FRAUDSCAPE

Depicting the UK's fraud landscape

www.cifas.org.uk | March 2012

CIFAS

The UK's Fraud Prevention Service

In this Report . . .

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 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

CIFAS

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 financial crime. It has 260 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 identified frauds in the fight to prevent further fraud.

The CIFAS National Fraud Database contains records of identified frauds that have been perpetrated 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.

This report examines and assesses the fraud cases recorded by CIFAS Member organisations during 2010 and 2011 to ascertain any key changes over that period. It looks at all frauds identified by the type of fraud committed and the product involved.

Introduction

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 2011. As Members share information on identified and proven frauds only, examination of the frauds recorded to the CIFAS National Fraud Database offers a clear picture of the fraud landscape in the UK.

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, along with definitions of terminology and explanations of the techniques used by fraudsters.

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.

In 2011, fraud rose by 9% compared with the previous year. Following on from the small decrease noted in 2010, therefore, this can only be seen as further proof that the challenge posed to the UK economy is vast and complex. Last year, CIFAS noted that the small decrease recorded in 2010 was 'likely to be the calm before the storm' and this year's edition of *Fraudscape* will examine this. It will also address issues surrounding the security measures taken by organisations and individuals, as well as the question of frauds related to the abuse of identity details.

Other questions are addressed including: Who are the victims of identity related crime? Who are the fraudsters? And where are these frauds concentrated? Finally, there is the ever-present question of 'Why?'. All of these are addressed in *Fraudscape*, looking not only at what happened in 2011, but what this means in the context of preceding years. Only by analysing fraud in this way can organisations and individuals be ready to anticipate, prevent and combat whatever comes next.

1. Executive Summary

In 2011, there were 236,516 frauds recorded by CIFAS Members; a 9% increase from 2010, and the highest number of frauds ever recorded. This means that the decrease seen in 2010 can only be seen as a 'blip' in the context of the overall pattern. Further analysis reveals:

- Identity Fraud and Facility Takeover Fraud account for 58% of all frauds. With 10% and 18% increases from 2010 respectively, the severity of the problem posed by identity related and 'data driven' crime is starkly illustrated.
- Misuse of Facility Fraud increased to nearly 54,000 frauds in 2011 and is the second largest fraud type. As fraud is not merely committed by anonymous third party criminals, 'first party frauds' remain a huge challenge for organisations too.
- The migration to new products identified first in 2009 has continued, with 2011 witnessing the emergence of the payday lender as a target. Some specific products remain key targets for fraud, however.
- The economic climate continued to affect the fraud landscape; acting as a likely driver and/or influence on the types of fraud being committed and, potentially, enabling much fraud to evade detection.

A new currency

The abuse of identity details accounted for more than one in two of all frauds in 2011, meaning that data now has its own intrinsic value. The changing patterns for the products most commonly targeted by identity fraudsters and account hijackers (such as bank accounts or communications products), however, underline the severity of the challenge this poses to organisations and individuals. As organisations become smarter and individuals more vigilant in looking after their own details, fraudsters vary their techniques and change their plans of attack.

Misuse as serious as (identity) abuse

Fraud committed by account holders cannot be seen as unimportant in comparison with the abuse of identity details, with a 13% increase in Misuse of Facility Fraud demonstrating the scale of the problem. Bank accounts, communications products and mail order accounts were most susceptible to misuse with economic hardship being the most obvious driving influence.

Variety – the spice of the fraudster's life

While all products will be vulnerable to fraud, the variation in products attacked, year on year, clearly shows that sectors cannot operate in silos. Notable increases in Identity Fraud against bank accounts, for example, will be offset by an equally visible decrease in Application Frauds. Insurance products, however, remain a target for those attempting simply to lie their way to a product – as do plastic card accounts and communications products. The emergence of the payday lender has also offered the fraudster a new target but (in spite of this) bank accounts, mail order, communications and plastic cards remain the most commonly attacked products – though the number of frauds against mail order products has decreased. As fraudsters find one option closed off to them, so their targets change; meaning that overarching trends seen over a five year period are built on top of an ever-shifting product landscape.

Other factors

These shifts and overall trends are influenced by numerous factors – addressed throughout this report – most notably the economic situation. The drop in Application Fraud slowed in comparison with preceding years and, perhaps, still demonstrates that tighter lending criteria is leading many applications to be rejected at the outset; removing any chance for fraud departments to check them. Does this mean that fraud has gone away, though? The increasingly embedded communications platforms such as smartphones, digital TV services or tablet PCs may also explain the surge in fraud against such products. Facility Takeover Fraud was the only type of fraud against communications products to decrease; demonstrating that while security can increase on accounts, other dangers will always exist.

The uncertainty of the economic climate means that the challenges for the fraud prevention community in the coming year remain unclear. What can be learnt from 2011, though, is that the fraudsters will not stand still. It is, therefore, imperative that everyone involved, including every person who has an identity that could be abused, plays their part to ensure that the chain is as unyielding to criminals as it can be. •

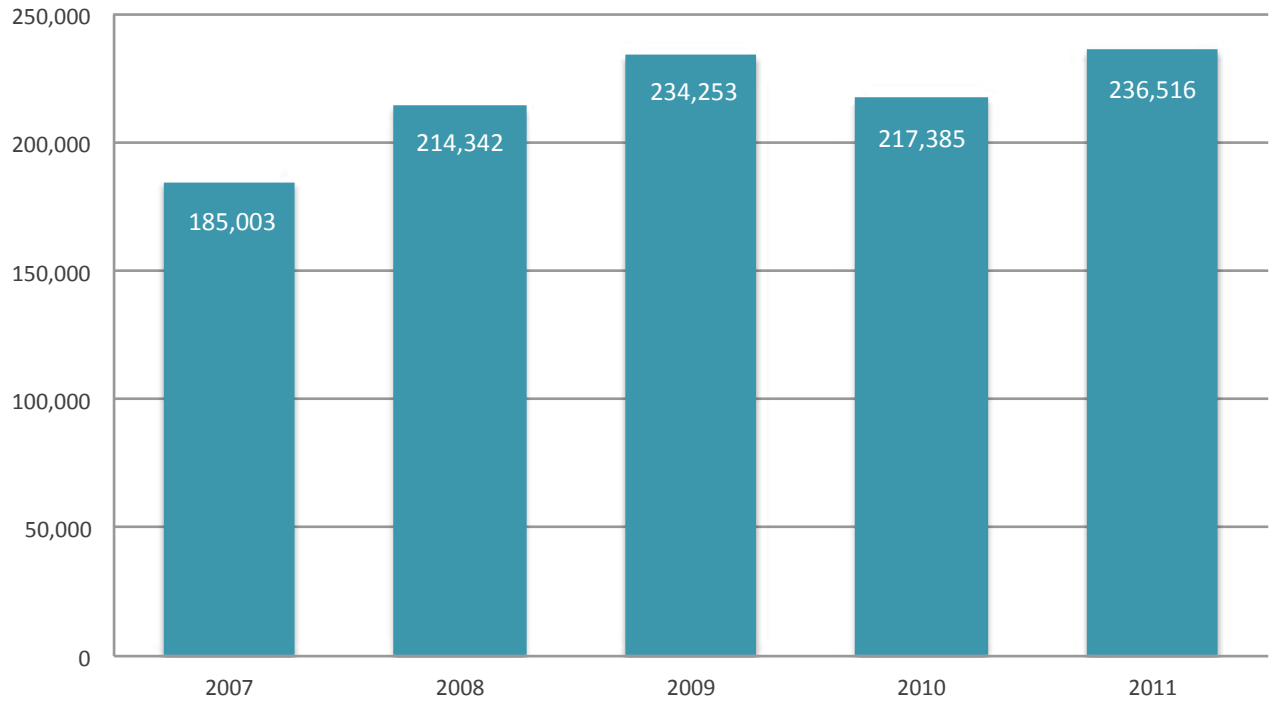
2. CIFAS National Fraud Database

2.1 An overview

A total of 236,516 frauds were identified by CIFAS Members in 2011. This is an increase of 9% compared with 2010. These frauds were filed to the National Fraud Database and the following report sets out an overview of recent trends.

Figure 2.1.1 sets out the number of frauds recorded to the National Fraud Database from 2007 until 2011. The 236,516 frauds recorded in 2011 represent a new high in reported cases, exceeding the 234,253 recorded in 2009. This suggests that the reduction seen in 2010 was an aberration in the otherwise relentless upward trend.

Total Frauds recorded on the National Fraud Database 2007-2011
Figure 2.1.1



2.2 Fraud by Fraud Type

Table 2.2.1 sets out the number of frauds recorded to the National Fraud Database within each fraud type in 2010 and 2011.

Frauds recorded by Fraud Type in 2010-2011
Table 2.2.1

Fraud Type	2010	2011	% change
Identity Fraud	102,672	113,259	+10.3%
Facility Takeover Fraud	21,226	25,070	+18.1%
Misuse of Facility Fraud	47,731	53,996	+13.1%
Application Fraud	44,680	43,263	-3.2%
Asset Conversion	539	532	-1.3%
False Insurance Claims	537	396	-26.3%
Total	**217,385**	**236,516**	**+8.8%**

It can be seen from *Table 2.2.1* that, of the six fraud types recorded to the National Fraud Database, three have increased and these include the two most commonly recorded fraud types: Identity Fraud and Misuse of Facility Fraud. Facility Takeover Fraud saw the greatest proportional increase from the previous year. The number of Application Frauds identified continued to decline, but the rate of decrease has slowed compared with previous years (a 23% decline in 2010 compared with 2009, following a 25% drop in 2009.)

Figure 2.2.1 (page 7) shows the percentage of all frauds recorded in 2011, broken down by fraud type. From this figure it can be seen that the two identity related fraud types, Identity Fraud and Facility Takeover Fraud, accounted for well over half (58%) of all the frauds recorded to the National Fraud Database in 2011.

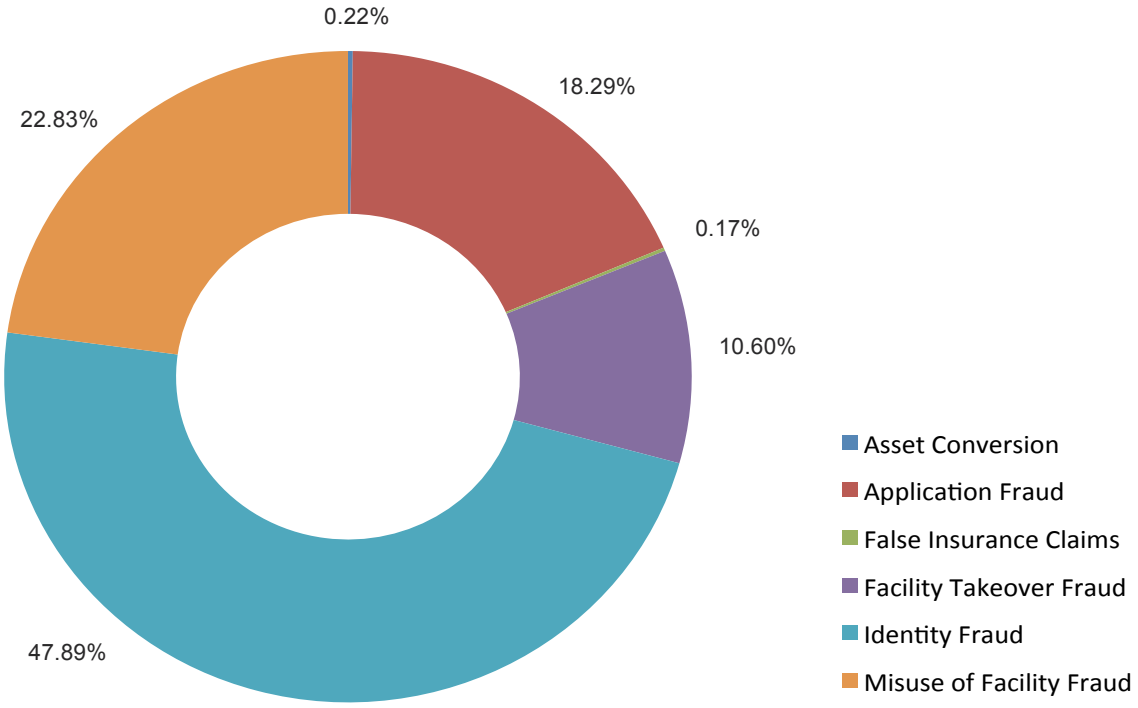
The prevalence of identity related crime is to some extent unsurprising, given the well documented proliferation of the likes of phishing emails and websites, designed to part large numbers of unsuspecting members of the public from their valuable personal information. This information can then be used by fraudsters to apply for new products or services in the name of their victims, or to gain access to their accounts and use them for their own ends.

The stagnation in the number of Application Frauds recorded reflects the equilibrium that has been established between two conflicting, but economy driven, factors. On one hand, there are more and more people in the UK who are finding times financially difficult. Some of these people will see submitting fraudulent applications for goods and services as a way of easing that pressure (albeit temporarily). Counterbalancing this increase in those who are willing to lie to gain credit and services, there is still a risk averse culture in many organisations which translates into high credit score thresholds. This means that an unknown number of fraudulent applications are failing to pass that scoring threshold and are being declined; therefore never reaching those organisations' fraud teams.

The effects of these financially challenging times can be seen elsewhere. Hardship can lead to individuals robbing Peter to pay Paul – perpetrating fraud against one organisation in order to keep up with repayments to another. It can also lead to people becoming more vulnerable to organised fraudsters; be it through falling prey to employment scams and being tricked into laundering money, colluding with the fraudsters for financial gain, or being scammed into parting with what little they have left in the belief that this will result in a big payout further down the line. •

Frauds recorded by Fraud Type in 2011

Figure 2.2.1



CIFAS
The UK's Fraud Prevention Service

Protective Registration

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 for more information about CIFAS Protective Registration.

tracesmart®

The **intelligent** way to fight fraud

TraceIQ is an unparalleled source of consumer data, providing access to a wealth of information including electoral rolls, CCJ records, and millions of consented landline and mobile phone numbers.

Allowing you to obtain a clear picture of the people you're dealing with, the web based investigation tool provides key personal characteristics which will help you to:

- Identify fraudulent applications/claims
- Evaluate the risk associated with an individual
- Investigate possible fraud
- Screen potential/existing employees

Find out how TraceIQ will help you prevent, detect and investigate fraud - contact us today and claim your free trial*.

*subject to terms and conditions

T: 029 2067 8555 **E:** freetrial@traceiq.co.uk **www.traceiq.co.uk**

3. Identity Related Crime

This section examines the two fraud types that centre upon the personal data and details of either an identifiable fraud victim or a completely fictitious individual. This reflects the fact that an 'identity' is not necessarily a simple definable concept.

A person's identity can be composed of a tapestry of details including (but not limited to): passport number, address, names, date of birth, financial footprint, telephone numbers, email addresses and passwords and more.

The combination of these factors, of course, can differ depending upon the person or organisation that is looking to verify an identity.

Identity related crimes, therefore, are those frauds where the fraudster has created, hijacked or obtained a set of these identity related details and uses them to obtain or access accounts, products and services using the details of another.

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.

Table 3.1.1 shows the number of cases of Identity Fraud recorded in 2010 and 2011. This shows that those products that are historically targeted by identity fraudsters have continued to experience an increase in the number of cases recorded (with the sole exception of mail order accounts).

