FRAUDSCAPE

Depicting the UK's fraud landscape

www.cifas.org.uk | February 2010

CIFAS

The UK's Fraud Prevention Service

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 265 Members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring and share dealing. Members share information about identified frauds in the fight to prevent further fraud.

The CIFAS database contains records of frauds that have been perpetrated against CIFAS Member organisations. In order to be recorded on the CIFAS database a case must satisfy a burden 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 identified by CIFAS Member organisations during 2008 and 2009 to ascertain any key differences between the typology of the frauds seen in 2009 compared with 2008. It looks at all frauds identified by the type of fraud committed and the product involved.

In this Report . . .

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

Website: www.cifas.org.uk www.identityfraud.org.uk

CIFAS

1. Introduction
by Peter Hurst, CIFAS Chief Executive

Fraud in the UK: it is a subject that receives much attention. But what is the true scale of fraud? And within that true scale, what has actually happened? Are there changes? Are there patterns? New developments? Or is fraud a consistent phenomenon: something that takes place now in the same way that it always has? And no matter what the answers to these questions may or may not be, what are the possible reasons?

CIFAS is the UK's Fraud Prevention Service, a not for profit organisation operating in the public interest, dedicated to the investigation, detection and prevention of fraud. Our 265 plus Members share information on identified fraud in order to prevent further fraud. As a result, analysis of the frauds recorded on the CIFAS database offer a definitive overview of the fraud landscape in the UK.

Irrespective of the size of the fraud (it could be £50, it could be over £50,000) or the type of organisation it was committed against, if it has been investigated and a burden of proof (sufficient evidence to take it to the police) established, then the CIFAS Member will have recorded it on the database. As a result, the fraud trends throughout 2009 are presented here: reliably and impartially. The frauds identified within this document are the actual frauds that CIFAS Members identified in 2009 compared with the actual frauds that they identified in 2008. They are not suspicions. They are frauds.

CIFAS annual fraud trends have long been released to the media and public alike, through a series of press releases and our website (www.cifas.org.uk). As fraud continues to escalate, however, it is time to look at the patterns and the changes that have taken place in a little more detail. The figures and analysis presented throughout this *Fraudscape* report are the result of the figures on the CIFAS database and the relationship that CIFAS shares with the fraud prevention teams of our Member organisations, the police and other prominent private and public sector organisations' fraud experts. We speak to them about what they identify, the trends they notice, the *modus operandi* of the fraudsters and the likely areas in which they will strike - and the results of these conversations feed into *Fraudscape*.

The rise in the more sophisticated current address fraud, or false insurance claims for staged or fictitious accidents is of interest. Equally, the decrease in plastic card fraud, but rise in frauds that target bank accounts and communications products may also be considered noteworthy.

Many questions are raised in *Fraudscape*: most frequently, whether the changes in fraudulent behaviour are solely attributable to the recession, or whether they are due to organised criminality? Overall, both play a part. Fraud, no matter what type, has one thing in common in all cases: people. The motivations of the individual fraudster may or may not differ from that of the organised criminal: but the recession will have affected them both, in the sense that their methods will need to adapt in relation to the economic situations that surround them. Some of the trends and methods identified within *Fraudscape* show that the organised fraudster has developed new ways of attempting to defraud organisations; and the same can be said of the individual fraudster attempting to commit fraud through a lack of perceived 'other (legal) options'. Sometimes, the answers are not easy to find. There are, however, conclusions that can be drawn - and *Fraudscape* does just that.

Fraudscape will give you the inside track on what happened in 2009 compared with 2008, and lay bare the fraud landscape of the UK.

2. The CIFAS Database - General Trends

2.1 Overview

In 2009, the number of frauds identified by CIFAS Members increased by almost 10% compared with 2008, with over 235,000 frauds being recorded to the CIFAS database in 2009.

Fraud cases recorded by CIFAS Members

Table 2.1.1

	2008	2009	% increase
Quarter 1 (Jan - Mar)	52,286	60,481	15.67%
Quarter 2 (Apr - Jun)	52,262	59,348	13.56%
Quarter 3 (Jul - Sept)	53,365	56,323	5.54%
Quarter 4 (Oct - Dec)	56,429	59,300	5.09%
Total Cases Filed	**214,342**	**235,452**	**9.85%**

2008 and 2009 Fraud cases recorded by quarter

Chart 2.1.1

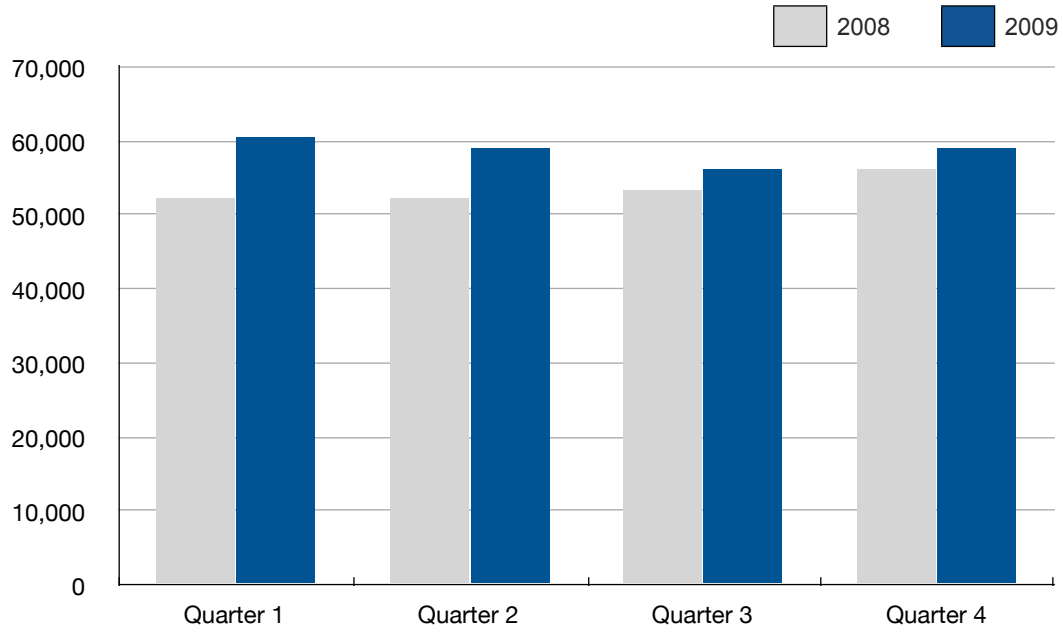


Chart 2.1.1 shows that more frauds were identified in each quarter of 2009 than in the corresponding quarter of 2008. In 2008 however, the two quarters that saw the most frauds identified were in the second half of the year, while in 2009 they were in the first half.

This may be a symptom of the economic climate (with people feeling that the recession was hitting hardest at the end of 2008 and the start of 2009), and turning to fraud in order to try and make ends meet or organised fraudsters becoming better at their trade. The third quarter of 2009 has been perceived by some as financially easier: leading to slightly

fewer recorded cases of fraud than the preceding quarter. Quarter 4 saw another increase, however, possibly due to the financial pressures generated by Christmas.

While it is often accepted across the fraud prevention community that fraud increases in times of recession, it would be naive to attribute this entirely to the financial crisis. There are other factors that could have contributed.

Many of the frauds identified will be attributable to opportunistic individuals who see fraud as a quick and easy way of acquiring goods, capital or services to which they are not entitled. This is especially true in times of recession - when those who are usually law abiding may feel themselves pushed down this route by financial hardship. The moral barriers to committing fraud are eroded further because the target for many of the frauds attempted (financial institutions, for instance) have been portrayed as being the 'villains of the piece' and responsible for the economic climate that is causing the potential fraudster the hardship. Conversely, a significant proportion of the frauds was committed not by one-off opportunists, but by serious organised criminals. These include career criminals who are, in effect, professional fraudsters, and organised criminal groups where the members collaborate to ensure effective perpetration of multiple offences.

Unfortunately, there is no way of identifying just how many of the total frauds recorded can be attributed to these serious organised fraudsters. What we can say is that they will be much better at committing fraud successfully than an opportunistic individual. The opportunists are likely to have little or no knowledge of the processes and fraud prevention techniques employed by the organisations they are attempting to defraud. The organised fraudster's livelihood on the other hand *depends* on being able to 'beat the system'.

CHRISTMAS EFFECT

For most people, Christmas is an expensive time of year. Some have trouble meeting this increased expenditure and will look for ways of covering any shortfall; with a proportion turning to fraud. This change in the level of fraudulent activity in the months preceding the festive period is known as "The Christmas Effect".

2.2 Fraud by fraud type

Frauds identified by CIFAS Members are classified into one of six fraud types. The definitions of these fraud types can be found in the boxes interspersed throughout this section.

Table 2.2.1 shows the number of frauds of each fraud type identified in 2008 and 2009.

