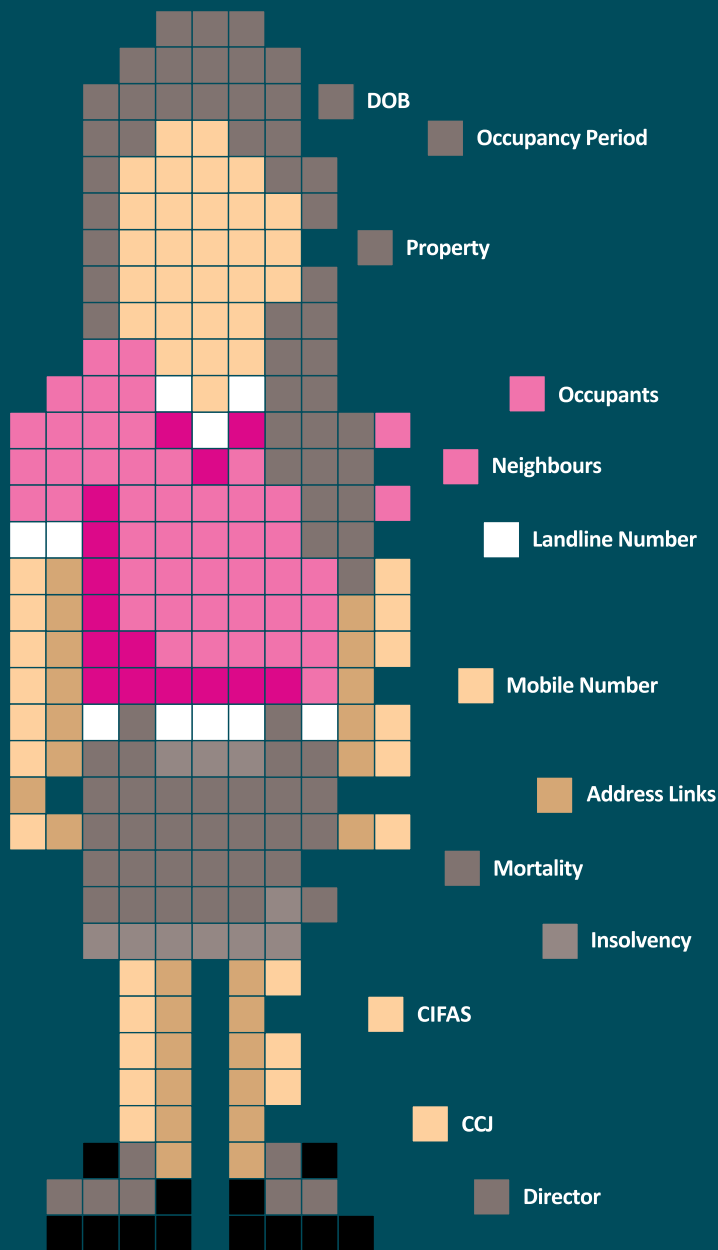
Age Distribution of First Party Frauds recorded by fraud type 2011-2012

Figure 6.5.3



in the first place, leaving a smaller number with assets to convert. There were also relatively few under 30s involved in False Insurance Claims. This was attributable partly to the number of home insurance claims. In order to make a false claim under home insurance, one needs to have a home insurance policy. A proportion of under 30s would still be living at home, or renting, and therefore would be less likely to have insurance. This is less prevalent among the older age brackets, where individuals have more to insure and a tendency to protect themselves and their belongings.

Only 3% of those involved in Application Fraud were over 60 and this age range accounted for only 2% of all first party fraudsters – making them the most honest of all the age ranges. What was peculiar, however, was that the older a subject was, the higher the likelihood that they had committed Application Fraud, with over 75% of the over 60s identified as involved in first party fraud having committed Application Fraud. •



## Building a full picture of fraudsters

Fraudsters will utilise any piece of personal data they can get their hands on to construct plausible stories; TraceIQ gives you the power to see the full picture and break down their deception.

Already utilised by an array of blue chip fraud investigation teams, **TraceIQ v2.2** features a range of powerful data and functionality including:

- ▶ **CIFAS National Fraud Database search feature**
- ▶ **Over 100 million mobile and landline numbers**
- ▶ **A wealth of consented data - including addresses, dates of birth and telephone numbers**

Experience **TraceIQ v2.2** for yourself - contact us today to claim your free, no-obligation trial

## 7. Defeating Fraud: Whose Responsibility is it Anyway?

The question of who is responsible for combating fraud will produce a variety of answers.