Identity Fraud cases by Product 2010-2011
Table 3.1.1

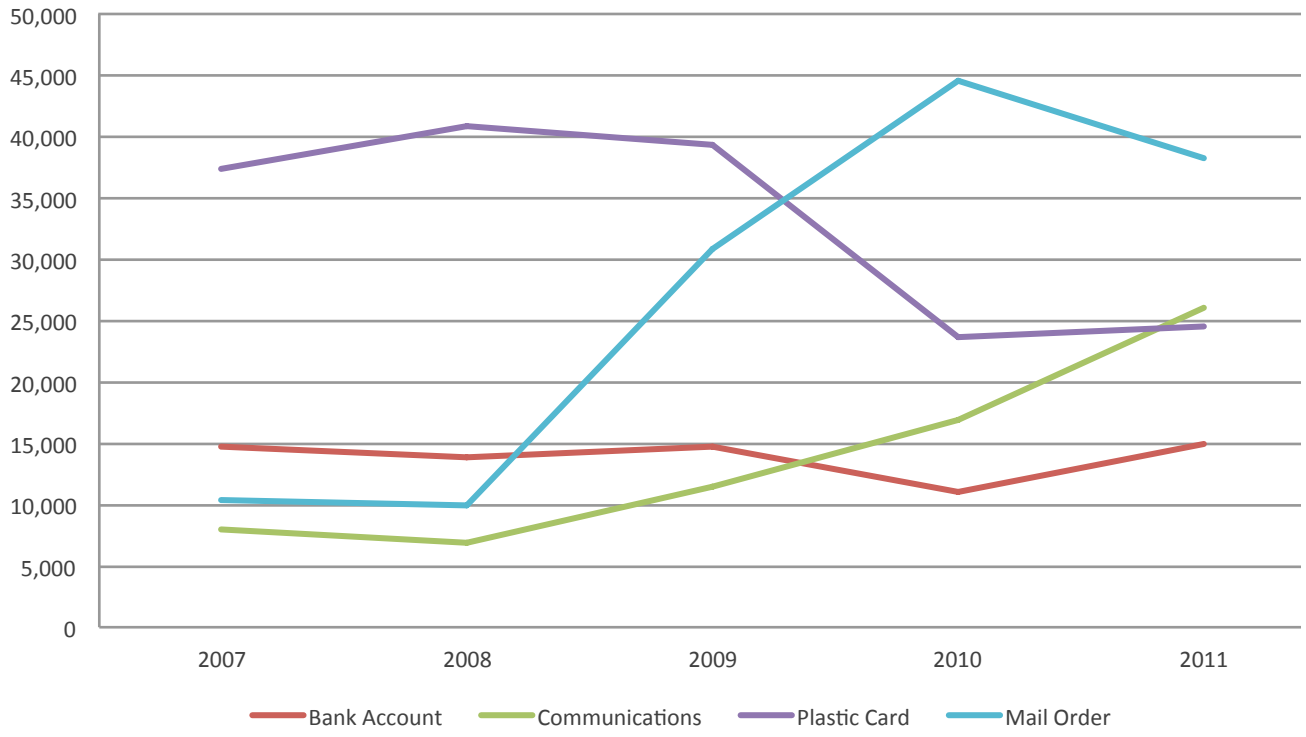
Product	2010	2011	% change
All-in-One	271	216	-20.3%
Asset Finance	472	325	-31.1%
Bank Account	11,030	14,873	+34.8%
Communications	16,821	25,996	+54.5%
Plastic Card	23,560	24,582	+4.3%
Insurance	108	27	-75.0%
Loan	2,404	3,795	+57.9%
Mail Order	44,577	38,336	-14.0%
Mortgage	66	68	+3.0%
Other	3,363	5,041	+49.9%
Total	**102,672**	**113,259**	**+10.3%**

Favourite things?

Figure 3.1.1 (page 10) focuses on the four most commonly targeted product types (namely bank accounts, communications products, plastic cards and mail order accounts). This shows that the increase in Identity Fraud on plastic card accounts seen in 2011 is in contrast to the declines seen in 2009 and 2010. Mirroring this, during 2011 there was a decline in Identity Fraud against mail order products following two years of rapid growth. This is attributable to a number of factors but, most notably, the decline in Identity Fraud against plastic card accounts in 2009 and 2010 was directly related to risk averse lending practices. A number of attempted Identity Frauds will have failed because the victims of this fraud (those whose identity >

Identity Fraud cases recorded by Product 2007-2011

Figure 3.1.1



has been hijacked) were actually not a sufficiently good credit risk to pass a lender's credit scoring thresholds. This will have led to a number of frauds going unrecorded, and it will also have resulted in identity fraudsters transferring their attention to products that are not subject to the same level of credit assessment. This then, partially explains the explosion in frauds recorded against the likes of mail order from 2008 to 2010.

The rewards that the fraudster obtains for a successful fraud against a mail order company will be smaller than those which they would obtain if they could fraudulently acquire a credit card, but their chances of success are likely to be higher. This demonstrates that fraudsters are prepared to change their 'business model' to accommodate changing circumstances, and such adaptability can be seen once again in 2011. As controls tightened around mail order, and lending conditions became more stable, fraudsters moved away slightly from attacking mail order at application stage, preferring to return to targeting plastic cards. The personal data that had been harvested, however, allowed them to try to take over existing mail order accounts (evidenced by an increase of over 40% in the number of Facility Takeover Frauds against mail order products).

The steady increase in the number of cases of Identity Fraud against communications products (almost exclusively mobile phones) gathered pace in 2011. This increase can be attributed to the emergence of the smart phone as the 'must-have' gadget; as it is both valuable and aspirational, and more difficult to obtain than a standard mobile phone contract due to more stringent verification and vetting procedures. Some identity fraudsters feel that there is a greater chance of getting the phone that they want if they use someone else's identity, even that of a family member. Other more organised fraudsters attempt to obtain these devices *en masse* in order to sell them on.

>

Identity Fraud Facilitator Definitions

There are various ways in which identity related crimes are perpetrated; ranging from those facilitated physically and those that occur digitally ('data driven crime'). Notable examples of the methods used by fraudsters to obtain identity details include the following:

Bin Raiding

Bin Raiding is, perhaps, the most traditional method used by organised fraudsters, and involves targeting the victims' bins – looking for envelopes, statements and any documentation that might contain details such as account numbers, personal details (e.g. names, addresses, postcodes, dates of birth etc) and information that gives a fuller picture of the intended victim.

Scams

Scams are confidence tricks, frequently designed to get people to part with money and/or financial and personal details. Notable examples include email charity fundraising requests following natural disasters, requests for help from a known contact who has had their email account hacked, and unsolicited 'prize draw' or 'lottery' communications. Frequently, scams take the form of phishing emails and fake websites.

Phishing

Phishing attacks involve the mass distribution of emails which appear to originate from legitimate sources – including financial institutions, charities or even Government departments. Victims are often directed to fake websites and are tricked into revealing information that gives an attacker access to the victim's bank account, payment card details or personal information.

Mail Accessing

Financial and personal details can often be accessed by intercepting or redirecting a victim's post – but fraudsters are also known to target multiple occupancy properties (e.g. student accommodation or shared dwellings) in order to steal mail and access details.

Hacking

Criminals are known to employ hacking as a means of attacking the computer systems of organisations in order to obtain the details of customers from an organisation's database(s).

Social Engineering

Social Engineering is, basically, the manipulation of situations and people into divulging confidential information, especially personal details. Many social engineering techniques take the form of a variation on a scam that can take either take place on a face to face basis or in the digital domain. Notable examples will include the use of social networking sites – often through forums and discussions leading to friend requests from persons not known to the intended victim. This is usually done in order to capture information from a person's profile or solicit requests for financial assistance. Fake surveys on the street or fraudsters posing as charity collectors are real world equivalents.

Malware

Malware is malicious software that infects a victim's computer. It can capture private information stored on an individual's computer and send it to fraudsters, who can use that information to impersonate the individual and commit fraud. Specific types of malware which aid fraudsters in obtaining information include:

- Spyware (a type of malware that collects little bits of information such as websites visited, passwords etc without the user's knowledge), and
- Trojans (a programme that may appear to be legitimate but actually acts maliciously – often giving fraudsters remote access to your computer, thus enabling the fraudster to record any sensitive details and documents stored on your computer).

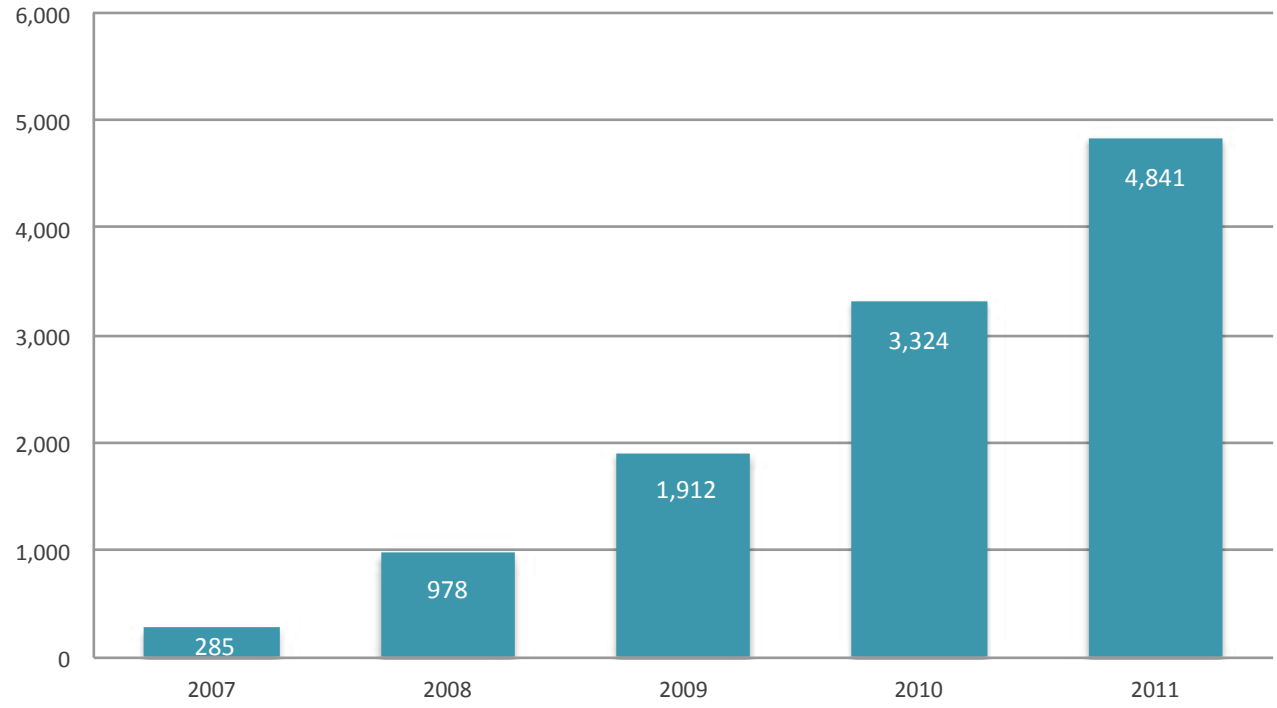
Data Data Data

These more organised attacks on telecommunications companies will be facilitated by criminals who obtain large quantities of compromised identity data. This data could be compromised through a number of channels, including being phished directly from the victim, malware attacks, being sold on by corrupt members of staff or being hacked directly from an organisation's database. This availability of personal data to the fraudsters will not only be fuelling attacks against telecommunications companies, but also against the likes of mail order companies and those that offer low value loans (e.g. payday lenders). These companies offer products where the value of a single fraud will be comparatively low, and consequently the number of checks made on an application may be fewer. In addition, the information requirements of the application process are generally more streamlined. Moreover, for a number of low value loans, the target market is those who are in a degree of financial difficulty and therefore their applications are far less likely to fail credit scoring because the thresholds are not so high.

It is not just personal details like name, birth date and address that are being compromised by the criminals – email addresses and passwords are also being obtained. The availability of this kind of data to fraudsters is one of the major drivers behind the increase in Facility Takeover Fraud (see pages 15 and 16).

Figure 3.1.2 illustrates the relentless increase since 2007 in the number of attempts by fraudsters to obtain someone else's credit file. This crime is, in itself, Identity Fraud; but it is also an enabler of further Identity Fraud. By amassing more information on their victim, which they can find from the credit file (as the credit file effectively operates as an audit trail for a person's financial and identity details) the fraudster is able to apply for products and services of a higher value and, consequently, applications are scrutinised with more rigour. This shows that although fraudsters have access to large quantities of personal data, and use this on an industrial scale against low value targets, there are those who are prepared to develop the identities they have compromised in order to target a bigger pay-off. •

Number of fraudulent attempts to obtain someone else's credit file
Figure 3.1.2



3.2 The ways and means of Identity Fraud

The most common way of perpetrating Identity Fraud during 2011 continued to be current address fraud. This form of Identity Fraud involves using the genuine current address of the victim (so, to the company receiving the application, it looks 'right') but it presents additional challenges to the fraudster; in that they then have to find ways of ensuring that the victim does not receive any correspondence relating to the fraud through the post. They can do this in a number of ways: by having the person's mail redirected (impersonating the victims again in order to set this up – another example of Identity Fraud to facilitate further Identity Fraud), or by intercepting the mail in another way, such as meeting the postman on the doorstep and pretending to live at the address. It must also be remembered that the fraudster, as well as the victim, may actually live at the address! In an age where fraudsters are known to hijack the identities of potentially hundreds of people at a time, it should not be forgotten that there are still instances of people impersonating family members and housemates; knowing that their victim will not, ultimately, be held financially liable. Finally, as more services go entirely online (paperless accounts for instance) the less the fraudster needs to worry about how to intercept physical post. The online environment is convenient for customers and more economical for business, but it also makes life easier for fraudsters.

Current address fraud accounted for almost 65% of all Identity Frauds attempted in 2011, which was slightly down from the previous year (68%). In its place, though, there has been a slight increase in the proportion of cases involving an entirely false identity. This sort of fraud was up to just over 10% of all Identity Frauds. Such false identities were most commonly used against communications companies, where they accounted for nearly a quarter of Identity Fraud cases. The likelihood is that these frauds were carried out by people who were not 'professional' fraudsters, but were looking to obtain an aspirational device, and thought that using a false name would allow them to obtain that device without then being responsible for the monthly bills.

A curious development in 2011 was that for some products (plastic cards, loans and mortgages) there was an increase in the proportion of previous address fraud cases. This type of fraud, where the fraudster essentially claims that their victim has just moved house (so the address given as the previous address on the application is actually the victim's real current address) had been decreasing in previous years; >

Definitions

Previous Address Fraud

The fraudster applies in the name of an innocent victim, gives an address accessible to the fraudster but unrelated to the victim as the current address on the application. The fraudster, then, gives the address where the victim is living as the previous address, claiming that he or she (as the victim) has just moved. This explains why the victim's data is still registered at the previous address on the application and means that any documentation/goods are sent to an address unconnected to the victim but to which the fraudster has access.

Current Address Fraud

The fraudster applies in the name of an innocent victim and uses the address where the victim is living as the current address on the application. This means that things look 'normal' to the lender (e.g. the victim is on the electoral roll at that address and his or her payment performance information is all located at that address too). The fraudster is likely to need to gain access to the victim's mail or premises to intercept the relevant documentation/goods.

Previous Occupier Fraud

Typically, this is carried out by opportunist fraudsters who have moved out into their victim's previous address. It occurs when the fraudster applies in the name of an innocent victim who has recently moved. The fraudster may well not know where the victim has moved to, so uses the victim's previous address as the current address on the application, and hopes the victim has not yet changed his or her address on accounts and the electoral roll.

False Identity

The fraudster applies using an entirely fictitious identity.

as fraudsters learned that organisations can more easily verify an applicant's address history. The re-emergence in 2011, therefore, is a little surprising.

Theories abound regarding the reasons behind this increase. It could be that there is a whole new 'generation' of identity fraudsters, making a high number of applications for products which generate purely cash related gains, like loans and credit cards. In doing so, as 'beginners' they may lack the understanding of the checks that organisations can carry out to verify this information. These 'new' fraudsters too may not be able or willing to make the extra effort required to carry out the more difficult current address fraud.

Another possibility is that some of the fraudsters carrying out previous address fraud are actually facilitating it with an earlier fraud. The most obvious link would be that some Facility Takeover Frauds (specifically those where the fraudster has already carried out an unauthorised address change) have been perpetrated to give credence to the assertion that the 'applicant' has just moved. Put another way, the fraudster uses one type of fraud to facilitate and appear to 'validate' another type of fraud. While all of these theories have been put forward by members of the fraud prevention community in an effort to explain this apparently anomalous increase, the reality is that only conjecture can be offered. The only constant truth about Identity Fraud is that the party named on the application was not the person actually submitting it and attempting fraud. The identity of the fraudsters, their motivations and experience remain unknown. The collaborative efforts of businesses, public sector bodies, organisations like CIFAS and law enforcement are working towards ensuring that any gaps in our knowledge are filled. Obtaining a more detailed understanding of the *nature* of fraud enables more effective apprehension and prosecution of these offenders, as well as ensuring that the most effective countermeasures can be put in place to prevent fraud at source.

Further information about the victims of identity related crime can be found in chapter 3.5. •

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.

Table 3.3.1 shows that the products that are most affected by Facility Takeover Frauds all saw an increase in 2011, with the exception of communications products. This is at odds with the previous three years, as can be seen from *Figure 3.3.1* below.