Fraud types

Table 2.2.1

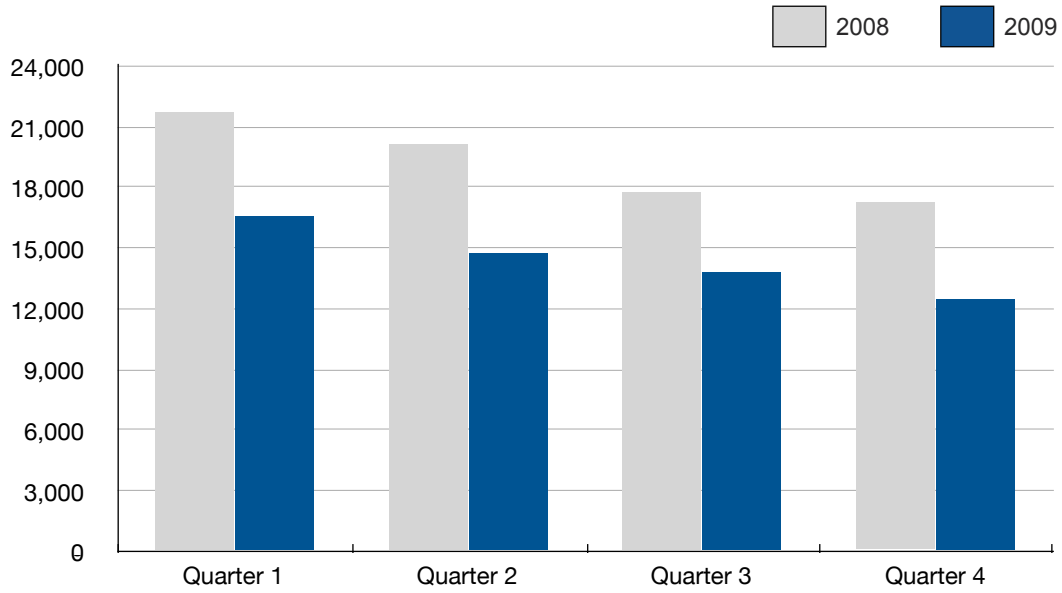
Fraud Type	2008	2009	% Increase
Application Fraud	77,023	57,825	-24.93%
False Insurance Claims	433	670	54.73%
Identity Fraud	77,642	102,327	31.79%
Misuse of Facility Fraud	39,447	50,512	28.05%
Facility Takeover Fraud	19,275	22,387	16.15%
Asset Conversion Fraud	522	532	1.92%

Application Fraud

These figures demonstrate that all types of fraud, with the exception of application fraud, saw an increase in 2009 compared with 2008. The number of application frauds (where the name on the application is the genuine name of the person applying) has decreased by almost a quarter. This is in contrast to identity fraud (where the person applying used either the name of an innocent victim or an entirely fictitious name) which increased by over 30%. The true scale of application fraud may be disguised by the current economic conditions. Not only are many unwilling to apply for credit, but due to tighter lending criteria, many applications are rejected outright before the fraud checking stage.

Application Fraud

Chart 2.2.1



False Insurance Claims

The biggest percentage increase between 2008 and 2009 was seen in the number of false insurance claims identified. This grew by over 50% - albeit from a modest starting point. It is likely that the increase in this type of fraud, especially, is a symptom of the recession. The nature of insurance itself is inclined to lead *some* people to feel a false sense of entitlement: 'if I've been paying for years without making a claim, isn't it about time I got something back?'. This can also lead to people inflating genuine claims, staging accidents in order to make claims, or pretending an event took place when none did. The presence of organised criminal networks, in the latter two, however, cannot be ignored.

Chart 2.2.2 shows that both 2008 and 2009 saw the same pattern of cases identified over the course of the year. In both years the numbers increased quarter on quarter until the final quarter of the year, which saw a decline. 2009, though, saw this effect magnified by a greater overall number of cases.

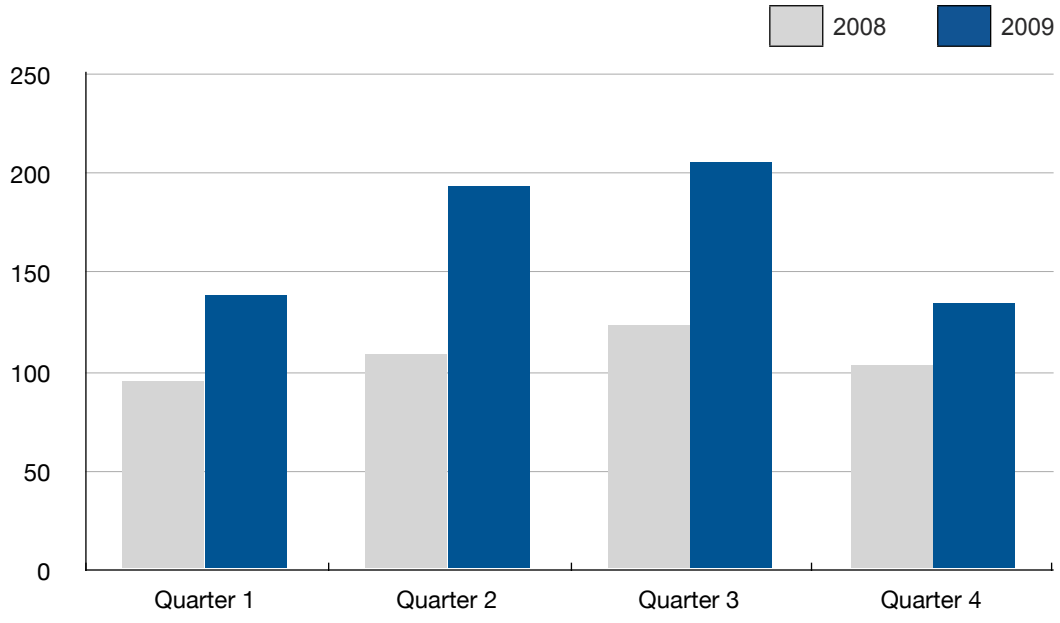
Application Frauds / False Insurance Claims

Fraud Type	2008	2009
Application Frauds	77,023	57,825
False Insurance Claims	433	670

Application Frauds/False Insurance Claims relate to applications or claims with material falsehoods (lies) or false supporting documentation (where the name given has not been identified as false).

False Insurance Claims

Chart 2.2.2



Identity Fraud

There are various reasons for the increase in identity fraud. There is the belief that credit is hard to come by, which means that some people do not think that they are 'creditworthy' enough to obtain the products and services they want, so they use the name and details of someone whom they think will pass a credit score.

Identity fraud has received considerable media attention in recent years, with plenty of advice for the public about keeping their identity safe and reassurances that victims of identity fraud will not be held liable for debts amassed in their name. This has had the positive effect of making people more aware of the value of their identity. The other side of this is that some people feel that using someone else's identity is acceptable because their 'victim' will not be held accountable. This leads to people using the personal details of their friends or family, as they already know all the information that is required to open new facilities, especially over the internet where there is no requirement to provide identity documents.

This increased awareness among consumers will also have had the effect of encouraging them to check their credit file regularly, thereby bringing to light accounts that have been opened successfully but fraudulently in their name. Identity fraud is well-known to be a preserve of organised criminals and criminal gangs. Compromised identity details are sold over the internet. Gangs use collusive staff within organisations to steal personal data and compromise identities. The organised fraudster will also make use of a number of tools (often legitimate) for their own ends, in order to maximise the chances of their fraud being successful.

Chart 2.2.3 shows that each quarter of 2009 saw more cases identified than any individual quarter of the previous year. The quarter on quarter upward trend seen in 2008 has generally plateaued in 2009, although at a higher level than in 2008. The exception is in Quarter 4 of 2009, which saw an increase that could, once again, be attributed partially to 'the Christmas Effect'.