On the one hand, organisations are to be expected to do all that they can to keep their customers safe and so, when they do not, customers will inevitably feel that they have been let down in some way. On the other hand, if an individual acts negligently in a way that makes it easier for a fraudster to impersonate them or take over an account, this cannot be laid at the door of the organisation. Furthermore, if arrests and sentences of prolific fraudsters are not forthcoming, is there any real deterrent to those who profit from fraud and economic crime?

### Complexities

The multiplicity of possible solutions put forward tend to deal only with a part of the problem. Organisations that make security too strenuous a process to get through may succeed in deflecting much of the fraudsters' attention, but they also risk losing customers who want a service provider that is easy to use.

Harsh sentences for prolific fraudsters may deter some individuals but risk making criminal actions far more insidious and wide ranging; drawing more and more people (willingly or unwillingly) in as accomplices until any hope of catching the ringleaders is lost.

Furthermore, what of those 'grey areas': people who have been duped unwittingly into allowing themselves to be used as a 'money mule', or those who did not see the use of fake payslips to support an application as a crime, more of a means to an end? Are they to be treated with the same severity as those whose fraud is more organised, more criminally motivated, and more damaging to victims?

### Recognition of equal responsibility

Much is made of the consumer or the individual, and it is true that the individual has as significant a role to play in defeating fraud as law enforcement or organisations. The oft expressed idea is that (in the UK) the concept of policing by consent ("derived not from fear but almost exclusively from public co-operation with the police"\*) is how law

enforcement works. While we expect the police to keep streets safe, for instance, the individual recognises that they must play a part too. To use an analogy, if an individual left their car unlocked with keys in the car too, would they be able to blame either the police for the theft of the car, or the insurance company for not paying out on any policy? Of course not!

Similarly, society recognises that certain standards of behaviour are ours to maintain. Therefore individuals do have a key part to play in keeping their data safe: whether it is by ensuring that their passwords or online accounts are secure or by keeping their computer fully shielded against online threats such as malware and spyware, for example.

### Corporate responsibility

But organisations cannot escape their responsibilities. As suggested previously in this report, shouldn't organisations have a responsibility to educate customers of what constitutes fraud and the potential consequences? Many will argue that it is their social and corporate responsibility at the very least. Similarly, many organisations have invested heavily in updating and changing their security and identification processes for online transactions and have updated terms and conditions to reflect these changes. How aware are their customers of the new terms, however, and what it means for them and their own responsibilities?

Similarly, with many online service providers now insisting that consumers must download specific security programmes, is it reasonable to expect the customer to do this when they have already paid for universally used and recognised security software (especially when individuals are also told to beware what programmes they download to their computers, lest they import malware)? Furthermore, within such terms and conditions, should it not be the responsibility of the organisation to ensure that accounts cannot be set up without complex passwords (e.g. mixes of upper and lower cases, numerals and symbols), and not simply with variations of the word 'Password'? If the customer is to be expected to use 'complex' passwords, then surely organisations have a responsibility to ensure that they do? >

\* Charles Reith, *A New Study of Police History* (1956) <http://britishfreedom.org/policing-by-consent/>

### **Completing the jigsaw**

And what is the role of government and law enforcement? In terms of reporting suspicious activity, much intelligence is shared with law enforcement since the 9/11 terrorist attacks. But, how many of these reports are acted upon by law enforcement? Or is it just organisations acting, by closing suspicious accounts? Increased intelligence gathering is playing its part – with law enforcement looking more at disruption work as a means of preventing fraud. Such disruption work, however, has to be aligned with the prosecution of those fraudsters who are apprehended. Similarly, can the private sector and consumers really be expected to do whatever they can in the fight against fraud, if government does not also act to co-operate and ensure that all public sector bodies join in with proven fraud fighting techniques such as data sharing?

The simple fact is that there is no way to defeat fraud completely. There is no silver bullet. And if there was, it would not be one person's or one organisation's responsibility. Ultimately, when it comes to whose responsibility it is to fight fraud, it is a shared one: and all parties must play an equal part, otherwise each and every effort will fail. ●

# Appendix: Fraud by Product Type

## All-in-one

- There has been a substantial increase in the number of frauds affecting all-in-one products, with the bulk of the increase relating to Facility Takeover Frauds. Fraudsters target this type of product to gain access to a range of products through one account, and to take advantage of an existing relationship.
- The reduction seen in both the number of Application Frauds and Identity Frauds relating to all-in-one accounts may indicate that these products are still subject to relatively high credit score cut-offs – so masking the true extent of the problem.