The decline in the takeover of communications accounts is surprising not only in that it is at odds with the general trend in Facility Takeovers, but that taking over a mobile phone account can also be a facilitator of the takeover of other accounts – such as bank accounts – which increased. Changes to online bank accounts are often confirmed through the use of text messaging systems now too; so taking over a mobile phone account can help to hide the takeover from >

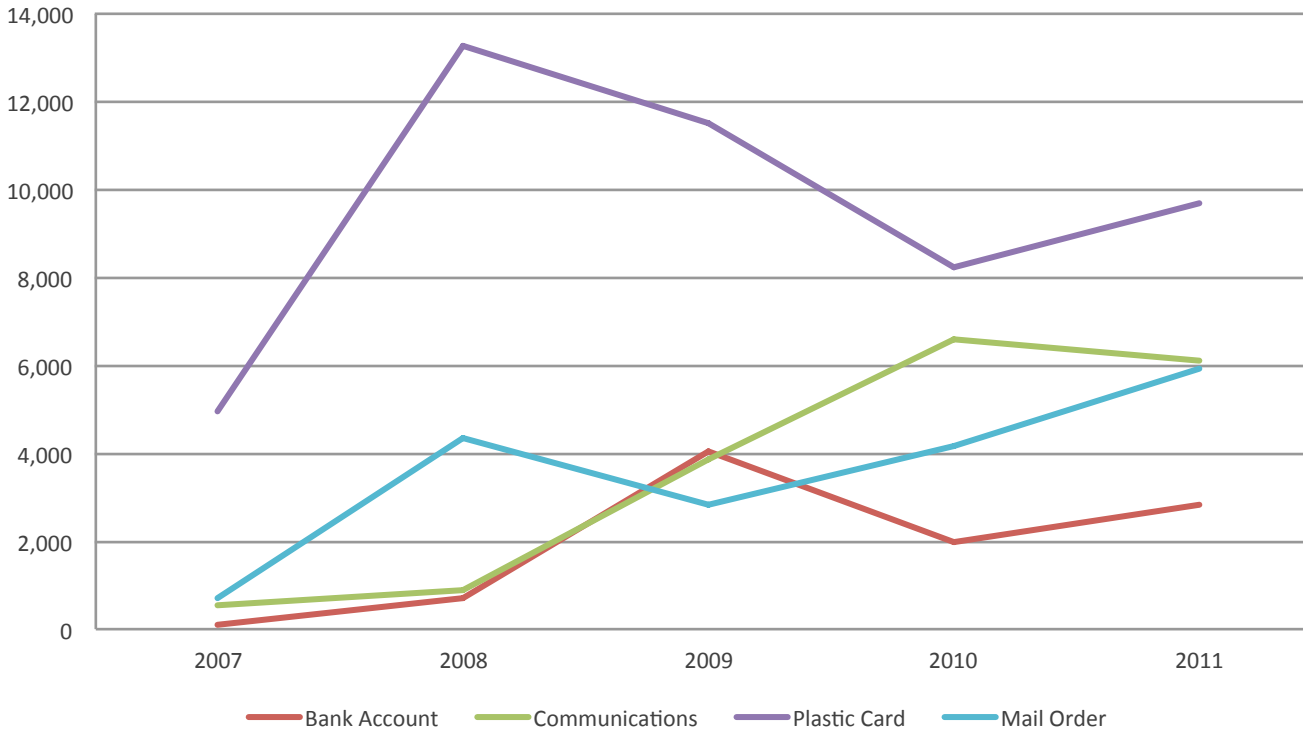
Facility Takeover Frauds recorded by Product 2010-2011

Table 3.3.1

Product Type	2010	2011	% change
All-in-One	255	209	-18.0%
Bank Account	1,974	2,814	+42.6%
Communications	6,590	6,136	-6.9%
Plastic Card	8,209	9,719	+18.4%
Loan	13	8	-38.5%
Mail Order	4,168	5,939	+42.5%
Mortgage	0	4	-
Other	17	241	+1317.6%
Total	**21,226**	**25,070**	**+18.1%**

Facility Takeover Fraud cases recorded by Product 2007-2011

Figure 3.3.1



the genuine account holder. Nonetheless, takeover of communications accounts is down – which may go hand in hand with the overall increase in Identity Frauds being committed against these products.

The most commonly hijacked accounts, however, are plastic card accounts; and 2011 saw an increase in the number of these cases for the first time in three years. Interestingly, more of the takeover of plastic card accounts was in order to make payments, rather than what had previously been the most common reason for taking over card accounts – to change the address and take receipt of new cards. What remains to be seen is whether this continues over the coming years, or whether this was a 'blip': a temporary tactic used by fraudsters.

The increase in the takeover of mail order accounts is perhaps unsurprising, as the decline in the number of Identity Frauds perpetrated against mail order accounts indicates that the security around account opening has been improved. Those fraudsters targeting mail order organisations, therefore, will have been forced to go down other avenues; in this case, taking over existing accounts and issuing unauthorised dispatch of goods instructions. The challenge will always be the same for all organisations; if the 'customer' answers all of the security questions and passes the security check, what can the organisation do? The need to balance customer service with fraud prevention remains as difficult as ever.

Within the increase in the number of takeovers of bank accounts, the most common reason for recording the fraud continued to be the unauthorised electronic payment instruction. This accounted, however, for only 37% of cases in 2011, down from 51% in 2010. This decrease was offset somewhat by a proportionate increase in the number of unauthorised address changes (up to 32%), which (as suggested earlier in this report) supports the idea that such frauds are being perpetrated in order to enable further frauds (most notably previous address Identity Fraud). There was also an increase in the use of intercepted or stolen cards (up to 12%). •

3.4 Channels used to perpetrate identity related crimes

There is evidence to suggest that the personal information being compromised by those intending to commit identity related crimes increasingly contains user names and passwords for online accounts, as Facility Takeover Frauds take place over the internet. Given the high level of security that surrounds many accounts, the simplest explanation for this is that the necessary information is known to the fraudster. There has, therefore, been a proportionate decrease in the number of takeovers that have happened over the phone, which would indicate that where fraudsters were previously able to talk their way round the member of staff to gain access to an account, they are now finding this route closed off to them. This underlines the vital necessity for account holders to review their settings, computer security, passwords etc regularly in order to counteract the threat from hi-tech fraudsters. >

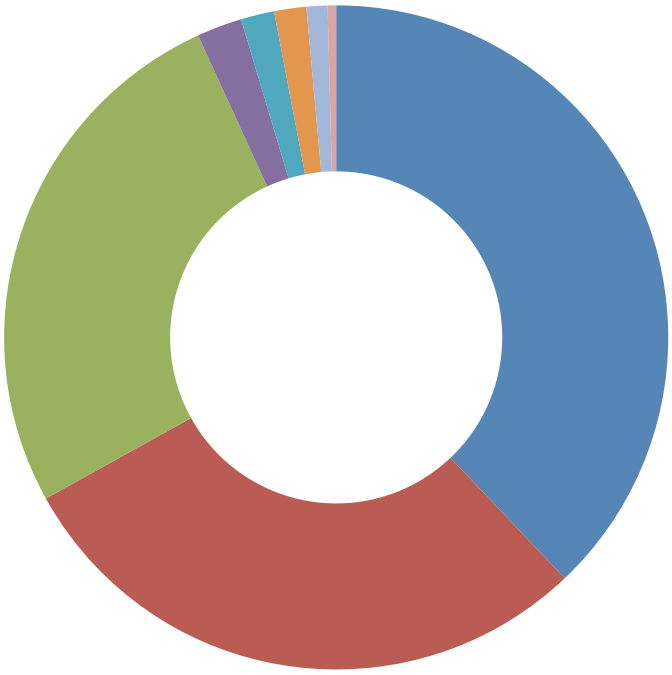
Proportion of Facility Takeover Fraud cases by Channel

Table 3.4.1

Channel	2010	2011
Internet	37.9%	62.4%
Telephone	29.0%	19.1%
Combination	26.2%	14.4%
Face to Face	2.2%	1.4%
Retailer	1.6%	0.7%
Dealer	1.6%	1.0%
Mail	1.0%	0.8%
Other	0.5%	0.2%

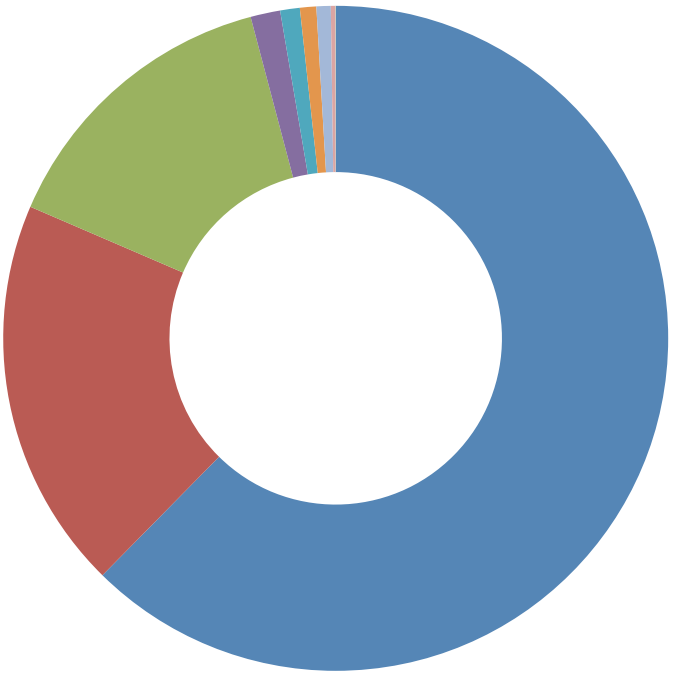
Facility Takeover Fraud Channels in 2010

Figure 3.4.1



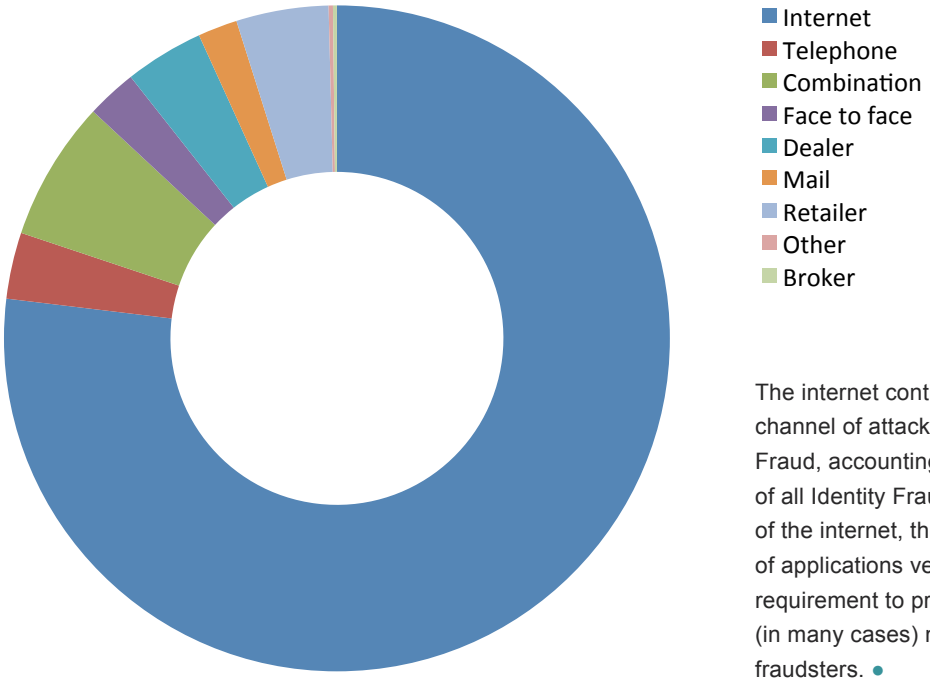
Facility Takeover Fraud Channels in 2011

Figure 3.4.2



Identity Fraud Channels in 2010

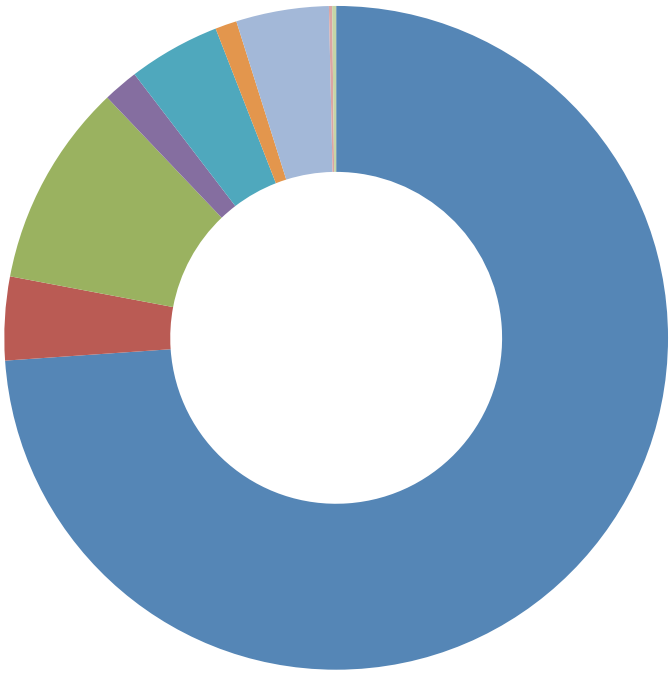
Figure 3.4.3



The internet continues to be the favourite channel of attack for those carrying out Identity Fraud, accounting for around three quarters of all Identity Fraud cases. The anonymity of the internet, the ability to make a number of applications very quickly and the lack of a requirement to produce identity documentation (in many cases) make it the ideal channel for fraudsters.

Identity Fraud Channels in 2011

Figure 3.4.4



Proportion of Identity Fraud cases by Channel

Table 3.4.2

Channel	2010	2011
Internet	76.9%	73.9%
Combination	6.8%	9.9%
Retailer	4.5%	4.5%
Dealer	3.8%	4.5%
Telephone	3.2%	4.1%
Face to Face	2.4%	1.7%
Mail	1.9%	1.1%
Other	0.5%	0.3%

3.5 The victims of identity related crime

The total recorded number of identifiable Victims of Identity Fraud and Facility Takeover are presented in *Table 3.5.1*.

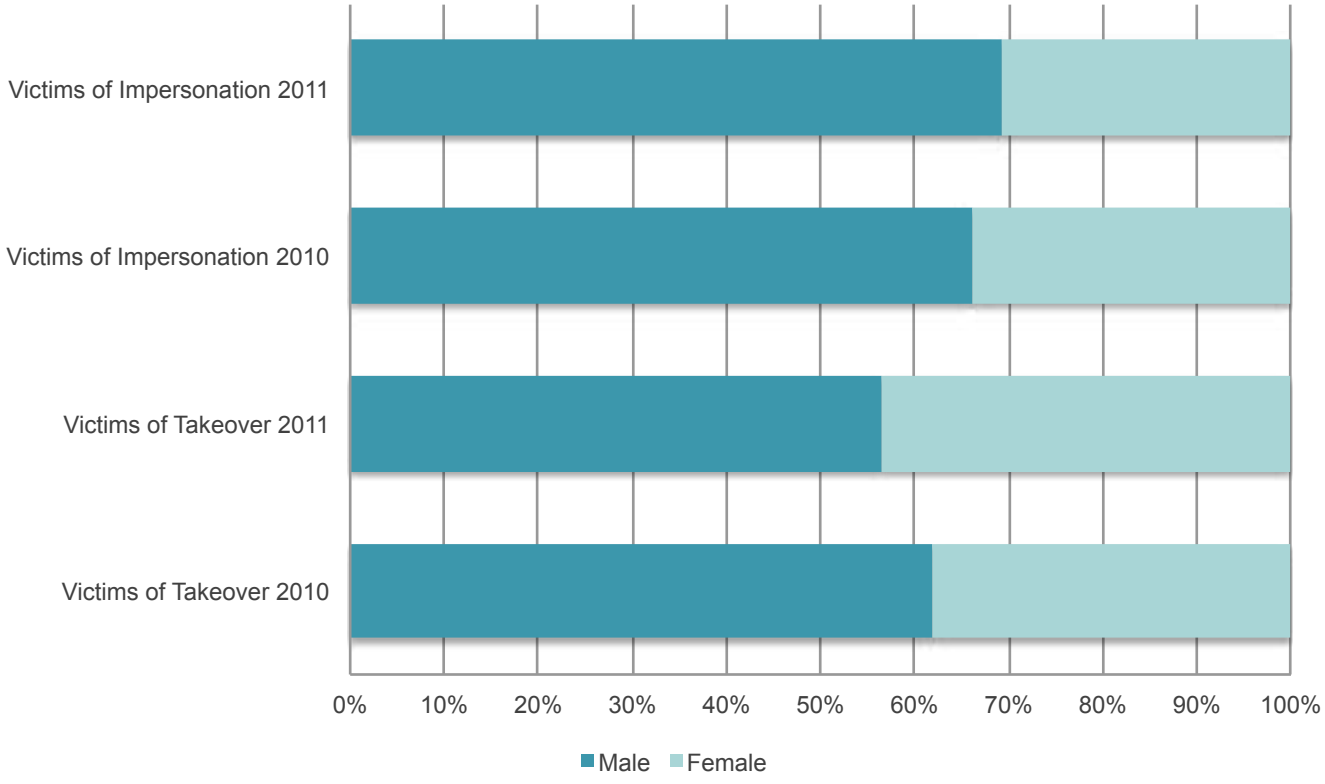
The gender of the Victims of Impersonation and Victims of Takeover is recorded in almost all cases – between 96% and 99% of the time depending on the type of fraud and the year. Instances where these details were not captured are usually explained by a gender non-specific name and the organisation not recording male or female options when asking for customer details. The gender split for both Victims of Impersonation and Takeover in 2010 and 2011 can be seen in *Figure 3.5.1*