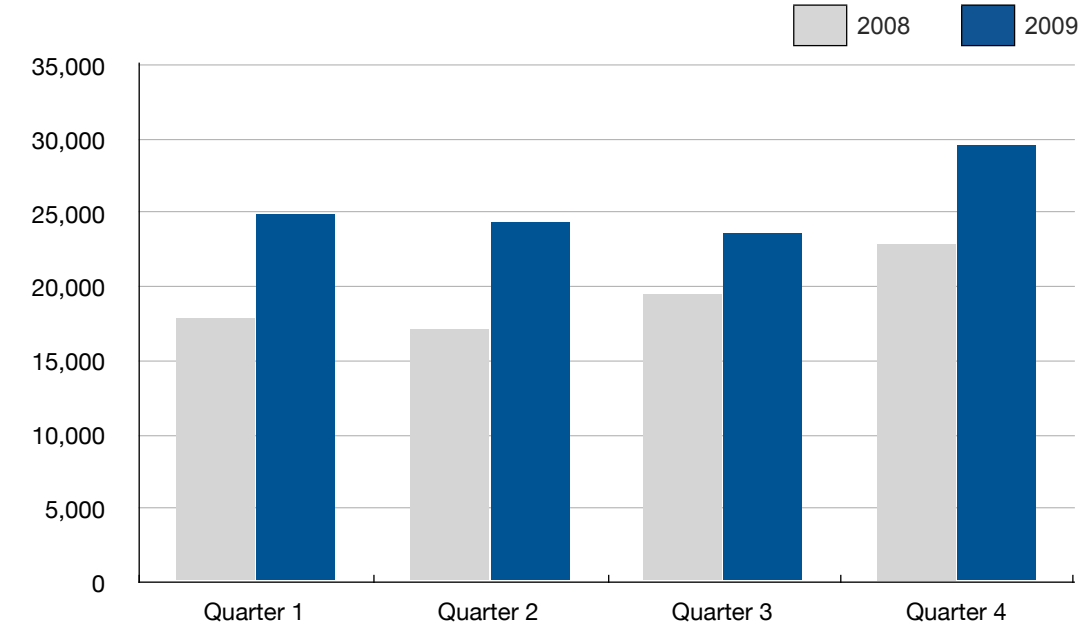
Identity Fraud

Fraud Type	2008	2009
Identity Fraud	77,642	102,327

Identity Fraud will include cases of false identity (the use of an entirely fictitious identity) and identity theft (stealing the identity of an innocent victim).

Identity Fraud

Chart 2.2.3



A bright e-IDea...

The National Fraud Authority (NFA) estimates that fraud costs the UK economy £30.5 billion annually. ID from Tracesmart, a leading electronic identity verification (e-ID) service, will protect you from this threat and allow you to:

- **Instantly identify genuine customers**
- **Streamline application processes**
- **Block suspicious transactions and applications**
- **Protect both your business and consumers from fraud**

Have a bright e-IDea; protect your business from fraud – call **029 2047 4150** today, for your free trial of ID from Tracesmart.

T: **029 2047 4150**
E: **info@tracesmartcorporate.co.uk**
www.tracesmartcorporate.co.uk

TRACESMART® CORPORATE

Misuse of Facility Fraud

Misuse of facility frauds increased by over 28% during 2009, on top of an increase of over 68% in 2008 compared with 2007. This can be attributed in part to the fraud and collections departments of organisations having more opportunity to identify these types of fraud. When there is less new business coming in, potential fraud losses have a more significant impact on the organisation's bottom line. In addition, more time is available to spend examining the continuing conduct of the account.

The current economic climate may have induced some people deliberately to misuse their accounts: writing cheques they know will bounce or running up bills that they have no intention of paying. There has also been growth in serious organised criminals paying people to launder funds through their bank accounts. Individuals are approached over the internet or in social situations, and convinced to allow criminals to use their account in return for money. Often the 'victims' find that funds that have been withdrawn from their account without a deposit being made, however, or that a deposit fails to clear, leaving the 'victims' with unauthorised overdrafts they cannot repay.

Chart 2.2.4 shows that the number of misuse of facility frauds identified in each quarter has declined over the second half of 2009, which could be the first sign that the relentless rise over the last couple of years is waning. If so, this could indicate that people feel that their economic circumstances are improving, and therefore they no longer need to abuse their own account. It also shows that the work put in by fraud prevention teams to identify these frauds has paid dividends: with the result that this line of attack is no longer as attractive to the fraudster. It could, however, mean that as lending increases, and attention is drawn to new accounts, frauds involving the deliberate misuse of facility are being unwittingly buried under the heading 'bad debt'.

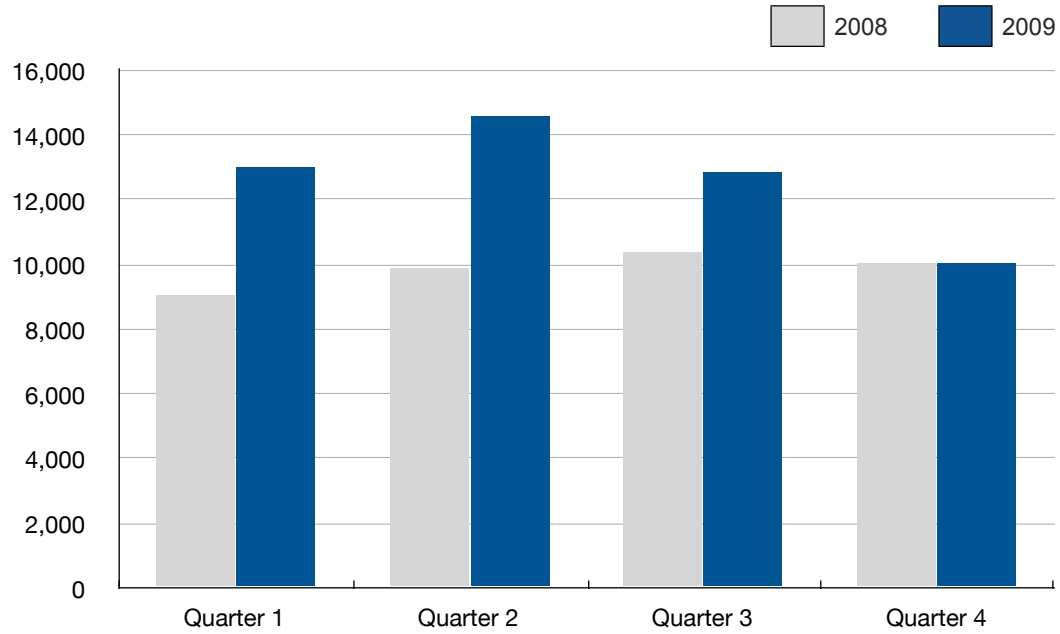
Misuse of Facility Fraud

Fraud Type	2008	2009
Misuse of Facility Fraud	39,447	50,512

Misuse of Facility Fraud occurs when an account, policy or other facility is used fraudulently.

Misuse of Facility Fraud

Chart 2.2.4



Facility Takeover Fraud

Facility takeover fraud has also continued to increase. A 207% increase in 2008 compared with 2007 has been followed by a further increase of over 16% in 2009. As with identity fraud, this can be partially attributed to:

1. opportunist fraudsters compromising the account of friends and family, safe in the knowledge that they will not be liable.
2. more organised fraudsters using the account and login details of innocent victims they have acquired through phishing attacks - (the use of spoof emails and websites designed to deceive the recipients into revealing their personal details, like user names and passwords) - or other means.

It is also possible that some are perpetrated by serious organised criminal gangs with the assistance of collusive employees in the organisations that hold the accounts. Those staff may be willing (paid for their trouble) or coerced (their assistance obtained by threats).

It can be seen from Chart 2.2.5 that the quarter on quarter increases seen during 2008 and the first quarter of 2009 have stabilised, with the number identified per quarter in 2009 more consistent than in 2008.

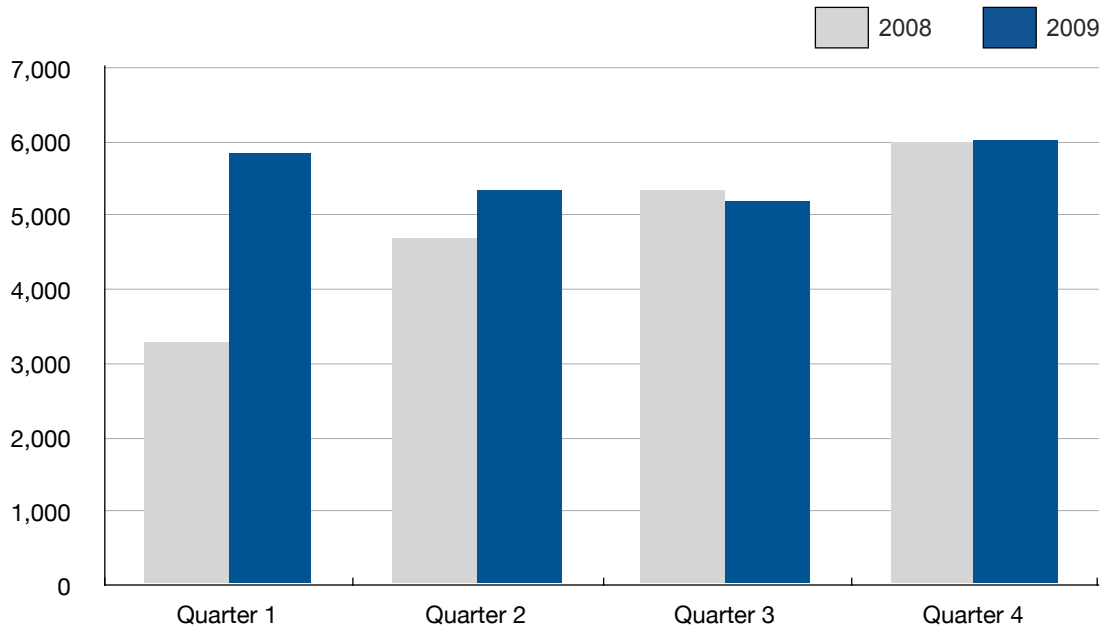
Facility Takeover Fraud

Fraud Type	2008	2009
Facility Takeover Fraud	19,275	22,387

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

Facility Takeover Fraud

Chart 2.2.5



Asset Conversion Fraud

The total number of asset conversion frauds has remained largely unchanged in 2009 compared with 2008, which is, to a certain extent, surprising. Asset conversion involves selling an asset to which the seller does not hold the title: in other words, selling something which isn't theirs. In most cases, this is a car on finance. It is a little surprising that there were not more of these cases in 2009 as this is a way for the fraudster both to obtain some cash and to dispose of an asset that they do not wish to continue to pay for. For people struggling financially in the current economic climate, this might start to sound like an attractive proposition.