An All-in-One product is one where a group of financial products are offered together and operate through interaction.

Fraud Type	2011	2012	% change
Application Fraud	86	27	-68.6%
Facility Takeover Fraud	209	583	+178.9%
Identity Fraud	216	178	-17.6%
Misuse of Facility Fraud	107	128	+19.6%
<b>Total</b>	<b>618</b>	<b>916</b>	<b>+48.2%</b>

## Asset Finance

- Frauds related to asset finance decreased in 2012 compared with 2011, although the percentage decrease was less than the year before (-14.8%).
- Application Fraud was the most common type of fraud against asset finance, even though it decreased: the number was still over 10 times greater than the next most common fraud type.
- Misuse of Facility Fraud gathered pace, with a 40% increase in 2012 compared with 2011, following a 6% increase the year before. 87% of these frauds related to fraudulent attempts to evade payment.

Fraud Type	2011	2012	% change
Asset Conversion Fraud	532	337	-36.7%
Application Fraud	6,945	6,632	-4.5%
Identity Fraud	325	282	-13.2%
Misuse of Facility Fraud	433	607	+40.2%
<b>Total</b>	<b>8,235</b>	<b>7,858</b>	<b>-4.6%</b>

## Bank Accounts

- Frauds against bank accounts decreased by 17% in 2012 compared with 2011, across all fraud types, except Facility Takeover Fraud.
- This increase is most probably explained by the proliferation of data available to fraudsters, and their desire to be able to access the money in their victim's account directly.
- The biggest decrease (by volume) was in Misuse of Facility Fraud. This was a result of a drop in the number of people identified as complicit in 'money muling' activity. However, the number of people falling victim to scams which tricked them in to laundering money (and therefore not recorded on the database).

Fraud Type	2011	2012	% change
Application Fraud	12,039	9,277	-22.9%
Facility Takeover Fraud	2,814	4,166	+48.0%
Identity Fraud	14,873	9,236	-37.9%
Misuse of Facility Fraud	41,018	35,801	-12.7%
<b>Total</b>	<b>70,744</b>	<b>58,480</b>	<b>-17.3%</b>

## Communications

- Fraud against communications products, predominantly mobile phones, decreased by 23% in 2012 compared with 2011, following an increase of 25% recorded in the previous year.
- The biggest decrease (by volume) was seen in Identity Fraud. This was strange, given the overall increase in this type of fraud. One of the reasons for the decrease, though, as well as that seen in Application Fraud, was the tightening up of security procedures used at the time of account opening.
- Facility Takeover Fraud was the only type of fraud against communications products to increase. In these cases the fraudster either wanted to access the account itself (to obtain upgrades etc.) or they were looking to use this as a springboard to taking over other types of account (e.g. bank accounts) and needed the communications platform as a facilitator.

Fraud Type	2011	2012	% change
Application Fraud	5,118	3,281	-35.9%
Facility Takeover Fraud	6,136	6,758	+10.1%
Identity Fraud	25,996	18,864	-27.4%
Misuse of Facility Fraud	5,477	3,897	-28.8%
<b>Total</b>	<b>42,727</b>	<b>32,800</b>	<b>-23.2%</b>

## Plastic Cards

- Fraud against plastic cards increased by over 26% compared with 2011. This followed a 6% increase the year before. All types of fraud perpetrated against plastic cards increased.
- The most substantial increases were in the identity related crime fraud types, showing that once again, plastic cards were a target of choice for identity fraudsters.
- First party frauds also increased, with more attempts to hide adverse credit information at application stage, and more fraudulent attempts to set up regular payment instructions from someone else's account.

Fraud Types	2011	2012	% change
Application Fraud	4,378	4,483	+2.4%
Facility Takeover Fraud	9,719	13,997	+44.0%
Identity Fraud	24,582	30,989	+26.1%
Misuse of Facility Fraud	3,471	3,557	+2.5%
<b>Total</b>	<b>42,150</b>	<b>53,026</b>	<b>+25.8%</b>

## Insurance

- Frauds against insurance increased by 9% in 2012 compared with 2011. This increase was driven almost exclusively by Application Frauds.
- These Application Frauds predominantly involved the provision of false or compromised payment details. It is believed that the majority of these frauds originated from 'ghost-brokers' – individuals who duped their 'clients' into believing they were insured.