Number of Victims of Impersonation and Takeover
Table 3.5.1

	2010	2011	% change
Victims of Impersonation	89,470	96,611	+8.0%
Victims of Takeover	21,322	25,250	+18.4%

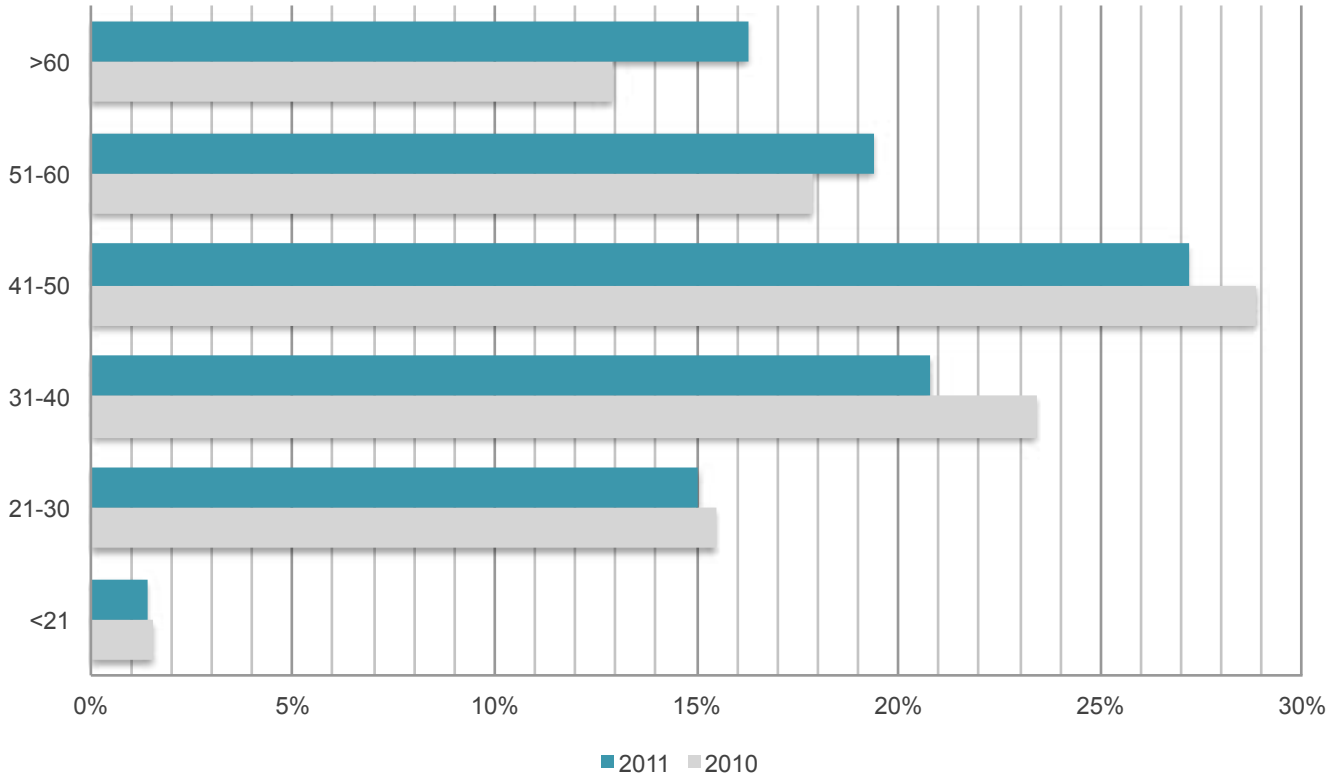
This shows that men continue to be victimised more than women, particularly in cases of impersonation. While the proportion of women who are Victims of Takeover continues to increase, curiously the proportion of women impersonated has decreased, albeit only slightly. >

Gender split of Victims of Impersonation and Takeover
Figure 3.5.1



Age distribution of Victims of Takeover

Figure 3.5.2



Figures 3.5.2 (above) and *3.5.3 (page 21)* show the age distributions of Victims of Takeover and Impersonation in 2010 and 2011. It can be seen from these charts that although there is a higher proportion of Victims of Impersonation in the older age categories than Victims of Takeover, the proportion of older Victims of Takeover has increased in 2011. This could indicate that, with some fraudsters, some screening of obtained data sets takes place, so that the fraudster can target certain demographics that they believe will be more profitable. It remains to be seen, however, whether this trend continues over the coming years.

Equally, this might demonstrate that the number of older people whose details have been phished by online fraudsters has increased, and therefore the number of potential victims within that age bracket has increased. The proportion of Victims of Impersonation in the 40-60 age bracket has increased, although the proportion over 60 has decreased.

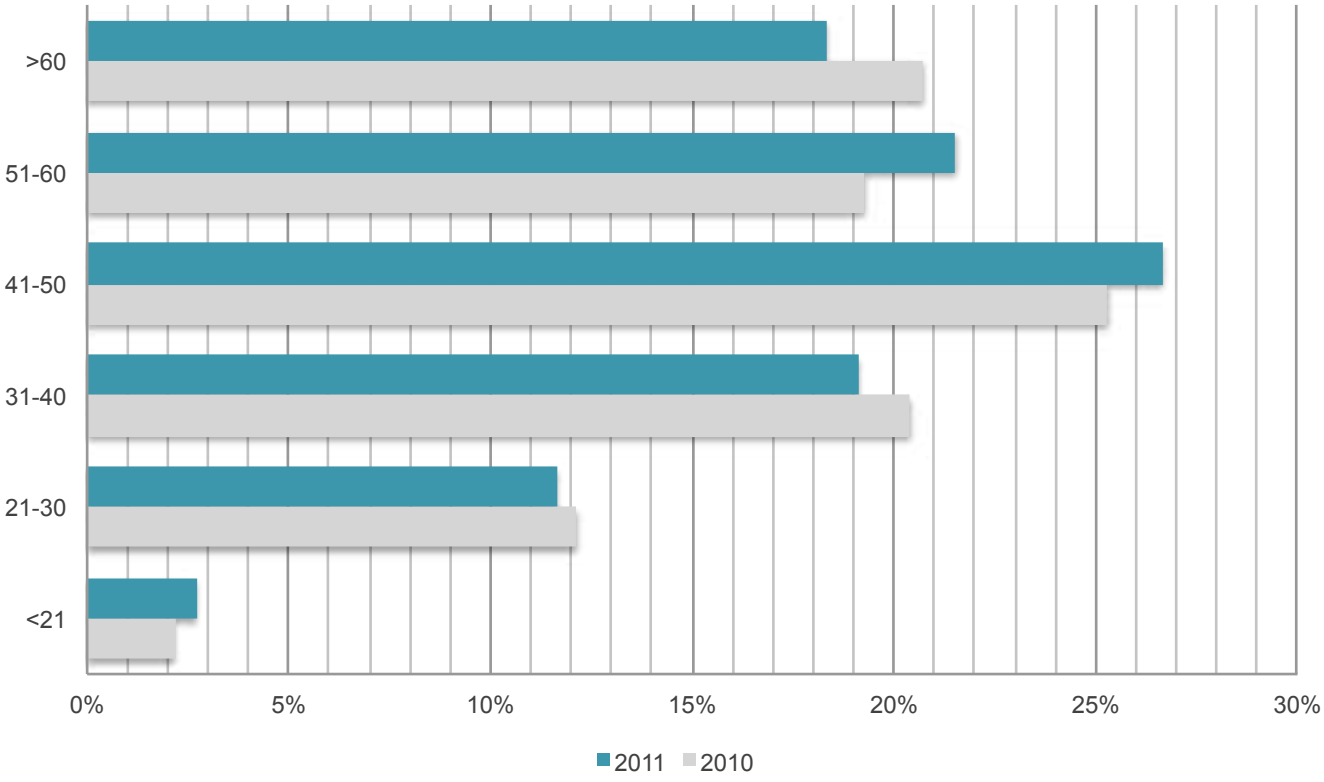
These figures seem to suggest that although a large number of impersonations will be as a result of personal data being compromised in bulk (meaning that victimisation is, to a certain extent, entirely random and arbitrary) some perpetrators of the impersonations continue to be more targeted in their approach; targeting those whom they feel are likely to be 'profitable' individuals. These are still, statistically, more likely to be mature men. In many cases, of course, (see *Figure 3.1.2* - page 12), their financial stability is likely to have been confirmed through a fraudulently obtained credit file.

Finally, and perhaps more cynically, there is an acknowledgement that some individuals have taken to claiming to be a Victim of Impersonation or Takeover – in order not to be held liable for funds lost. In such cases, of course, it becomes the responsibility of the organisation to disprove such claims – a costly and potentially fraught scenario.

While these attempts can normally be identified and confirmed – and would result, therefore, in the purported 'victim' being recorded as a first party fraud – it has to be considered that, if successful, that individual will be recorded as a victim of fraud when they were not. This danger is one that organisations have been coming to terms with and will remain a challenge over the coming years. •

Age distribution of Victims of Impersonation

Figure 3.5.3



3.6 The location of identity crime

The following pages contain a range of UK maps which illustrate where Victims of Impersonation (*map A*) and Victims of Takeover (*map B*) are located. Both have been population adjusted, with all boundaries and populations based upon local authority areas. 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.

Proving the point

Map A shows the locations of Victims of Impersonation in 2011, with *Map B* showing the location of Victims of Takeover. Both comprehensively demonstrate that, even when population is taken into account, there are more instances of victimisation in the more heavily populated areas. This is most obviously true in London, but can also be seen clearly in the Midlands and the North West. In addition, we clearly see that victimisation is high throughout the London Authority areas.

There are some interesting differences, however, when looking at the two maps together. First, the areas with the highest number of victims per thousand people are far greater, in their geographical reach, in London and the South Eastern area for Identity Fraud than they are for Facility Takeover Fraud. Second, the Orkney and Shetland Islands had a greater relative preponderance of Victims of Takeover than Victims of Impersonation. Finally, what particular circumstances or vulnerabilities were exploited by fraudsters in order to take over the accounts of people based in Daventry (near Birmingham) and Monmouthshire (South Wales) as opposed to impersonating them?

While there are interesting divergences between these two maps, they are not telling us *everything* that we might want to know.

Further insights into population and location

Map C shows the same Local Authority areas but reveals the corresponding proportions of individuals who were recorded by CIFAS Members in 2011 as being either Victims of Impersonation or Takeover: the distribution ranging between 100% Victims of Impersonation and 100% Victims of Takeover. Areas where the instances of impersonation are greater are in green, and areas where instances of takeover are greater are in purple.

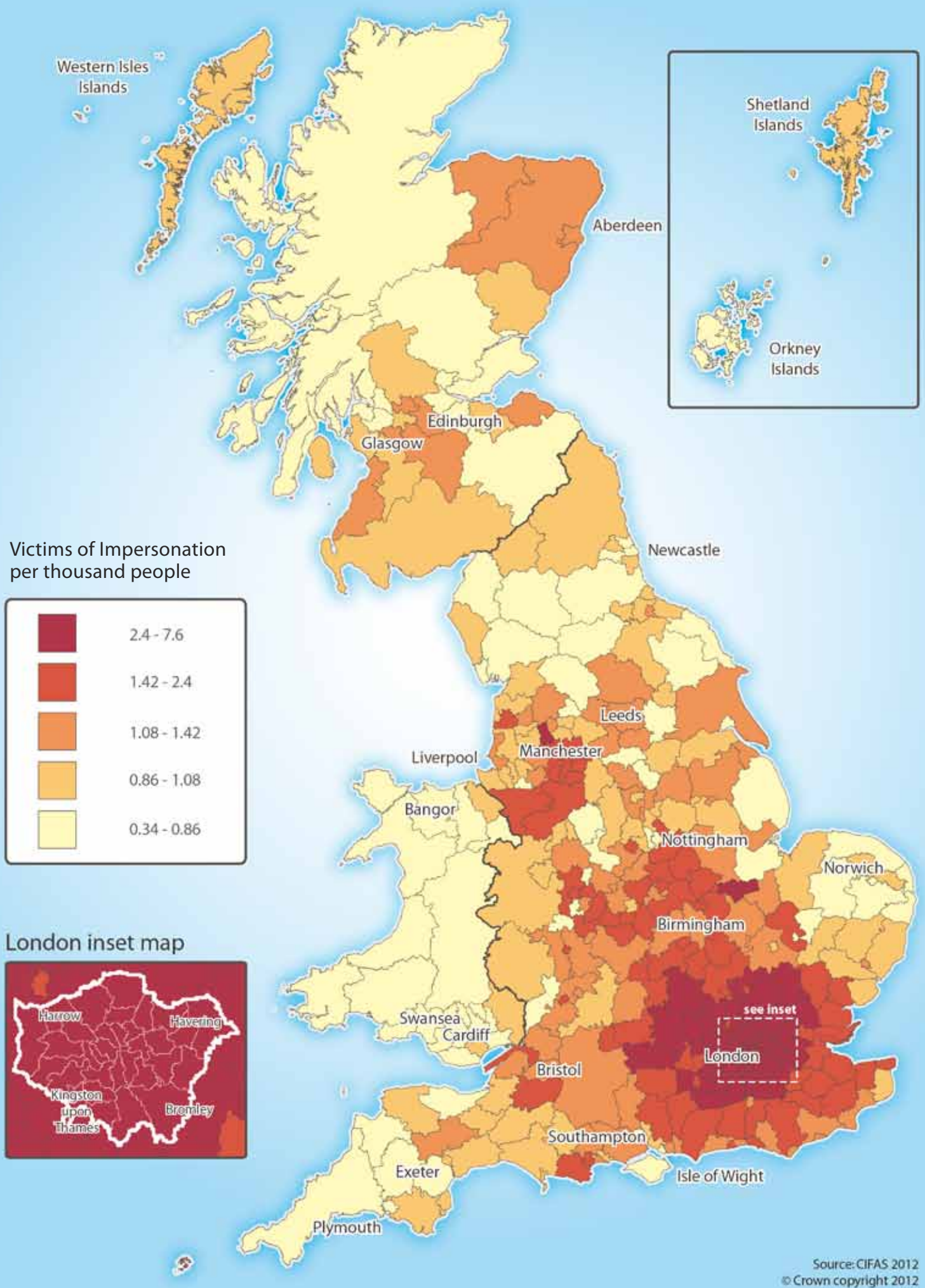
What *map C* shows is that Victims of Impersonation are *most concentrated* in these urban areas. The high levels of Identity Fraud are most prominent in London and its commuter belt, the Midlands and the North West area. Victims of Takeover, however, are more widely distributed across the country; with areas as spread out as the Western, Orkney and Shetland Isles, central Wales, the Cumbrian coast, mid Norfolk and north Devon all revealing that there is a greater proportion of Victims of Takeover than Victims of Impersonation in less populated areas.

This reiterates the differences in the nature of the individuals targeted (see section 3.5). Victims of Impersonation are, to a certain extent, targeted more for *who they are* or *where they live* (i.e. the victim is likely to be approved for credit or located somewhere convenient to the fraudster). While such discrimination is less marked than it was a few years ago, address continues to be an important factor. In cases of Facility Takeover, however, all that is needed is access to the account. As cybercrime plays such a key role for the fraudster – through phishing, malware etc – the need to intercept post or goods is not so important when taking over an account.