The counter argument, however, is that this involves the fraudster parting with their car, which may be something that they are not prepared to do. In addition, the fraudster may wish to avoid the prospect of a debt-collector coming to visit to chase payment for a vehicle that has already been sold.

Chart 2.2.6 shows that the small percentage increase in cases seen in 2009 compared with 2008 actually hides a quarter on quarter increase in the number of asset conversions throughout 2009. This may indicate that, while not the first choice as a source of ready cash, people increasingly feel that selling their car (even when not entitled to do so) is a way of relieving their financial pressures.

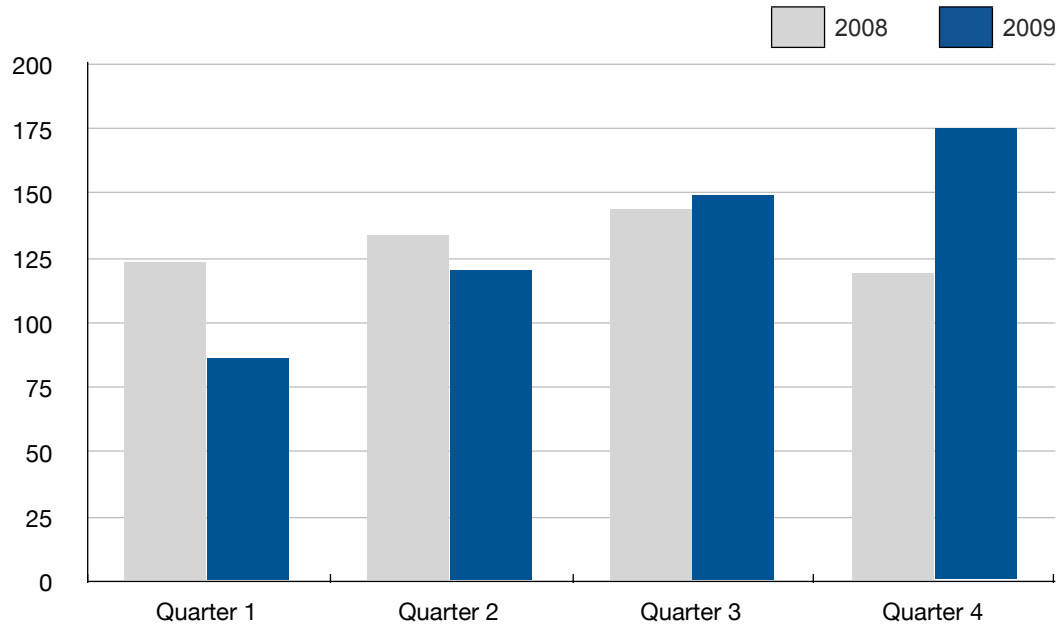
Asset Conversion Fraud

Fraud Type	2008	2009
Asset Conversion Fraud	522	532

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

Asset Conversion Fraud

Chart 2.2.6



2.3 Fraud cases by product group

Cases identified by CIFAS Members record the product the fraudster applied for, or was successful in obtaining. These products have been grouped into 10 categories for the purposes of comparison. Table 2.3.1 shows the number of cases identified by Members in 2008 and 2009, classified by the type of product that was involved in the fraud.

Fraud cases filed by product group

Table 2.3.1

Product	2008	2009	% Increase
Mail Order	17,562	38,718	120.46%
Communications	15,212	23,939	57.37%
Loans	14,290	6,653	-53.44%
Mortgages	2,998	3,004	0.20%
Bank Accounts	72,988	80,105	9.75%
Plastic Cards	70,423	63,396	-9.98%
Asset Finance	12,986	9,579	-26.24%
All-in-One	498	571	14.66%
Insurance	5,978	6,106	2.14%
Other	1,407	2,182	55.08%

Mail Order and Communications

Table 2.3.1 shows that the biggest increase in cases identified involved mail order accounts, where there were 120% more frauds in 2009 than there were in 2008. Communications products (mostly involving mobile telephone accounts) also saw a substantial increase, by over 57% in 2009 compared with 2008.

It is notable that these are products that are considered by the fraudster to be more 'easy access', and perhaps a quick and effective way of obtaining goods fraudulently. Yet the volume identified by CIFAS Members demonstrates that they are not as accessible as the fraudsters might have imagined. Both 2008 and 2009 show the same pattern - relatively stable volumes of fraud identified, but with a noticeable spike in the last quarter of the year.

This spike in the last quarter of the year comes with a backdrop of economic woes affecting retail sales in the run up to Christmas. This indicates that the public were still unwilling to spend money. Christmas is a time when spending is expected, however, and this can lead to the more unscrupulous seeking to get something for nothing.

Loans

The number of frauds relating to loans decreased by over 53% in 2009 compared with 2008. This is most likely a symptom of restricted lending, making this particular form of fraud a less attractive proposition. Fraudsters may feel that other products (e.g. mail order and communications accounts), present a greater chance of success and so they have migrated away from a product where applications attract a greater degree of scrutiny. In addition to this, those who would commit fraud in order to obtain a loan larger than they can afford but with the intention of repaying it, may be deterred by the idea of over-extending themselves in a time of uncertainty.

Mortgages

As signs of life returned to the housing market after the collapse during the recession, for the first time since 2006 there is a year on year increase in the number of mortgage fraud cases identified by CIFAS Members. This is evidence that the return of rising house prices is once again encouraging fraudsters back to mortgage fraud. For the serious organised fraudster, the greatest profit can be gained when the asset increases in value. This means that when house prices are declining, other forms of fraud may be more attractive, but this changes when property prices start to rise again.

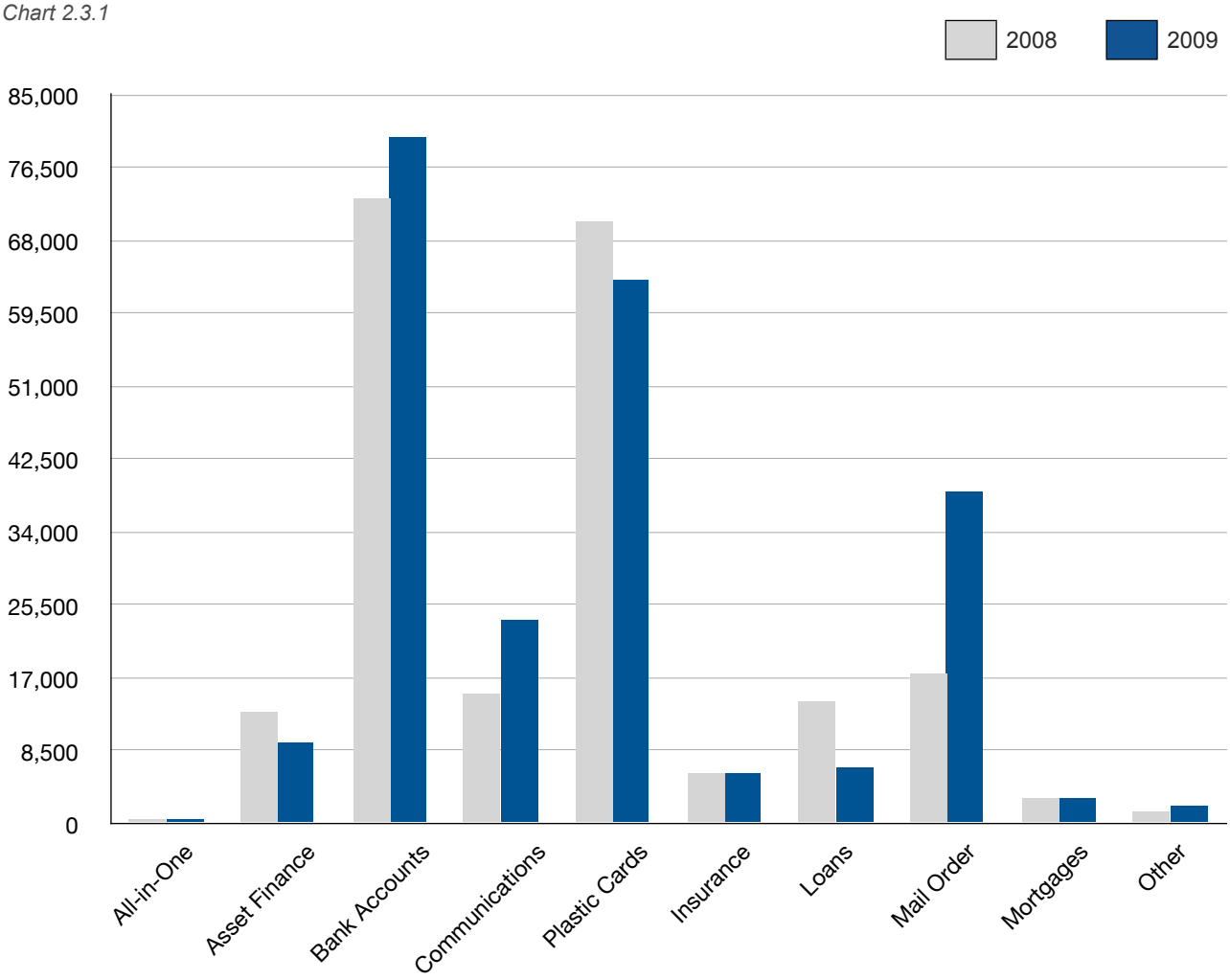
Most opportunistic mortgage fraudsters tell lies on their application to make themselves seem capable of repaying a mortgage that they may not be able to afford - but with the intention of repaying the mortgage and keeping the property. Their chances of doing this decline in times of recession, with the added danger that the value of the asset is declining as well. This makes the gamble of over-extending themselves not worth the risk. When house prices start to appreciate, however, (especially when there is encouragement for people to get on to the housing ladder before prices get too high) the dangers involved in financial over-extension seem smaller. So the inclination to tell some lies on an application resurfaces in order to secure a higher mortgage than they would otherwise get. The same fear of depreciating house prices will doubtlessly also influence the more organised fraudster.