Fraud Type	2011	2012	% change
Application Fraud	7,426	8,292	+11.7%
False Insurance Claims	396	279	-30.1%
Identity Fraud	27	32	+18.5%
Misuse of Facility Fraud	90	61	-32.2%
<b>Total</b>	<b>7,939</b>	<b>8,664</b>	<b>+9.1%</b>

## Loans

- Frauds against loan products increased by 46% in 2012 compared with 2011, with the majority of the increase driven by an 87% increase in Identity Fraud.
- This increase was a reflection of the increased take-up of payday loans and other forms of less traditional lending, both by identity fraudsters and by first party fraudsters (Application Fraud). This was undoubtedly prompted by the speed and perceived accessibility of these products.

Fraud Type	2011	2012	% change
Application Fraud	3,958	4,355	+10.0%
Facility Takeover Fraud	8	5	-37.5%
Identity Fraud	3,795	7,104	+87.2%
Misuse of Facility Fraud	334	341	+2.1%
<b>Total</b>	<b>8,095</b>	<b>11,805</b>	<b>+45.8%</b>

## Mail Order

- Frauds against mail order accounts increased by 45% in 2012 compared with 2011, following a 6% drop the year before. This increase was driven by mail order again being extensively targeted by identity fraudsters, something which contributed substantially to the overall increase in Identity Fraud seen in 2012.
- The number of Facility Takeover Frauds against mail order accounts continued to increase, as fraudsters attempted to piggy-back on existing relationships.
- Although the volumes were smaller (and at odds with the increases seen in identity related crimes) there were fewer first party frauds associated with mail order: with fewer fraudulent applications to obtain accounts and fewer attempts to evade payment for goods already ordered.

Fraud Type	2011	2012	% change
Application Fraud	174	93	-46.6%
Facility Takeover Fraud	5,939	12,889	+117.0%
Identity Fraud	38,336	54,480	+42.1%
Misuse of Facility Fraud	2,952	1,278	-56.7%
<b>Total</b>	<b>47,401</b>	<b>68,740</b>	<b>+45.0%</b>

## Mortgages

- There was a 5% increase in the number of frauds against mortgages in 2012 compared with 2011. In contrast to most other products, there was an increase in first party frauds, and a decrease in identity related crimes.
- There were more cases of hiding adverse credit information in Application Frauds than in 2011, and also more cases where someone with a residential mortgage had rented out their property without informing their mortgage provider.

Fraud Type	2011	2012	% change
Application Fraud	2,994	3,142	+4.9%
Facility Takeover Fraud	4	2	-50.0%
Identity Fraud	68	59	-13.2%
Misuse of Facility Fraud	87	123	+41.4%
<b>Total</b>	<b>3,153</b>	<b>3,326</b>	<b>+5.5%</b>

## Other

- Frauds relating to other products decreased substantially in 2012 compared with 2011. This was primarily due to fewer fraudulent attempts to obtain credit files being identified. Given that a fraudulently obtained credit file is a facilitator of further Identity Fraud (and in light of the overall increases in Identity Fraud) this is surprising.
- The number of Application Frauds for 'other' products almost doubled in 2012 compared with 2011. These Application Frauds were predominantly to obtain share dealing accounts.

Fraud Type	2011	2012	% change
Application Fraud	145	286	+97.2%
Facility Takeover Fraud	241	28	-88.4%
Identity Fraud	5,041	2,365	-53.1%
Misuse of Facility Fraud	27	31	+14.8%
<b>Total</b>	<b>5,454</b>	<b>2,710</b>	<b>-50.3%</b>

For further information, please  
contact our Research and  
Communications Team

CIFAS  
6th Floor, Lynton House  
7-12 Tavistock Square  
London  
WC1H 9LT

[press@cifas.org.uk](mailto:press@cifas.org.uk)



The UK's Fraud Prevention Service

CIFAS – The UK's Fraud Prevention Service  
6th Floor, Lynton House  
7-12 Tavistock Square  
London  
WC1H 9LT

[www.cifas.org.uk](http://www.cifas.org.uk)

CIFAS - A company limited by Guarantee. Registered in England and Wales No.2584687 at  
6th Floor, Lynton House, 7-12 Tavistock Square, London WC1H 9LT