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

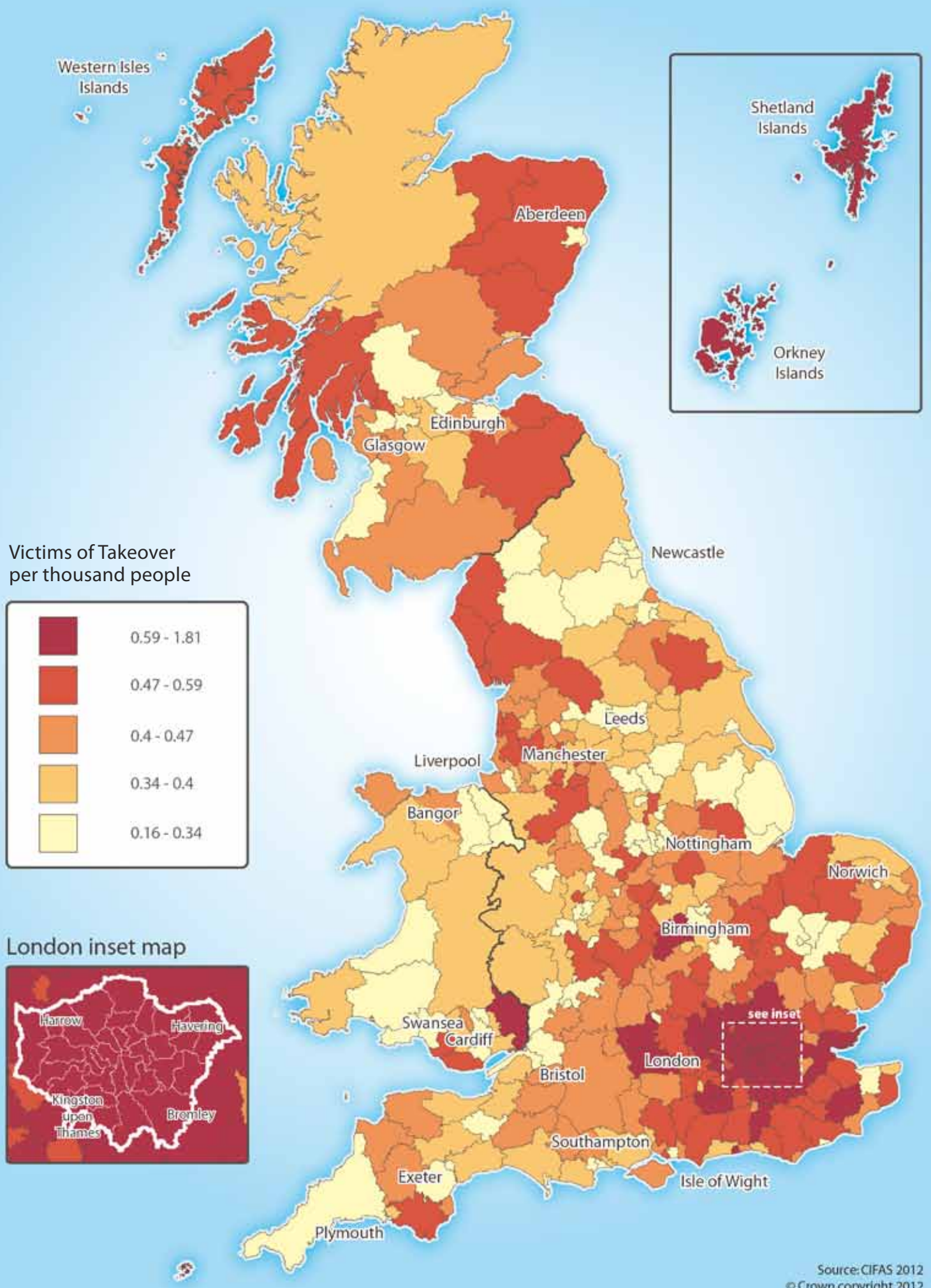
Ordnance Survey

A: Victims of Impersonation in 2011 per thousand people by local authority area



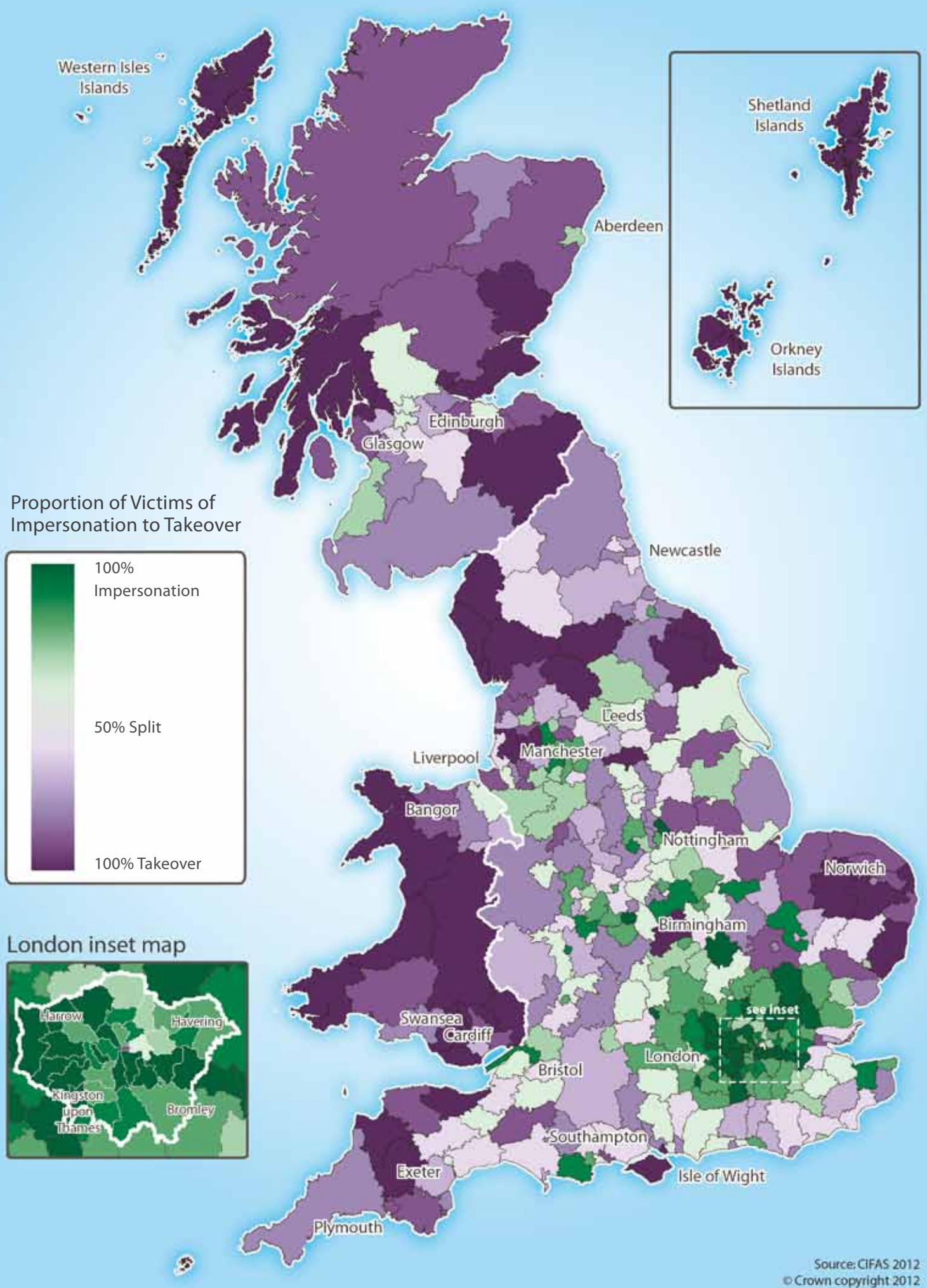
Ordnance Survey

B: Victims of Takeover in 2011 per thousand people by local authority area



Source: CIFAS 2012

C: Proportion of Victims of Impersonation to Victims of Takeover in 2011 by local authority area



4. The Fraud Landscape

Map D presents the total number of frauds – including first party frauds (see section 5) – recorded in 2011, per thousand people by local authority area. As with previous years, the clearest finding is that the highest levels of fraud are concentrated in urban areas, most noticeably in and around London. Other 'urban hotspots' – where the number of frauds per thousand people is visibly higher in one area than other surrounding areas – include the Manchester region (comprising Blackburn with Darwen, Bolton, Salford, Rochdale, Oldham and Manchester), Bradford, Coventry and Glasgow City.

So far, so unsurprising; but there are some interesting anomalies – most obviously Worcester, the Wolverhampton/Sandwell/Birmingham area and the Cambridgeshire/Peterborough cluster. These areas, while containing large urban centres of population in national terms, obviously represented centres of fraud activity in 2011 which far outstripped the surrounding areas. The particular reasons behind such concentration of activity are, of course, impossible to determine from a map alone.

The picture in the rest of the UK, however, presents an overarching pattern of fraud being concentrated in the South East, Thames Valley, and stretching along the M6/M62 and M4/M5 corridors – with other occasional concentrations in South Wales, North East Scotland and North East England.

What is perhaps most interesting and enlightening, however, is what the national fraud map reveals in conjunction with the other maps – in terms of the frauds taking place in an area. *Map D* shows a comparatively low number of frauds per thousand people in the Northern Scottish Authority areas and across much of South and Central Wales. Looking at *map B* (the number of Victims of Takeover per thousand people – page 24), however, shows that these same areas score more highly in terms of the number of Facility Takeover victims per thousand of population. The implication, of course, is that the low – overall – fraud level is made up predominantly by these cases of Facility Takeover, i.e. the people living in these areas are innocent victims and not complicit in fraud.

Tables 4.1.1 and 4.1.2 – for additional interest – show the top ten London and non-London postal districts for the total number of frauds recorded in the UK during 2011. ●

Top Ten London Postal Districts for Fraud
Table 4.1.1

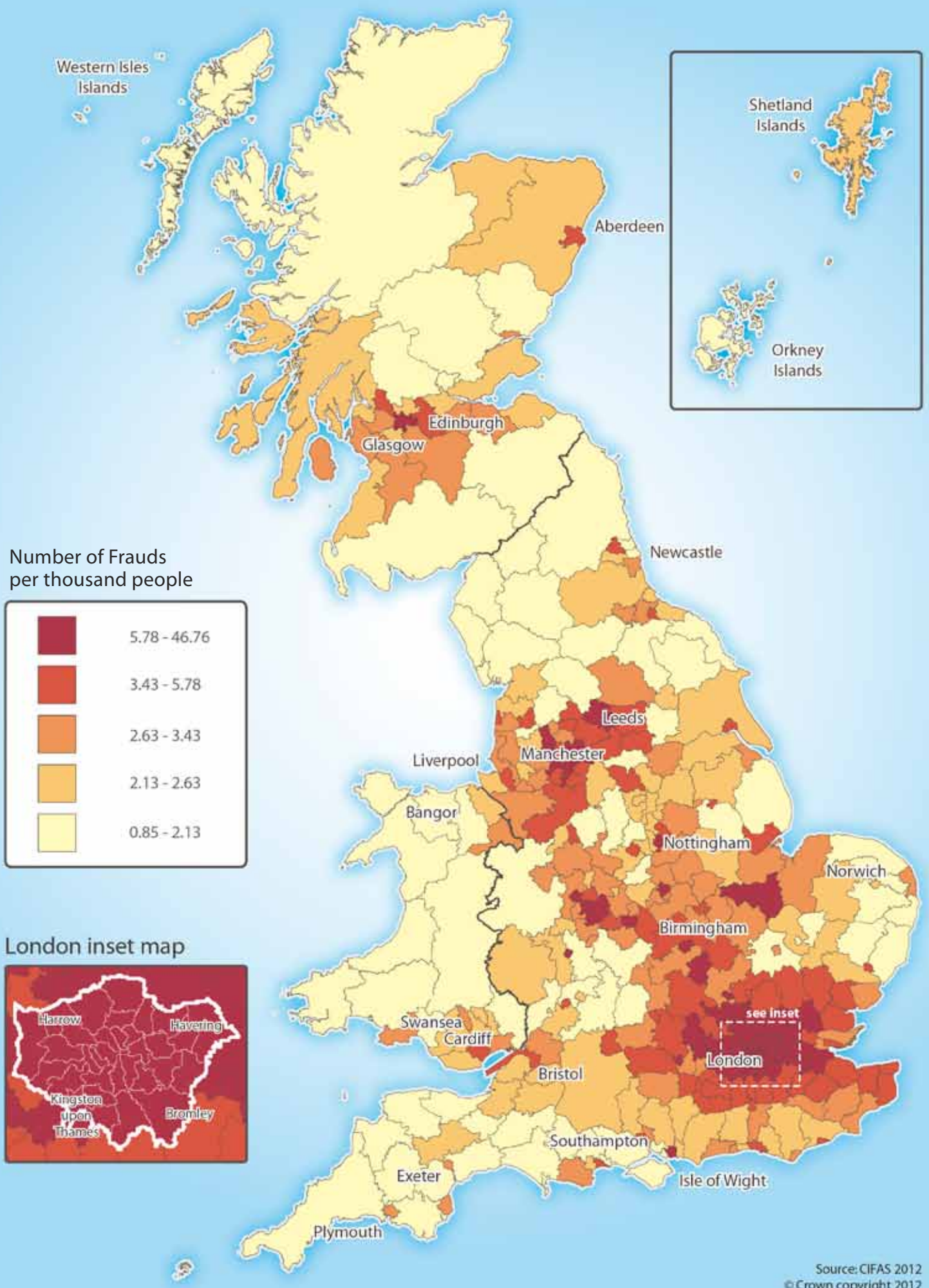
Postal District	Name	Number of times an address used in fraud
E6	East Ham	2,252
IG11	Barking	1,972
SE18	Woolwich	1,940
E17	Walthamstow	1,629
CR0	Croydon	1,613
SE15	Peckham	1,484
E7	Forest Gate	1,417
E13	Plaistow	1,331
IG1	Ilford	1,320
SE28	Thamesmead	1,286

Top Ten non-London Postal Districts for Fraud
Table 4.1.2

Postal District	Name	Number of times an address used in fraud
LU1	Luton	767
AL10	Hatfield	744
SL1	Slough	706
CV1	Coventry	664
LE3	Leicester	648
M8	Manchester	620
LE2	Leicester	598
CV2	Coventry	567
PE1	Peterborough	563
M14	Manchester	530

Ordnance Survey

D: Total number of frauds in 2011 per thousand people by local authority area



Ordnance Survey marks the spot

Where claimants in the same neighbourhood are colluding

Our up-to-the-minute geographic intelligence provides banks and insurers with vital information, enabling them to analyse fraud hot spots, make better-informed decisions and protect themselves against fraudsters. In fact, organisations are seeing savings of up to 15% on the total cost of fraud investigation and prevention.

Discover more at **www.ordnancesurvey.co.uk/cifas**

Ordnance Survey®

5. 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.

Previously, it had been thought that first party frauds were less likely to be the preserve of organised criminal networks than identity related frauds – however, the two categories can never be considered to be mutually exclusive.

An example of this is an individual allowing their bank account to be used to receive unauthorised payments from other sources that turn out to be criminal accounts.

5.1 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.

Table 5.1.1 shows the number of Misuse of Facility Frauds recorded in 2011 compared with 2010. Overall, the number of instances of Misuse of Facility Fraud increased just over 13%. The vast majority of misuse cases related to bank accounts, which increased a further 10% on the back of increases in previous years. Other notable rises were seen in cases of misuse of communications accounts and mail order accounts, although there was a decrease in misuse of plastic card accounts – the only product that saw a reduction.

Misuse of Facility Frauds recorded by Product 2010-2011
Table 5.1.1

Product	2010	2011	% change
All-in-One	56	107	+91.1%
Asset Finance	407	433	+6.4%
Bank Account	37,144	41,018	+10.4%
Communications	4,163	5,477	+31.6%
Plastic Card	4,052	3,471	-14.3%
Insurance	90	90	-
Loan	204	334	+63.7%
Mail Order	1,504	2,952	+96.3%
Mortgage	85	87	+2.4%
Other	26	27	+3.8%
Total	**47,731**	**53,996**	**+13.1%**

Commonly held, commonly abused

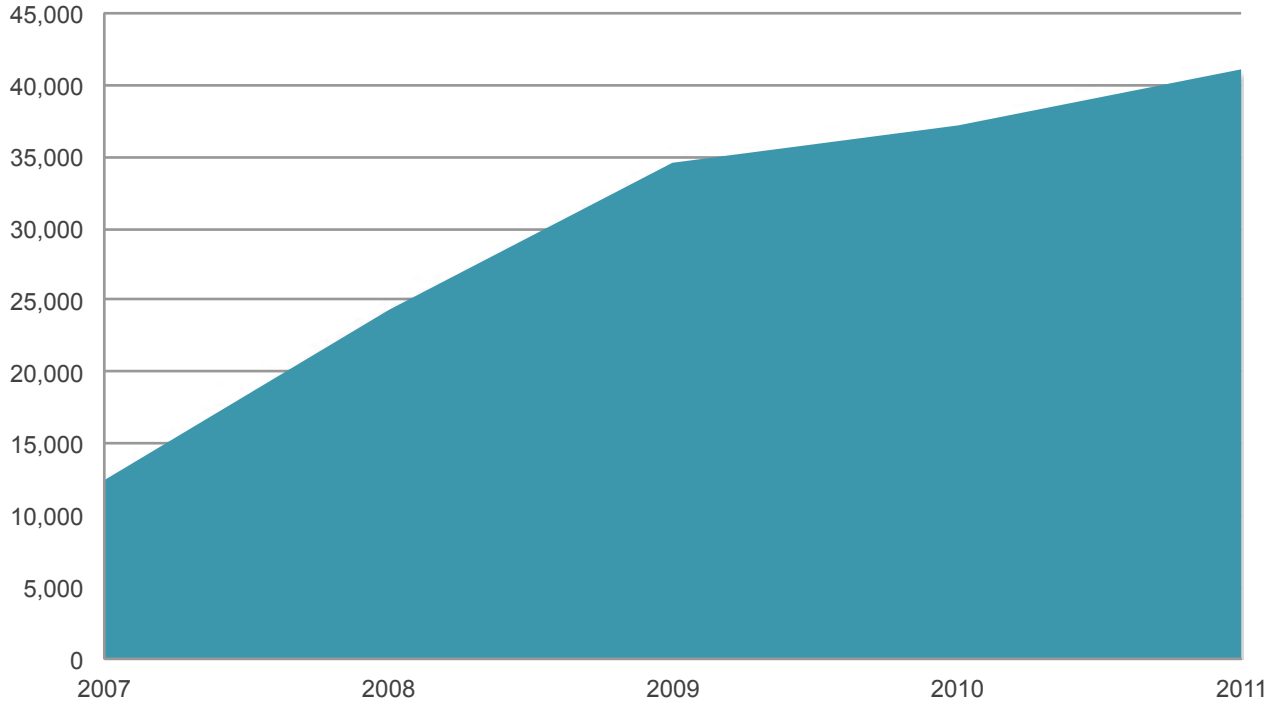
The bank account is one of the most important financial products an individual can have access to and is the first building block of a financial identity. A key part of the Government's financial inclusion initiative has been to make sure that every citizen has a bank account, while many other products will require their customer also to have a bank account (especially in an age where more organisations

are encouraging account holders to pay by direct debit). Therefore, overall trends and figures regarding the scale of any misuse of bank accounts give a dramatic insight into how fraud has changed from one year to the next; and how circumstances might lead some to misuse a product that they (otherwise) could not imagine being without. >

Figure 5.1.1 below shows that there has been a year on year increase in misuse of bank accounts over the last five years, although the rate of increase is not as rapid as it was in 2008 and 2009.