Bank Accounts and Plastic Cards

There has been an increase of almost 10% in frauds involving bank accounts in 2009 compared with 2008, while there was a decrease of almost 10% in the number of frauds involving plastic cards. The reasons for this will be examined more closely in the sections relating to each product. (Please refer to sections 3.3 and 3.5)

Fraud cases by product type

Chart 2.3.1



Asset Finance

The number of frauds involving the financing of assets, most often cars, has declined by over 26% in 2009 compared with 2008.

In May 2009, the Government introduced the scrappage scheme for cars over 10 years old, in order to stimulate the motor manufacturing industry which had been in decline. This has successfully contributed to an increase in sales of new cars, and seems to have arrested the decline in the number of frauds relating to asset finance. This in itself, though, raises questions - if the number of cars being sold has increased over the second half of 2009, why has this not translated into a rise in the number of related frauds?

There are various possibilities. First, has the number of new sales translated into more applications for credit? There will be a number of people who will have taken the opportunity to buy a new car outright. Such purchases will therefore not be contributing to the number of applications for asset finance. As the amount of the finance required has been reduced, it may be that some people feel that the motor industry's desire to sell cars means that credit checking may be less stringent and therefore applicants believe they are more likely to be approved for finance. Because of this, they perceive that there is no need to tell the little lies that they might otherwise have deemed necessary to get the response that they want.

The counter argument to this is that there may be those who feel that if they don't take the opportunity to get a new car with the scrappage scheme now, they will have missed the boat and will be stuck with a vehicle that was worth potentially £3,000 (with some dealers' incentives) but is now back to being worth only a couple of hundred pounds. Those who are already overstretched, might feel it necessary to commit fraud on their application in order to secure finance. This, of course, only applies to those who commit fraud to obtain an asset that they have every intention of actually paying for (it's just that they and the asset finance company have differing opinions about their ability to do so).

The scrappage scheme will have very little effect on those fraudsters who have no intention of repaying the outstanding finance. If someone doesn't intend to pay back the money, especially if they have used another person's name to apply for the finance, then the value of the finance agreement will make very little difference. It's also worth mentioning that, given the criteria required to be eligible for scrappage (e.g. that the car needs to be owned by the current owner for the last 12 months), a fraudster who applied in someone else's name would probably have to steal their victim's car and registration documents as well as their identity!

2.4 Who is the fraudster?

Although there is no definitive identikit for a fraudster, examining the personal details of those individuals who have been identified as being involved in frauds can shed some light on the most common features.

Average age of fraudsters

Table 2.4.1

	2008	2009
Average Age	42.63	39.28
Average Age (Men)	43.00	39.50
Average Age (Women)	41.89	38.78

Gender of fraudsters

Table 2.4.2

	2008	2009
% Men	66.29%	68.96%
% Women	33.71%	31.04%

Tables 2.4.1 and 2.4.2 show that between 2008 and 2009 there has been a reduction in the average age of those involved in fraud cases, and that the proportion of men involved has increased. Those involved in fraud cases are mostly men, who account for over two thirds of the individuals involved. The average age of men involved has reduced from 43 years to 39.5 years. The average age of women involved has reduced by just over 3 years to 38.75 years. So male subjects in fraud cases, on average, continue to be older than their female counterparts, but the gap is narrowing.

This implies that it is men who are more driven to commit fraud when times get tighter. It may be that they are fulfilling the 'traditional' male role of the bread winner and therefore turning to more desperate measures to provide for their families. Alternatively, it could be that men are just less willing to go without the luxuries that they have come to expect in more affluent times, and see committing fraud as a way of continuing to obtain them. Equally it may show that men are also more traditionally those involved in organised crime.

Average age and gender distribution of fraudsters by product group

Table 2.4.3

	Average Age					Gender Distribution			
	2008		2009			2008		2009	
	Men	Women	Men	Women		Men	Women	Men	Women
Asset Conversion Fraud	40.18	37.11	37.85	36.02		78.95%	21.05%	79.14%	20.86%
Application Fraud	36.78	35.71	35.99	35.12		64.86%	35.14%	66.03%	33.97%
False Insurance Claim	40.86	39.35	39.28	39.01		62.21%	37.79%	64.90%	35.10%
Facility Takeover Fraud	51.69	47.08	47.58	44.71		66.54%	33.46%	67.84%	32.16%
Identity Fraud	46.47	44.95	45.89	45.16		69.26%	30.74%	68.11%	31.89%
Misuse of Facility Fraud	33.24	32.03	31.67	30.79		72.07%	27.93%	72.00%	28.00%

Table 2.4.3 shows that men are increasingly involved in most types of fraud apart from misuse of facility fraud, where the distribution was almost identical and identity fraud, where the proportion of women increased. Average ages decreased across the board, apart from women involved in identity fraud. The fact that in 2009, the proportion and average age of women involved in identity fraud cases has become more aligned to the men could be a sign that fraudsters are focusing less on their traditional victim of impersonation, the middle aged man, and seeing women as viable targets for impersonation as well. It could also be a sign of a greater number of identity frauds being perpetrated by organised fraudsters who are making applications in greater volumes - using data that has been obtained *en masse* through avenues such as phishing, use of spyware and bulk data thefts. The individuals whose personal details are compromised in such a manner are unlikely to be as deliberately targeted, as cases where fraudsters had carefully picked the individual that they wished to impersonate.

2.5 Fraud maps - 2009

The maps on the following two pages show:

- the location of the addresses actively involved in the fraud cases identified by CIFAS Members within the UK in 2009.('Actively involved' means that any previous addresses not being used by the fraudster have not been included)
- the location of the addresses involved in identity fraud in 2009.

As the maps will show, they have been organised by the county boundaries in existence in 1995: prior to the introduction of unitary authorities and reclassification of county boundaries. Inset boxes for 2008 are included for comparison in both cases. These maps are a result of a collaboration between CIFAS and Ordnance Survey.

Addresses involved in fraud in 2009
(p18)

The number of identified fraud cases increased by 10% in 2009 compared with 2008, but there are few visible differences in the location of those frauds between 2008 and 2009. Unsurprisingly, the main centres for fraudulent activity are in areas of high population density: most noticeably the South East and the North West. These areas cover London and its commuter belt, and Manchester and Liverpool and the surrounding areas.

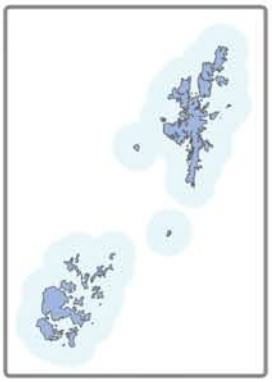
In the Midlands and towards the North, there has been some off-setting between Nottinghamshire and North and South Yorkshire; the number of frauds in the former decreasing while the level in the Yorkshire counties increased. The number of frauds identified in the Lothian region of Scotland (which includes Edinburgh) perhaps surprisingly saw a reduction in fraud levels in 2009 compared with 2008. Both East and West Sussex on the South coast saw increases as did Norfolk in East Anglia, although this was not reflected in neighbouring Suffolk, which continues to experience relatively low levels of fraud.

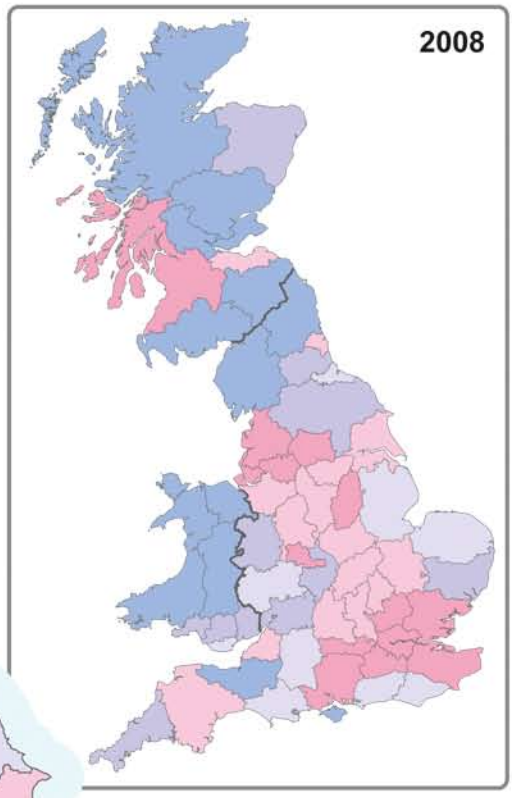
Identity fraud in 2009
(p19)

There has been a significant increase in the number of cases of identity fraud recorded in 2009 compared with 2008, and this is illustrated by the increase in the red hues on the map. The main identity fraud hotspots in 2008 were London, the South East and the North West. In 2009, it is noticeable that it has also leached into other areas, with a noticeable concentration of high levels of Identity Fraud occurring along the M1 corridor.

The South West has not been immune to this bleed effect either. In 2008, only Avon - which includes Bristol, the major population centre of the South West - experienced the highest levels of identity fraud. In 2009, however, this high level of identity fraud has moved west from the Hampshire/Berkshire/Oxfordshire area to include Dorset, Wiltshire and Devon. Even Somerset (which previously saw relatively low levels of identity fraud) has seen a noticeable increase in 2009. One of the areas relatively unaffected by identity fraud has previously been Wales and the bordering English counties (e.g. Hereford and Worcester and Shropshire). The increase experienced in the South West of England and M1 corridor, sees the Wales/English border area surrounded by increases in identity fraud. What we can see, also, are increasing levels in South Wales and Clwyd, leaving only Powys in Central Wales and Dyfed and Gwynedd in the West still experiencing the lowest levels of identity fraud.

Addresses involved in fraud in 2009





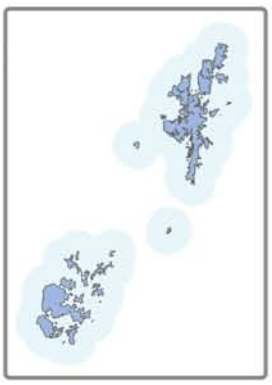
Number of times that addresses have been actively involved in frauds recorded by CIFAS Members

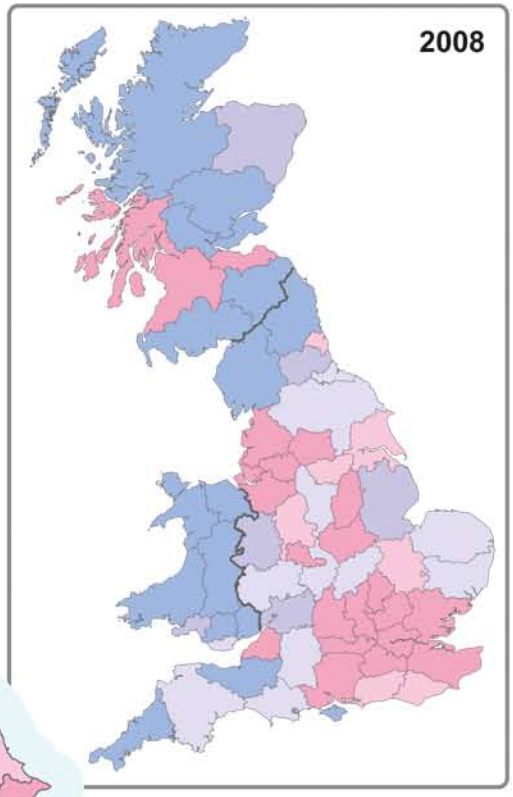
- 3,301+
- 2,001 to 3,300
- 1,401 to 2,000
- 801 to 1,400
- 1 to 800

County boundaries 1995 - prior to the introduction of Unitary Authorities

Source: CIFAS 2010

Identity fraud in 2009





Number of times that addresses have been actively involved in cases of identity fraud recorded by CIFAS Members

- 801+
- 701 to 800
- 401 to 700
- 301 to 400
- 1 to 300

County boundaries 1995 - prior to the introduction of Unitary Authorities

Source: CIFAS 2010

3. Fraud by Product Group

3.1 All-in-one Frauds

An all-in-one product is one where a group of financial products is offered together and interact together (for instance a bank account off-setting a mortgage).

All-in-one frauds by fraud type

Table 3.1.1

Fraud Type	2008	2009	% Change
Application Fraud	172	194	12.79%
Facility Takeover Fraud	16	109	581.25%
Identity Fraud	246	189	-23.17%
Misuse of Facility Fraud	64	79	23.44%
Total Frauds	498	571	14.66%

Application fraud shows surprising rise

The number of all-in-one frauds increased by almost 15% in 2009 compared with 2008. A large proportion of this increase can be attributed to a steep rise in application fraud on these products.

In contrast to the trends seen across all other products, there were more application frauds and fewer identity frauds where the product was an all-in-one product. It could be that the nature of the product (i.e. the combination of financial services involved) means that the figures display aspects of the frauds that are affected by the various products involved. For example, the low level of identity fraud is probably a reflection of the low level of identity fraud typically seen in mortgage fraud. Unless the fraudster is a serious organised fraudster (attempting to obtain property for profit or to launder funds), as opposed to a fraudster who wants to live in a house that they are unlikely to be able to afford, then there is little point in using a false identity.

The increase in the number of facility takeover frauds is probably related to the bank account aspect of all-in-one frauds. Increasingly, bank accounts are being taken over by fraudsters in order to take unauthorised payments out of those accounts. Fundamentally, the fraudster is stealing money - they're just doing it electronically.

Are fraudsters seeking new targets?

The number of all-in-one frauds is relatively small, which makes the findings here less significant than those seen for other products. It gives, though, a good idea of the fraud behaviour that CIFAS Members are experiencing in relation to this product. The increases could, therefore, also be an indication that fraudsters are turning to this type of product. As the fraud controls on the more traditionally targeted products (bank accounts, credit cards etc) are getting tighter, fraudsters are turning their attention to what they *perceive* (erroneously) to be a 'softer target'.

Economic hardship drives change in fraudster behaviour

When application fraud was identified for an all-in-one product, the fraudster was most frequently attempting to hide adverse credit information (by failing to disclose an address that they were required to provide). In 2008, this accounted for 65% of application frauds whereas in 2009 this has increased to over 74%. This increase is probably a reflection of the indebtedness of the UK population as well as the economic climate.

Having debts to repay makes it less likely that the individual is able to keep up with those repayments during adverse

economic conditions. Inability to keep up with repayments means that the person will have adverse credit information recorded on their credit file. In turn, this leads to a desire to hide that fact when applying for new products - most commonly hoping that if they don't tell a lender about an address associated with the adverse information, then the lender won't find out.

> "Identity fraudsters prefer to make their applications over the internet, where there is a distance between them and their crime"

Another notable change is that in relation to all-in-one products there were far more instances of someone trying to hide adverse credit information by applying using an alias. This typically means married women applying in either their married name or maiden name, depending on which name the adverse credit information is in. This accounted for 5% of application fraud cases in 2008, but was up to 14% in 2009.

To impersonate or not to impersonate?

Surprisingly, in cases of impersonation related to all-in-one products, the fraudster was more likely to commit previous address fraud as opposed to current address fraud in 2009. Previous address fraud is less sophisticated than current address fraud and less likely to be successful, so in recent years the trend in identity fraud generally has been towards current address fraud.

There is a clear distinction in the fraudster's preferred application channel between identity fraud and application fraud cases. In cases of application fraud, the fraudster is far more willing to walk into a branch and make the application in person. Identity fraudsters prefer to make their applications over the internet, where there is a distance between them and their crime. One of the main reasons for this will be that someone applying in their own name, even if they are lying about other aspects of their application, will have all the appropriate identity documentation. An identity fraudster, on the other hand, may not have this and, therefore, will look to use a channel that uses electronic identity verification, even if this means that they have to know more information about their victim.