Number of Misuse of Bank Account cases

Figure 5.1.1



The majority of these cases (63%) relate to instances where the fraudster has paid a false financial instrument in to their account: be that a cheque or an electronic payment. Some of these cases will be opportunistic (where the individual sees an opportunity to gain a financial advantage by doing such things as altering a cheque). Others will be more organised; e.g. using a bank account to take receipt of funds to which the account holder is not entitled and/or may be the result of a previous fraud, such as the proceeds of a fraudulent benefits claim. The most worrying proportion of these frauds, though, relates to those instances where the individual has been recruited as a 'money mule', for example, working on behalf of serious organised criminals to launder the proceeds of crime or to facilitate the receipt of fraudulently obtained benefit payments.

Organised criminals are known to target those short of money; offering them cash in return for the use of > their bank account. Students are a prime example of those targeted. They typically have a low income and may well be youthfully naïve enough not to realise the full implications of their actions; seeing instead some 'easy money' and failing to anticipate the repercussions that their actions have. A particularly malicious form of this fraud, though, involves serious organised criminals coercing individuals into opening an account, before taking complete control of that account.

Unfortunately, these figures may well represent just the tip of the iceberg. An individual who has been scammed or duped into becoming a money mule (for instance, by responding to an employment scam) has not committed a criminal offence and is, therefore, not recorded to the National Fraud Database. Employment scams often offer the victims the opportunity to become a 'payment processing agent' or some variant of this title: usually a role where the applicant is merely required to receive >

funds into his or her bank account and then transfer it to another, or withdraw it and wire it overseas. People allowing their bank accounts to be used in such a way will often not realise that anything is wrong, until their bank account has been closed: as banks are not prepared to facilitate money laundering. Unfortunately, the present economic climate has left many people without work and, therefore, susceptible to this kind of scam. It is probably also the case that those who would question the legitimacy of such an offer in better times, may ignore the nagging doubts in the back of their mind when times are not so good. In such ways, criminals effectively are persuading individuals into misusing their own identities and accounts – as a form of human shield for other criminal behaviour. Such activity, of course, could represent a third strand to identity related crime.

In addition to the increase in the number of cases of false instruments being paid in to bank accounts, there was also a rise in the number of cases of customers retaining wrongful credit. This is where a customer refuses to return funds erroneously credited to his or her account. This type of fraud accounted for 23% of misuse of bank account cases in 2011, up from 18% in 2010. Unfortunately, it is impossible to state a definite reason for the increase; although financial desperation leading some to be unwilling to return what is not theirs, and reduced headcount in banks resulting in an increased workload on remaining staff remain likely contributors. Equally, it might be a combination of both, meaning that organisations must look at their own processes and ensure that errors of this kind do not take place. >

Money Mules

Definition: The term 'money mule' is most commonly used to describe an individual who allows his or her bank account to be used to facilitate the movement of criminal funds. The mule either knowingly helps to move, or is tricked into moving, money through his or her own account and then to a third party, who is often located in another country.

Methods: The primary driver behind these transactions is a fraudster located overseas who has obtained funds through phishing or trojan scams and intends to launder these funds out of the UK. As it is difficult to make cross-border transfers from UK accounts, the fraudsters need collaborators with other UK accounts to move the funds for them.

The fraudster asks the individual to receive a transfer of funds into his or her bank account, and then instructs the person either to send these funds on to another account, or to withdraw the funds (in Sterling or foreign currency), or to send them overseas using a legitimate money transfer service. The individual carrying out these transfers is typically offered payment, frequently in the form of commission, for this use of their account. This individual, the 'mule', may be complicit or completely unaware of the true nature of their actions.

Fake employment scams: Fraudsters are also known to contact people using email addresses harvested through phishing scams or legitimate recruitment websites – offering jobs based 'at home' with a high salary for a few hours a week. These adverts state that the recruiter's overseas company is seeking 'UK representatives' or 'agents' to act on its behalf for a period of time. Job titles will be typically vague; along the lines of Financial Manager, Payment Processing Agent or Money Transfer Manager. Once recruited, the new 'employee' will begin to receive regular deposits into his or her account. Minus a small commission, the mule is then asked to withdraw or transfer the funds for placement into an overseas account.

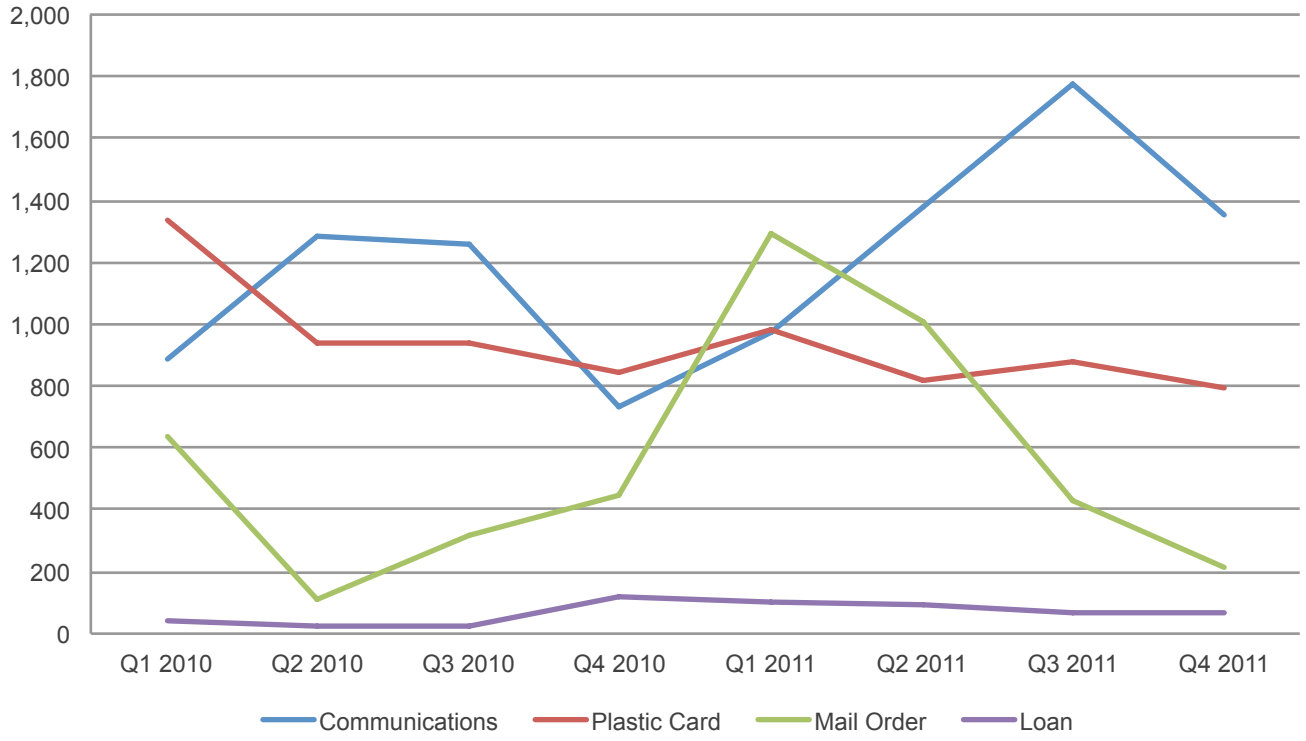
Targets: University students are often recruited as they are more likely to have unblemished credit records and low incomes, and can be attracted by such schemes as these, as they offer an apparently easy way to make some additional money.

The unemployed are sometimes targeted through legitimate employment websites. Difficulties in obtaining work may lead to some people becoming willing to take any likely looking role, without applying the same scrutiny that the person would usually apply to an approach by an employer or recruiter.

People moving to the UK have also been approached, sometimes in their home countries, and offered jobs in the UK – moving funds as outlined above. In addition, people moving away from the UK are approached to hand over their bank accounts or good credit record when they leave, in order for fraudsters to make future use of them.

Number of Misuse of Facility cases by Product

Figure 5.1.2

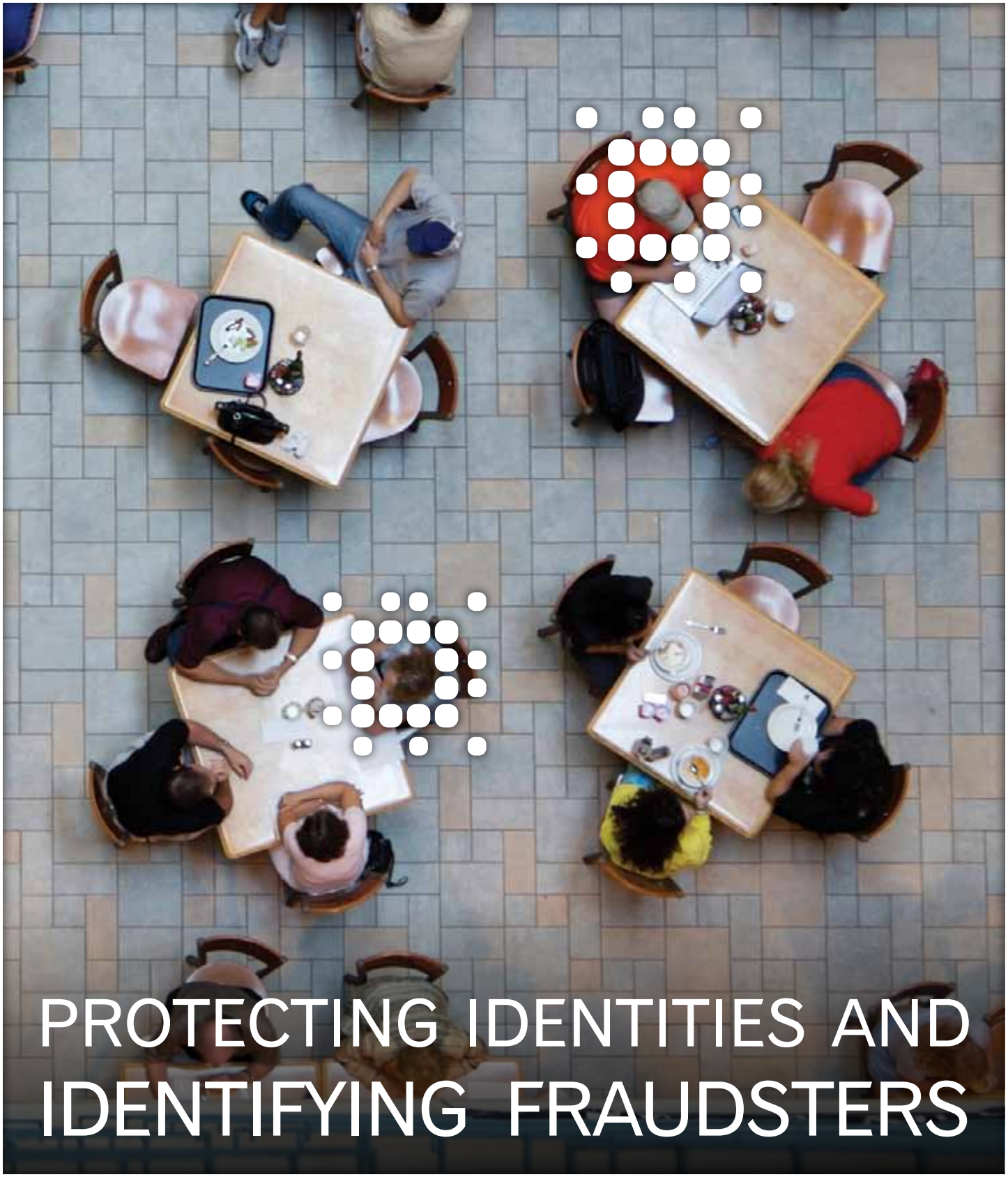


But it's not just bank accounts

Figure 5.1.2 shows the number of cases of Misuse of Facility identified against communications products, plastic cards, mail order and loans (the four products that experienced the most misuse after bank accounts) for each quarter in 2010 and 2011.

The majority of the misuse of communications accounts – perhaps surprisingly – related to digital media services (such as cable or satellite television packages), and not mobile phone accounts. 60% of cases involving the misuse of communications accounts were regular payment frauds (which means the fraudster set up a fraudulent instruction to debit an innocent party's account). This essentially means the fraudster is trying to get someone else to pay their subscription for them. Almost all of the rest of the misuse of communications cases related to instances where the customer never had any intention of honouring their agreement to pay for the services that they were receiving. It is noticeable that the number of misuse of communications accounts increased over the course of most of 2011, although there was a drop in the fourth quarter of the year. There was a corresponding drop in Q4 of 2010 as well, and these dips at the end of the year may well have explanations other than there actually being less fraud taking place. The overall increase seen over the year, however, was likely to be another symptom of the economic conditions; with people seeing their disposable income reduce and therefore they looked for ways to retain their digital television service without actually paying for it.

Misuse of mail order accounts (nearly all of which related to the evasion of payments where there was no intent to honour the debt and evidence of an intent to defraud) had been increasing since the start of the second quarter of 2010. It then spiked in the first quarter of 2011, and has been declining ever since. The abrupt spike can probably be attributed to people dodging payment for Christmas gifts – especially in financially taxing times. The time lag between the ordering of the goods and the establishment of proof of fraudulent evasion of payment also explains why levels of this type of fraud remained relatively high in the second quarter of the year. •



PROTECTING IDENTITIES AND IDENTIFYING FRAUDSTERS

Experian™
A world of insight

Experian is a world leader in helping people and organisations make sense of complex data and reach informed financial and commercial decisions. We help individual consumers protect their identities and assist businesses to protect customer accounts by authenticating identity and identifying fraudsters.
To learn more, visit experian.co.uk

5.2 Application Fraud

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

Table 5.2.1 shows the number of cases of Application Fraud identified in 2011 compared with 2010. Overall there was a slight drop in the number of cases recorded but, as mentioned earlier, this drop represents a markedly slower decrease than seen in previous years. Within the overall decrease, five product types actually saw an increase in Application Frauds while five saw a fall. Application Frauds against bank accounts (the largest group), however, saw a 32% decrease from 2010 levels, while Application Frauds against insurance products saw an increase of over 150%; which made this the second most common product type targeted by application fraudsters.

Application Frauds recorded by Product 2010-2011

Table 5.2.1

Product	2010	2011	% change
All-in-One	179	86	-52.0%
Asset Finance	8,247	6,945	-15.8%
Bank Account	17,756	12,039	-32.2%
Communications	4,578	5,118	+11.8%
Plastic Card	3,830	4,378	+14.3%
Insurance	2,944	7,426	+152.2%
Loan	3,397	3,958	+16.5%
Mail Order	246	174	-29.3%
Mortgage	3,391	2,994	-11.7%
Other	112	145	+29.5%
Total	**44,680**	**43,263**	**-3.20%**

Figure 5.2.1 (page 35) shows that, following a peak in 2008, there has been a substantial decline in Application Fraud cases against bank accounts; decreasing by 60% since 2007. As the largest product category this decrease is the most obvious on the graph, but it is actually loan products which have seen the biggest decline in the number of cases; having dropped 68% during the same time period. The only two products which are experiencing more Application Fraud now than in 2007 are insurance and communications – the non-credit related products.