This distinction has become more noticeable in 2009 compared with 2008. In 2008, just under 50% of application frauds for all-in-one products were made face-to-face, and 30% via the internet. In 2009 this has changed to over 52% face-to-face with just over 23% via the internet. For identity fraud, 2008 saw 78% attempted over the internet and 10% face-to-face, while 2009 saw 89% attempted via the internet and under 5% attempted in person. The majority of the rest of the attempted application frauds and identity frauds were made over the phone. Charts 3.1.1 and 3.1.2 (overleaf) clearly illustrate this difference in the preferences of application and identity fraudsters for an all-in-one product.

DEFINITIONS

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 voter's roll at that address and their payment performance information is all at that address). The fraudster must be able to gain access to the victim's mail to intercept the relevant documentation.

Previous Address Fraud

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

DEFINITIONS

Previous Occupier Fraud

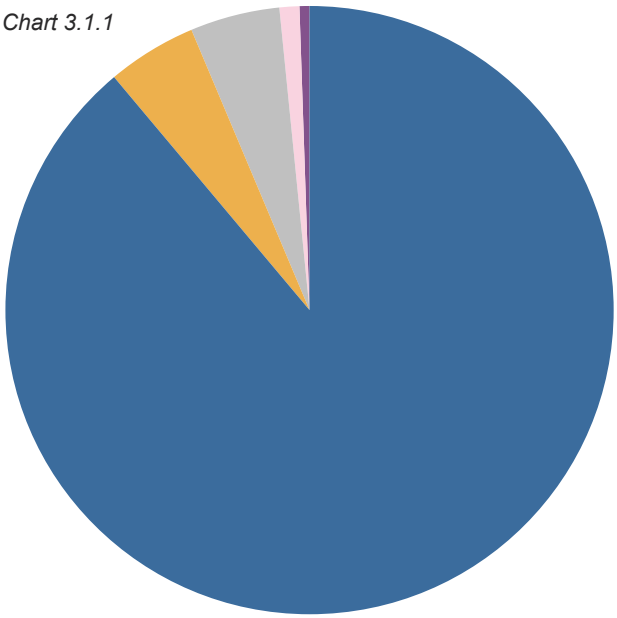
Typically, this is carried out by opportunist fraudsters who have moved into their victim's previous address. It occurs when the fraudster applies in the name of an innocent victim who has recently moved. The fraudster may well not know where the victim has moved to, so uses the victim's previous address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

False Identity

The fraudster applies using an entirely fictitious identity.

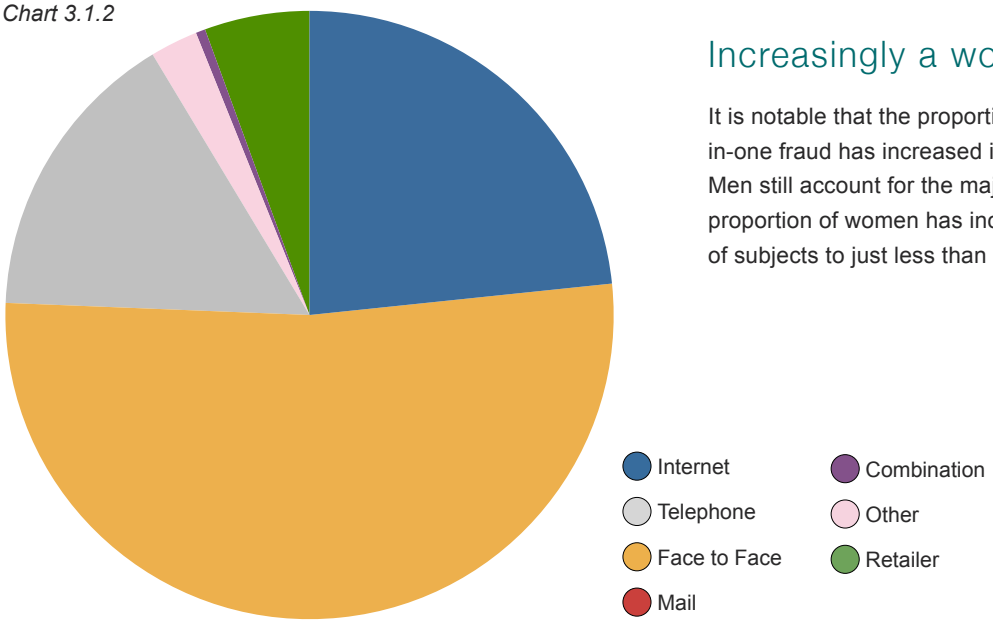
All-in-one Application Channel - Identity Fraud 2009

Chart 3.1.1



All-in-one Application Channel - Application Fraud 2009

Chart 3.1.2



The self-employment conundrum

The number of application fraudsters for all-in-one products who claim to be self-employed increased in 2009 compared with 2008. In 2008, just over 9% of men and just under 6% of women who were identified as application fraudsters claimed that they were self-employed, while in 2009 this has risen to just under 16% of men and just over 12% of women. This could be due to more people who are genuinely self-employed feeling that they have to commit application fraud to make themselves appear more creditworthy in order to be accepted under present lending conditions.

Another contributory factor, however, will be that as unemployment increases, so does the number of people who feel that an easier way to cover up their lack of employment is to claim to be self-employed. The number of identity fraud cases involving the self-employed remains low - given that most people believe that being self-employed makes it harder to obtain credit - so the self-employed do not generally make the most obvious targets for an identity fraudster.

Increasingly a woman's game?

It is notable that the proportion of women involved in all-in-one fraud has increased in 2009 compared with 2008. Men still account for the majority of subjects, but the proportion of women has increased from just over 28% of subjects to just less than 37%. (See table 3.1.2)

Gender distribution by fraud type

Table 3.1.2

	2008		2009	
Fraud Type	**% Male**	**% Female**	**% Male**	**% Female**
Application Fraud	65.00%	35.00%	61.04%	38.96%
Facility Takeover Fraud	63.33%	36.67%	52.04%	47.96%
Identity Fraud	73.87%	26.13%	70.59%	29.41%
Misuse of Facility Fraud	81.82%	18.18%	75.34%	24.66%
Total Frauds	71.81%	28.19%	63.42%	36.58%

In relation to all-in-one products, all types of fraud have seen an increase in the proportion of women involved, but particularly in the area of facility takeover fraud, where the distribution between men and women is close to being even (although the number of facility takeover cases was very low in 2008). The increase in the number of female victims of identity fraud indicates that the fraudsters are concentrating less on the 'typical' victims: men in their 40s who are perceived to be settled in their home life (married, good income, own their home) and are therefore 'good' identities for the fraudster to try and use. This could be to do with the increasing social standing of women (meaning that fraudsters also see women as equally 'good' identities to target) or it could be a reflection of the origin of the compromise of the identity being abused. If the fraudster is using volume data then it is more likely that victimisation is random and therefore a greater reflection of the distribution of the population generally.

Finally the increase in the proportion of women involved in application fraud and misuse of facility fraud is most likely to be a reflection of the economic conditions and that, when times get tighter, women are increasingly likely to resort to "a little lie here, a little bounced payment there" to address their financial problems.

All-in-one subjects average age (by fraud type)

Table 3.1.3

	2008		2009	
Case Type	**Men**	**Women**	**Men**	**Women**
Application Fraud	36.12	35.80	35.36	36.24
Facility Takeover Fraud	43.53	43.64	49.87	49.08
Identity Fraud	45.86	44.62	46.12	47.31
Misuse of Facility Fraud	34.39	38.75	33.11	32.33
Total Frauds	42.23	41.28	42.70	43.76

The average ages of both men and women involved in all-in-one fraud is increasing, although more so for women than men. (See Table 3.1.3)

The average age of the male fraudster involved in application fraud and misuse of facility fraud has actually decreased while the age of those involved in identity-related crime has increased. Identity-related crimes have also seen the biggest average age increase for female subjects, which adds credence to the view that identity fraudsters (be they stealing an identity to open a new account or compromising an existing account) are targeting those that are the most likely to yield the greatest gains for their effort. In the cases of facility takeover, this suggests a more organised approach, involving collusive or coerced employees in order to target the 'best' victims.

3.2 Asset Finance Frauds

Table 3.2.1 shows the types of fraud that occurred in relation to asset finance in 2008 and 2009.