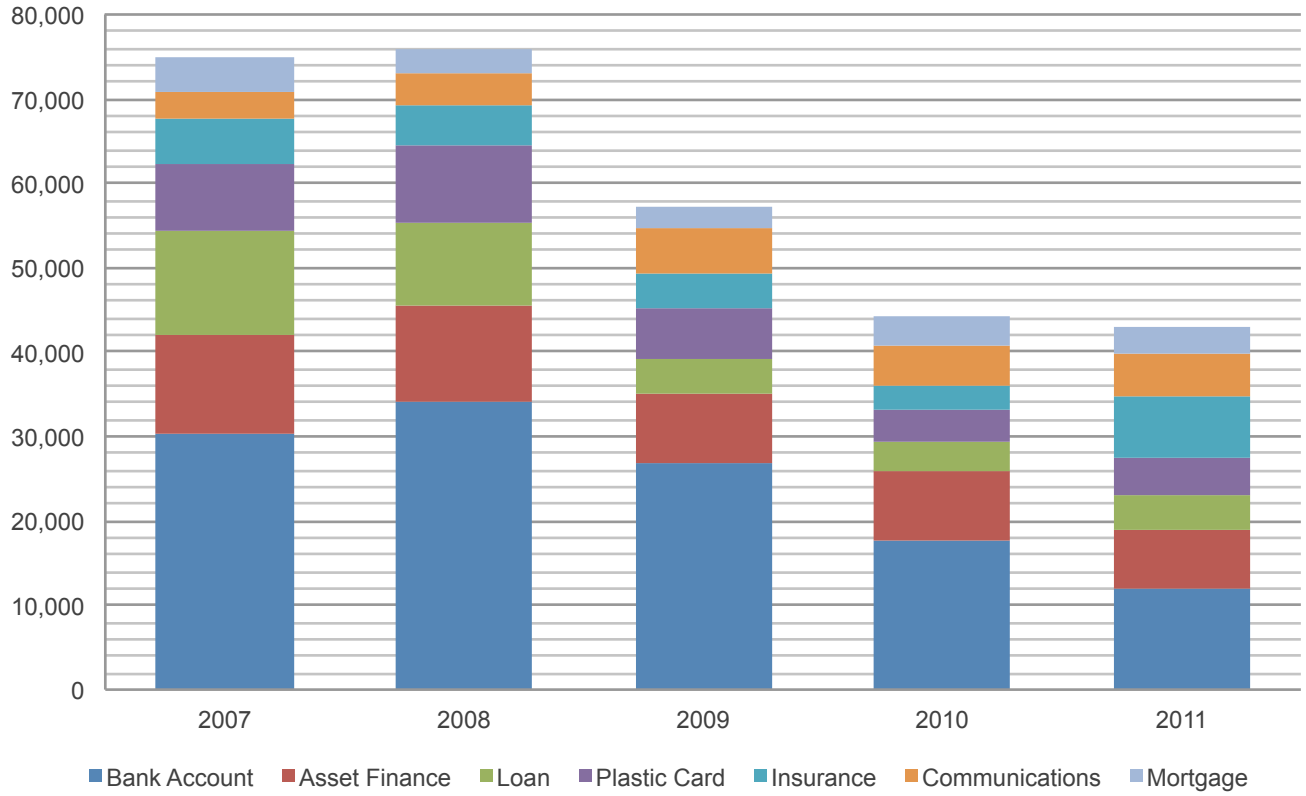
The reasons for this can be laid squarely at the door of the economy. The credit crunch meant that there was a caution about lending – so only the most creditworthy and risk free applicants were likely to be approved during an initial lending decision. The majority of Application Fraud cases were identified and recorded because the applicant had failed to disclose a previous address where there was adverse credit information recorded in their name. The reason for this was simply that applicants were trying to make themselves look like less of a bad credit risk and this type of Application Fraud accounted for over 60% of Application Frauds in 2011. In times when credit is more readily available, this type of deceit may mean that the application passes initial credit scoring only to be picked up later by the fraud department.

In the present circumstances, however, telling lies to avoid appearing to be a bad credit risk does not guarantee that the fraudster becomes a sufficiently good credit risk to pass scoring. Consequently, the number of recorded Application Fraud cases against credit products has decreased in recent years. It does not mean that they have not been attempted, but it does mean that they could never be identified simply because the lies told did not lead to a successful application.

Another reason for the decline in numbers was that there were some people who, prior to the credit crunch, wanted a loan (for example) and had every intention of repaying the sum borrowed – but would also have been aware that there was adverse credit data against them. They knew, therefore, that the likelihood of their application being approved was low. Some of these, subsequently, attempted to hide this adverse information in order to be approved. In the present climate, however, those who may previously have been prepared to overstretch >

Application Frauds recorded by product type 2007-2011

Figure 5.2.1



themselves financially may no longer be willing to take the risk of biting off more than they can chew.

A change is coming

There have been some indications that the overall situation of declining Application Fraud levels is reversing. For example, there has been an increase in the number of Application Fraud cases recorded against plastic cards and loans. Interestingly, in cases of Application Fraud to obtain a plastic card, while the number of cases of hiding addresses with adverse credit information has increased in number, it actually accounts for a lower proportion of the cases in 2011 than it did in 2010 (63% down from 70%). The difference comprises cases where the applicant has provided false employment information. The number of these cases accounted for almost a quarter of Application Frauds in 2011, up from 13% the year before. With unemployment at the end of November 2011 at the highest level since 1994, and 2.685 million people out of work (Office for National Statistics), this increase is unsurprising.

This same applies to Application Frauds for mortgages. Although the total number of Application Frauds identified in 2011 decreased compared with 2010, the number of cases where false employment details were provided almost doubled – up to 512 cases (17% of Application Frauds) from 283 (8%) the year before. Historically, mortgage Application Frauds have always seen a high level of falsification of documents (most commonly of payslips) in order to make it seem that the applicant earns more than is actually the case. Now it seems that more applicants are having to lie about earning anything at all.

But there's more ...

This is not the case with Application Frauds against loans, however, where the proportion of cases involving the provision of false employment details actually dropped to 10% of cases, from 15% the year before. This somewhat counterintuitive finding is likely to be due to the emergence of payday lenders. These lenders specifically cater for those who need cash quickly in order to make ends meet, but only need it for a short period of time. One of the selling points of these loans is that the application >

process is very quick and hassle free. This means that less information is validated as part of the application process and, therefore, that employment details are checked less often. If the lender does not check for employment details because it is not relevant to their decision about whether to lend or not, then an applicant who is out of work and covers this up, is not identified.

The other aspect of payday loans that has contributed to the increase in Application Fraud cases identified is that they are specifically designed with the cash-strapped in mind. Such applicants are expected to have lower credit scores. This means that the credit scoring thresholds that shield 'traditional' lenders from fraudulent applications are not applicable to payday lenders. This gives an organisation's fraud department the opportunity to investigate, identify and record these frauds when they occur.

Insurance presents different challenges

Application Frauds against insurers follow a very different pattern. As an individual's credit rating has little bearing on the granting of an insurance policy, there are far fewer instances of people failing to disclose adverse credit information. There are, however, plenty of people massaging the details on the proposal in an attempt to get the lowest quote possible. This can involve attempting to hide previous claims or convictions – the number of these cases doubled in 2011 compared with 2010. There was a substantial increase in the number of cases where the applicant submitted numerous applications with inconsistent information (25% of Application Frauds against insurers in 2011, up from 16% the year before). This is done, obviously, with the intent of discovering which combination of details would give them the lowest quote, rather than giving a truthful response to the question asked.

The most prominent fraud in insurance proposals, however, was the provision of false bank details. This accounted for just over 30% of Application Fraud cases in 2011, up from 24% the year before. In these cases, which were predominantly for motor insurance, the fraudster was intending to obtain genuine insurance documents, even though the policy itself would have been cancelled when the fraud was discovered. The applicant might or might not have been aware of this so they might have believed that they were still covered for the period of time highlighted in the certificate. If the fraudster had been aware that the policy would be voided, then the objective was more likely to have been with a view to producing a 'genuine' certificate in order to tax the vehicle or to be able to produce evidence of insurance if requested by the police.

More worrying, however, is the spectre of 'ghost brokering'. This occurs when someone poses as an insurance broker, and makes applications on behalf of their clients. They take the premium from their clients, but provide false bank details on the application – pocketing the money from their client. The documentation is issued, but when the bank details are identified as false, the policy is voided. The clients will then be in possession of genuine documents, not backed by valid cover, so will be unaware that they are actually driving illegally and will find themselves out of pocket in the event of a claim. •

5.3 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).

The Asset Conversion Fraud type is specific to asset finance organisations. This type of fraud represents only a small proportion of the frauds suffered by asset finance organisations, however – less than one in ten frauds. The vast majority of frauds against asset finance organisations were Application Fraud, most usually people telling lies on the application to obtain a vehicle which they probably would not be able to afford. Asset conversion, though, while presenting only a limited risk in terms of the number of frauds, presents a much more substantial risk in terms of fraud losses. Application Frauds are mostly identified before credit is granted, so the organisation incurs no financial loss. When a (typically subject to a hire purchase agreement) vehicle is sold unlawfully, however, the organisations involved lose the outstanding value of the vehicle, which could be substantial. It is possible that the vehicle might be recovered, but this cannot be guaranteed, and the recovery process can be costly. In addition, there is the particular risk that high-value cars which are converted in this way are often shipped out of the country.

Number of Asset Conversion Frauds 2010-2011

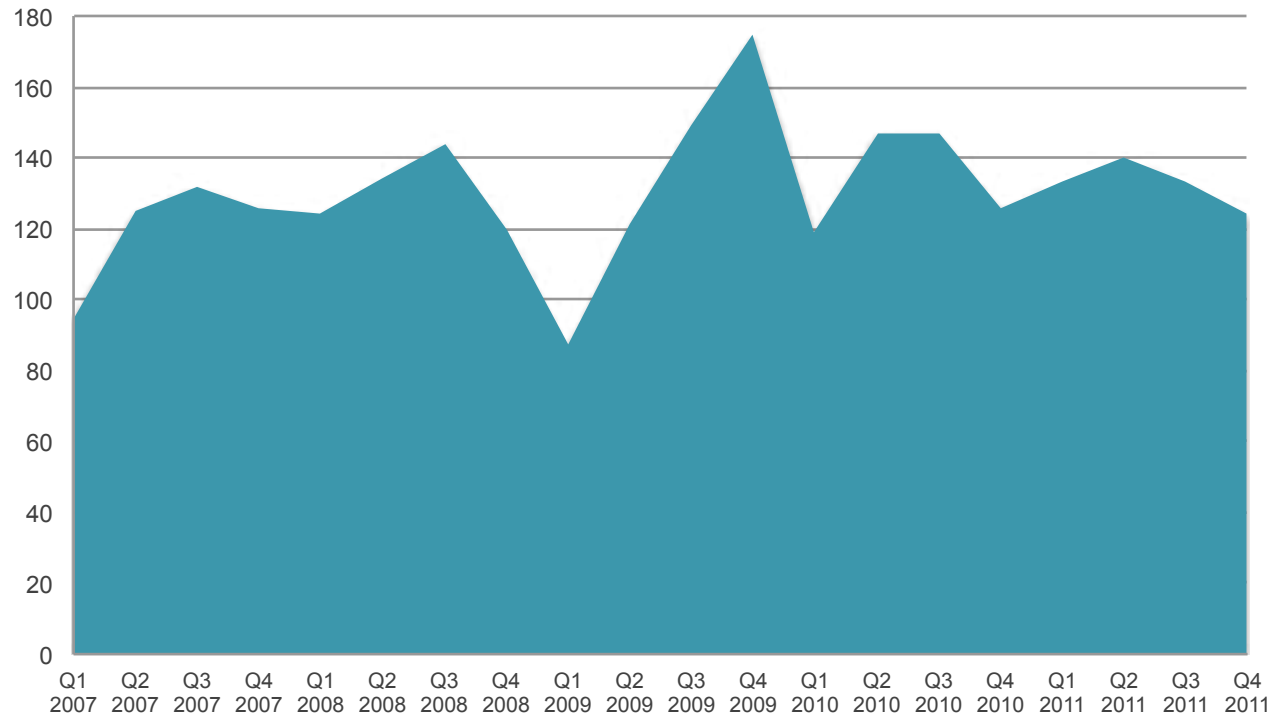
Table 5.3.1

Product	2010	2011	% change
Asset Finance	539	532	-1.3%

The total number of Asset Conversion Frauds decreased slightly in 2011 compared with 2010, but by only seven cases. *Figure 5.3.1* shows that, with the exception of 2009, the number of Asset Conversions identified per quarter over the last five years fluctuated relatively little. This indicates that this sort of fraud is relatively recession-proof.

Total Number of Asset Conversion cases

Figure 5.3.1



5.4 False Insurance Claims

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

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 conviction means that only a percentage of attempted False Insurance Claims are recorded by CIFAS. It is often the case that attempts by the insurer to ratify the claim results in the claimant withdrawing it, walking away when they realise that their attempt will be unsuccessful. This, of course, denies the insurer the opportunity to verify whether or not the claim was fraudulent. Figures reported by the Association of British Insurers put the number of fraudulent insurance claims in 2010 at 133,000.

So, while the False Insurance Claims recorded on the National Fraud Database did not encompass all of the frauds that had taken place, they nevertheless provide intelligence in relation to the cases that were recorded.

Number of False Insurance Claims recorded in 2010-2011

Table 5.4.1

Product Type	2010	2011	% Change
Insurance	537	396	-26.3%

One for the road

Fraudulent claims against motor insurance policies increased by 17.5% in 2011 compared with 2010 (up to 255 cases). Most notable was that the proportion of these cases which involved a staged accident went up to almost 60% of false claims against motor insurance. This is worrying as it bears the hallmarks of 'cash for crash' accidents, where criminals deliberately crash vehicles on UK roads in order to make false claims. This obviously endangers the safety of those both directly involved in the crash and any innocent bystanders. These crashes are staged not just to claim the value of the vehicles involved, but also to claim damages for such things as personal injury (potentially certified by a complicit doctor), vehicle hire while the crashed car is being repaired and inflated bills for that repair. Recruiting people to take part in these staged accidents is made easier when times are tight, as there are likely to be more people who have become desperate enough to accept cash.

Of course, it shouldn't be assumed that all staged accidents are the work of organised criminal gangs. It is likely that some of these accidents were arranged by someone whose aim was simply to claim for the value of the vehicle.

Home is also where the fraud is

The number of false claims against home insurance policies declined in 2011 compared with 2010. This drop, however, had more to do with the changing mix of organisations recording false home insurance claims than any lessening of the UK public's propensity to submit false claims. It is interesting, though, that within those false claims that were recorded there was a proportionate increase in the instances of someone submitting a claim for an event they were not entitled to claim for (for instance where the damage occurred outside of the cover period). This accounted for just over half of all false home insurance claim cases up from 37% the year before. Conversely there was a proportionate decrease in the cases that involved a claim being inflated (down to 14% of cases).

So, it would seem that when an individual makes a false claim, they were increasingly claiming for events for which they did not have cover, as opposed to the more opportunistic inflation of the value of a claim for a genuine event. This makes the claims submitted appear to be more calculated. It is easier to understand (without condoning) the mentality that, when someone has been paying their premiums for years, they feel they are 'entitled' to try and get as much as possible when the opportunity presents itself (particularly when there isn't the same amount of disposable income available), to the much more unconscionable attempt to take what they are not entitled to at all. •

5.5 Who are the first party fraudsters?

As previously explained, in Section 3.2 (page 14), it is impossible to say who, precisely, the fraudsters are; largely because (in the case of identity related crime) it is impossible to state categorically who the identity criminals are. As a result, when asking the question 'who are the fraudsters?' it is the first party fraudsters who provide an answer. For a definition of first party fraud see the beginning of Section 5 (page 29).

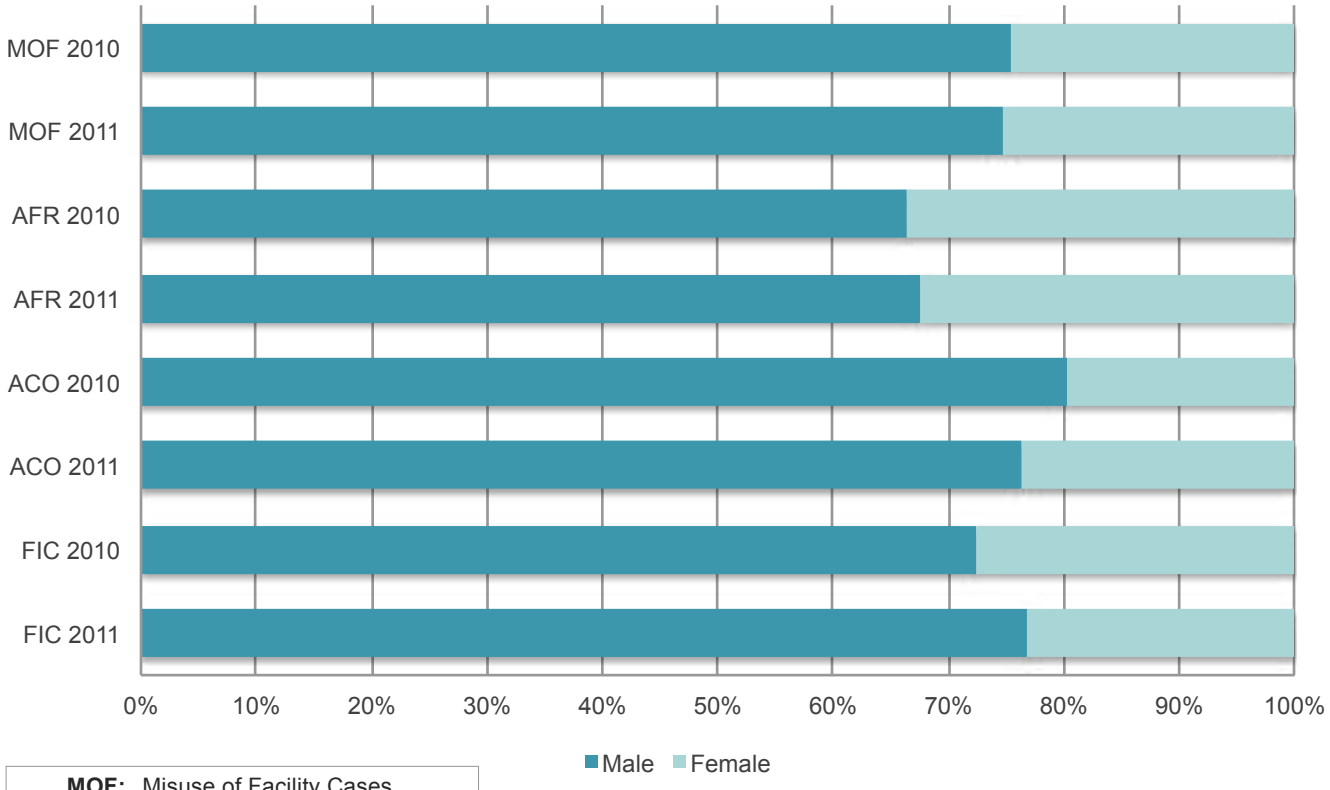
The gender of the subjects involved in first party fraud cases was recorded over 94% of the time. The gender distribution for each of the types of fraud under the 'first party fraud' banner are shown in *Figure 5.5.1* below.

Boys vs girls

Figure 5.5.1 shows that men were involved in first party frauds far more than women. This was particularly the case for Asset Conversion, where men accounted for 80% of subjects in 2010, although in 2011 this figure was down slightly to 76%. Conversely, there was a slight increase in the proportion of men making false insurance claims. This was a symptom of the swing towards false motor insurance claims, as opposed to home contents cover. Historically, there was a higher proportion of women prepared to submit fraudulent home insurance claims than claims against motor insurance. >

Gender distribution of those involved in fraud

Figure 5.5.1



MOF: Misuse of Facility Cases
AFR: Application Fraud Cases
ACO: Account Takeover Cases
FIC: False Insurance Claims

Application Fraud continued to be the fraud type that saw the highest proportion of female involvement, although this fluctuated across the products affected. Women were most commonly involved with Application Frauds to obtain mail order accounts (55% of subjects in 2011) and communications products (mostly mobile phone accounts) where they made up 43% of subjects. Historically, there was a proportionately higher number of women involved in Application Fraud for plastic cards, but in 2011 this decreased – down to 40% of subjects from 48% the year before.

Young vs old

Figures 5.5.2 and *5.5.3* show the age distribution of those involved in first party frauds. *Figure 5.5.2* shows which type of fraud those of a given age range were involved in, and *Figure 5.5.3* highlights the ages of those involved in a given fraud type. This shows that the younger the subject, the higher the proportion of times they have been involved in Misuse of Facility Fraud, while the older the subject, the higher the level of involvement in Application Fraud.

Those who have been involved in false insurance claims tend to be older than those involved in other types of fraud. This could be due to the nature of some of the products that false claims are made against. Home contents cover, for instance, is less likely to be required by someone under 21 who is more likely still to live with their parents, meaning that few under 21s would be making a claim at all, let alone a fraudulent one. It may also be the case that the older a person is, the longer they are likely to have been paying premiums. This may contribute to a feeling that the claimant is 'owed' something by their insurer. So, when times get tight, they may feel justified in attempting to collect on that perceived 'debt' by inflating a claim or submitting an entirely fictitious one.

The fraud type that sees the highest proportion of involvement by the very young, the under 21 and the >

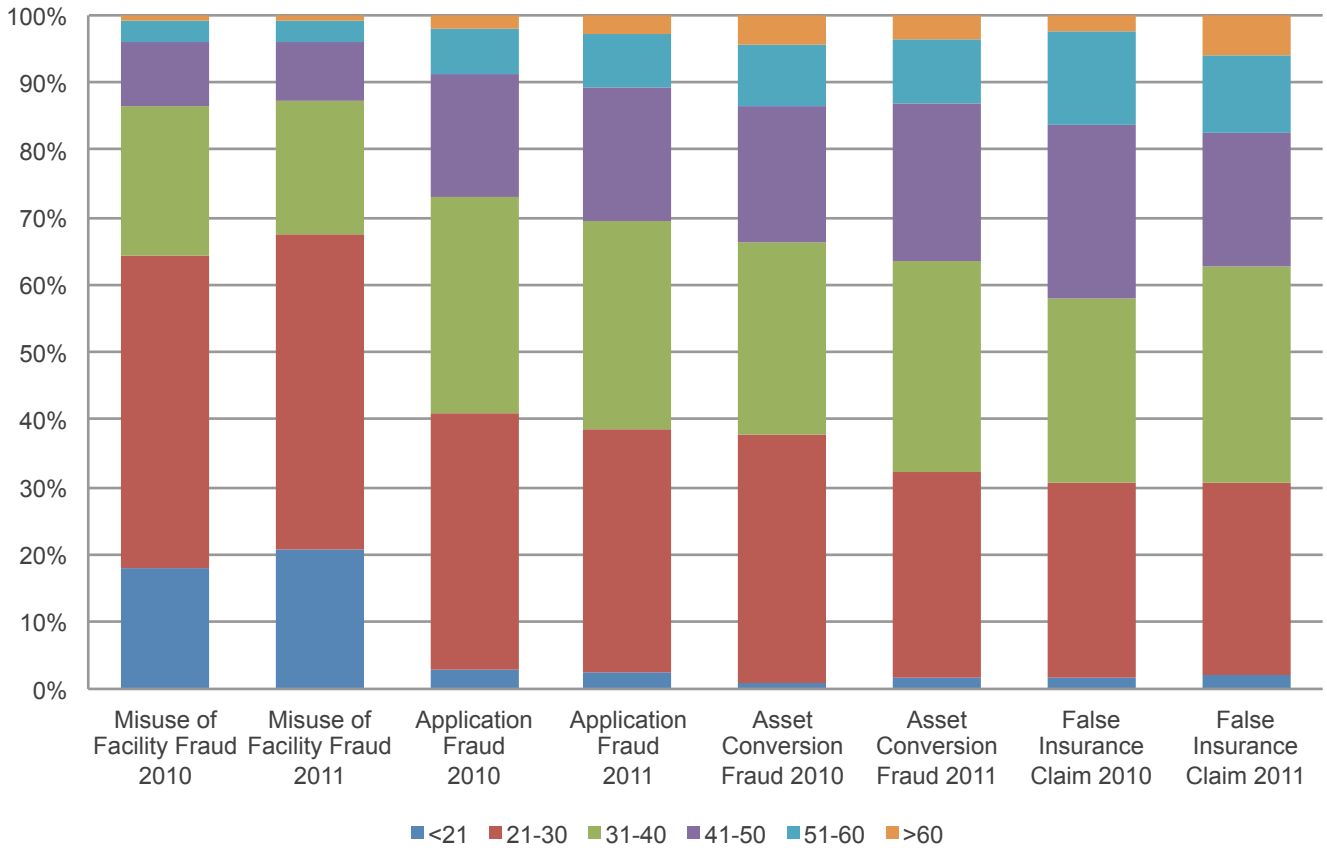
Age distribution of those involved in fraud
Figure 5.5.2

21 to 30 age brackets, is Misuse of Facility Fraud. This is unsurprising given the nature of a lot of these frauds, specifically the 'money mule' cases where people have been recruited by organised criminals to allow money to be laundered through their bank account. These criminals target this age range frequently as they believe them to be more likely to accept payment and not ask questions.

Youthful naïvety may well be the reason why such mules do not realise the consequences or implications of what they have been asked to do. It is also the case that in the present economic conditions, as numerous other findings and headlines attest, it is the young who are finding it the most difficult to gain employment; making them more susceptible to the advances of criminals. •

Age distribution of subjects involved in fraud

Figure 5.5.3




Stop
Staff Fraud
before it starts
CIFAS
The UK's Fraud Prevention Service
www.cifas.org.uk

Appendix: Fraud by Product Type

1. All-in-One

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

- There has been a decrease in the number of cases of recorded fraud affecting all-in-one products, although the number of cases of fraudulent misuse of these accounts almost doubled.
- The number of frauds which affects these products is low, however, so a comparatively small change in the number of cases recorded translates to a more substantial percentage change.

Fraud Type	2010	2011	% change
Identity Fraud	271	216	-20.3%
Facility Takeover Fraud	255	209	-18.0%
Misuse of Facility Fraud	56	107	+91.1%
Application Fraud	179	86	-52.0%
Total	**761**	**618**	**-18.8%**

2. Asset Finance

- The frauds related to asset finance decreased in 2011 compared with 2010.
- The majority of frauds continued to relate to cases of Application Fraud, and risk averse lending practices are likely to have accounted for a lot of the decrease in these types of fraud.
- There was a small increase in cases of Misuse of Facility Fraud, with slightly more individuals resorting to fraudulent means to keep up with payments.

Fraud Type	2010	2011	% change
Identity Fraud	472	325	-31.1%
Misuse of Facility Fraud	407	433	+6.4%
Application Fraud	8,247	6,945	-15.8%
Asset Conversion Fraud	539	532	-1.3%
Total	**9,665**	**8,235**	**-14.8%**

3. Bank Accounts

- Fraud against bank accounts increased in 2011 compared with 2010, with the largest increases seen in identity related crimes.
- Increasing Identity Fraud and Facility Takeover Fraud may have been as a result of the increasing availability of personal information to fraudsters – particularly if this information includes user names and passwords.
- Many of the Misuse of Facility Frauds recorded against bank accounts showed worrying signs of being related to 'money mule' activity, with account holders moving money on behalf of organised criminals.

Fraud Type	2010	2011	% change
Identity Fraud	11,030	14,873	+34.8%
Facility Takeover Fraud	1,974	2,814	+42.6%
Misuse of Facility Fraud	37,144	41,018	+10.4%
Application Fraud	17,756	12,039	-32.2%
Total	**67,904**	**70,744**	**+4.1%**

4. Communications

- Frauds against communications providers increased by almost a quarter in 2011 compared with 2010. Much of this increase is likely to have been driven by fraudsters attempting to obtain valuable and aspirational devices, such as smartphones.
- The increase in Misuse of Facility Fraud was largely attributable to fraudsters attempting to have others pay the subscription for their digital TV package.
- The decrease in Facility Takeover Fraud was surprising in the light of the overall increases in both Facility Takeover Fraud and fraud against communications companies.

Fraud Type	2010	2011	% change
Identity Fraud	16,821	25,996	+54.5%
Facility Takeover Fraud	6,590	6,136	-6.9%
Misuse of Facility Fraud	4,163	5,477	+31.6%
Application Fraud	4,578	5,118	+11.8%
Total	**32,152**	**42,727**	**+24.8%**

5. Plastic Cards

- Fraud against plastic cards increased in 2011 compared with 2010, with increases in all types of fraud apart from Misuse of Facility.
- The increases in Identity and Application Fraud would start to suggest the first signs of increased fraudster confidence in the economy – more of their fraudulent applications were passing credit scoring, and making it to the fraud teams to be identified and recorded.
- Takeover of plastic card accounts increased, as fraudsters used these compromised accounts as another way to make payments.

Fraud Type	2010	2011	% change
Identity Fraud	23,560	24,582	+4.3%
Facility Takeover Fraud	8,209	9,719	+18.4%
Misuse of Facility Fraud	4,052	3,471	-14.3%
Application Fraud	3,830	4,378	+14.3%
Total	**39,651**	**42,150**	**+6.3%**

6. Insurance

- The number of frauds against insurers increased dramatically, but this was almost entirely due to an increase in the number of cases of Application Fraud.
- These Application Frauds involved the provision of false bank details, so the applicant could evade paying the premium and also involved the manipulation of application details to try to get lower premiums.

Fraud Type	2010	2011	% change
Identity Fraud	108	27	-75.0%
Misuse of Facility Fraud	90	90	0%
Application Fraud	2,944	7,426	+152.2%
False Insurance Claims	537	396	-26.3%
Total	**3,679**	**7,939**	**+115.8%**

7. Loans

- Fraud against loans increased in 2011 compared with 2010, with increases seen for all fraud types apart from Facility Takeover Fraud – but the number of these was very small.
- As with the increases seen in fraud against plastic cards, the increases in Application and Identity Fraud may have been a sign of less risk averse lending revealing more fraud, but it is also reveals that fraudsters were targeting the much more accessible payday loans.
- Increasing Misuse of Facility Fraud against loans would seem to suggest that more people were turning to fraudulent means in an attempt to keep up repayments.

Fraud Type	2010	2011	% change
Identity Fraud	2,404	3,795	+57.9%
Facility Takeover Fraud	13	8	-38.5%
Misuse of Facility Fraud	204	334	+63.7%
Application Fraud	3,397	3,958	+16.5%
Total	**6,018**	**8,095**	**+34.5%**

8. Mail Order

- While the overall number of frauds against mail order decreased in 2011 compared with 2010, this was primarily due to a decrease in the number of Identity Frauds perpetrated. This was somewhat offset by an increase in the takeover of mail order accounts. The implication is that the security around account opening was increased, leading to fraudsters targeting already opened accounts.
- The increase in Misuse of Facility Fraud was almost exclusively due to fraudulent attempts to evade payment.

Fraud Type	2010	2011	% change
Identity Fraud	44,577	38,336	-14.0%
Facility Takeover Fraud	4,168	5,939	+42.5%
Misuse of Facility Fraud	1,504	2,952	+96.3%
Application Fraud	246	174	-29.3%
Total	**50,495**	**47,401**	**-6.1%**

9. Mortgages

- The number of frauds against mortgages decreased in 2011 compared with 2010.
- This decrease was due to a drop in Application Frauds, which may well be linked to increasing unemployment. Lack of employment and concerns about future prospects may have been putting off those fraudsters who would have committed Application Fraud to obtain a larger mortgage than they could afford to repay (but would have taken out the mortgage with every intention of repaying).

Fraud Type	2010	2011	% change
Identity Fraud	66	68	+3.0%
Facility Takeover Fraud	0	4	-
Misuse of Facility Fraud	85	87	+2.4%
Application Fraud	3,391	2,994	-11.7%
Total	**3,542**	**3,153**	**-11.0%**

10. Other

- The amount of fraud against 'Other' products increased in 2011 compared with 2010.
- The majority of cases in this group related to fraudulent attempts to obtain someone else's credit file – instances where Identity Fraud was a means to facilitate further fraud.
- The other major increase was in the number of Facility Takeover Frauds, although the numbers themselves were comparatively low. These related to the takeover of share dealing accounts and unauthorised electronic payment instructions. This illustrates that fraudsters are prepared to look beyond the obvious targets to take money from others.

Fraud Type	2010	2011	% change
Identity Fraud	3,363	5,041	+49.9%
Facility Takeover Fraud	17	241	+1,317.6%
Misuse of Facility Fraud	26	27	+3.8%
Application Fraud	112	145	+29.5%
Total	**3,518**	**5,454**	**+55.03%**

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

CIFAS

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