Asset Finance frauds by fraud type

Table 3.2.1

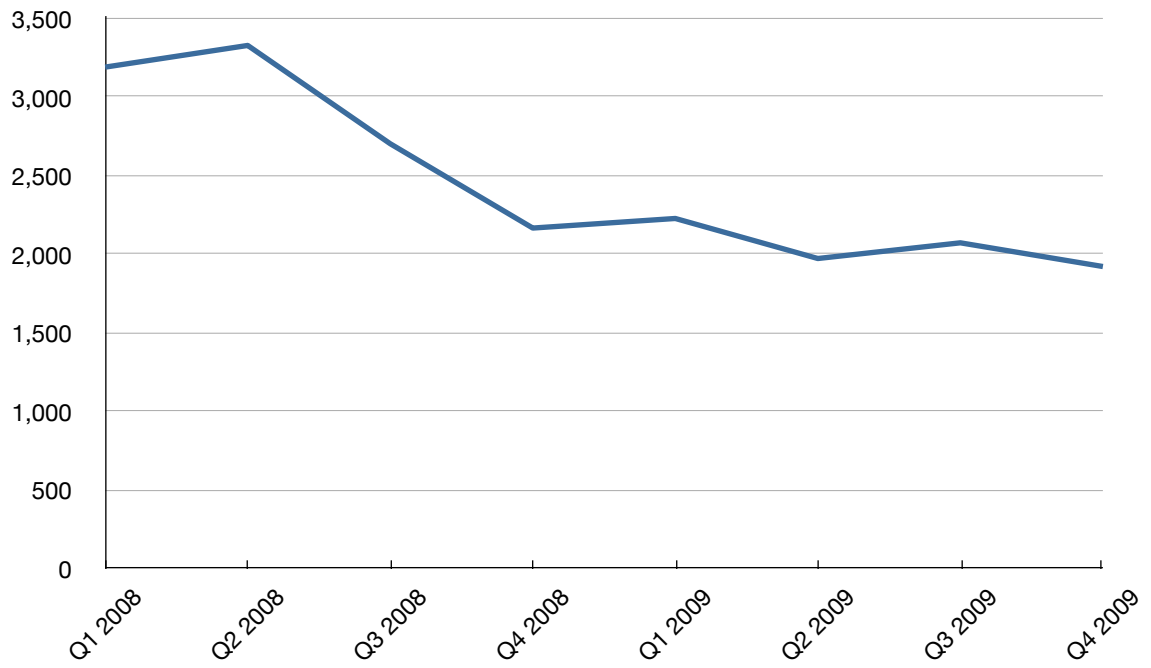
Fraud Type	2008	2009	% Change
Asset Conversion Fraud	521	526	0.96%
Application Fraud	11,393	8,196	-28.06%
Identity Fraud	766	479	-37.47%
Misuse of Facility Fraud	306	378	23.53%
Total Frauds	12,986	9,579	-26.24%

Application and identity fraud decrease

The level of application fraud for asset finance has declined in line with the downward trend in application fraud seen across all other product groups. Levels of identity fraud, however, have also declined by over a third, which is notably at odds with the levels of identity fraud seen across all other products. As discussed earlier (see page 15), the Government's scrappage scheme has boosted new car sales in the second half of the year, but this is unlikely to make identity fraud for car finance more attractive.

Asset Finance Application Fraud in 2008 and 2009

Chart 3.2.1



Asset Finance cases by fraud type

Chart 3.2.2

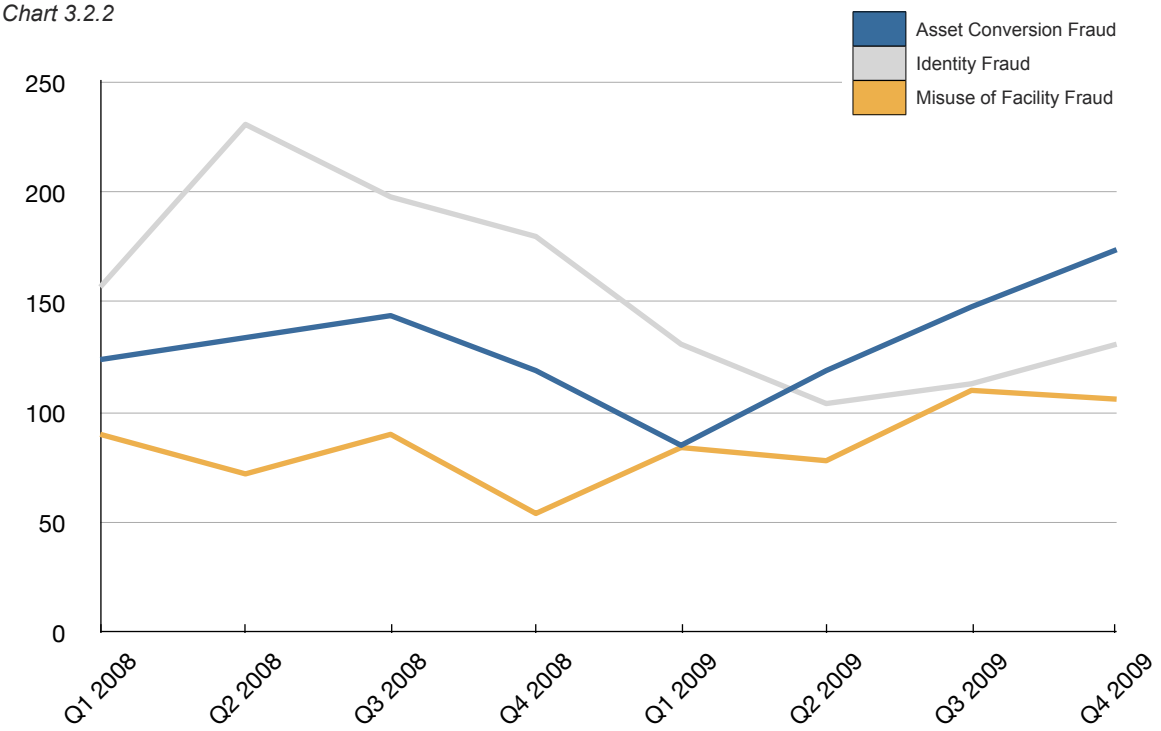


Chart 3.2.1 shows the number of asset finance application fraud cases identified during 2008 and 2009, and demonstrates that the decline in cases slows in the second half of 2009, after scrappage was introduced.

Chart 3.2.2 shows the other fraud types.

Signs of financial desperation driving asset finance fraud

The number of asset conversion cases (where the fraudster sells an asset that is still owned by the finance company) increased sharply in 2009 after a substantial decline in the second half of 2008. Misuse of facility cases have been increasing steadily since the last quarter of 2008. These frauds could be attributable to the increasingly desperate. Those who can no longer afford the repayments on their car finance may choose both to offload the asset (and make some cash into the bargain) or fraudulently try to avoid payment or continue payments with false instruments (e.g. cheques that they know will bounce or transfers that they know will not go through).

Asset finance organisations have identified that cloned, third-party credit cards have become an increasing problem in this area. Where a cloned card has been used, it is evidence of a more premeditated fraud carried out by a serious fraudster. The fraudster has obtained a cloned card in order to make a payment that will be charged to someone else's account.

The preserve of the organised fraudster

The decrease in identity fraud relating to asset finance could be attributed to more stringent enforcement of the requirement for dealers not to release a car on finance without seeing the driving licence with the correct current address on it. This requirement means that, where a fraudster is able to get hold of the genuine person's driving licence, they are unlikely to be able to use it unless they physically resemble the victim, or (in the case of old style paper licences) can pass for a similar age. It also argues that the identity frauds being committed are increasingly the preserve of the serious organised fraudster who has access to high quality false documentation.

In 2008, the most common identity fraud seen by asset finance organisations was previous address fraud, where the fraudster pretends that the victim has just moved. In 2009, the most common type of fraud was current address fraud, where the fraudster uses the victim's genuine address as the current address on the application. Current address fraud, because it involves more use of the victim's true details, is generally more likely to be successful. It is, however, more difficult to perpetrate as it requires the fraudster to plan more and use more tools to facilitate the crime (such as redirecting mail). The increased effort and planning involved in current address fraud means that there it is a greater likelihood, again, that it is being perpetrated by organised career criminals.

3.3 Bank Account Frauds

The number of bank account frauds can be seen in Table 3.3.1.

Bank Account cases by fraud type

Table 3.3.1

Fraud Type	2008	2009	% Change
Application Fraud	34,039	26,822	-21.20%
Facility Takeover Fraud	729	4,051	455.69%
Identity Fraud	13,832	14,661	5.99%
Misuse of Facility Fraud	24,388	34,571	41.75%
Total Frauds	72,988	80,105	9.75%

Bank accounts the target for account hijackers

The number of facility takeover frauds on bank accounts increased dramatically, from less than 1,000 cases in 2008 to well over 4,000 in 2009. Facility takeover allows the fraudster to plunder the bank account of funds and in over 87% of cases in 2009, the fraud involved unauthorised electronic payment instructions. Many of these cases are likely to be perpetrated through the fraudster managing to deceive the innocent victims into revealing their personal details (e.g. phishing attacks). Another possibility is that, while a data breach - itself - is nothing new, the levels of sophistication used by organised criminals trading details online are. This may, therefore, equally impact upon the figures. Alternatively, some may have been facilitated by a collusive member of bank staff.

The number of misuse of facility cases has also increased significantly. This can be attributed as much to the number of people who are doctoring cheques as it can to those who allow their accounts to be used to launder funds or as a repository for the proceeds of unauthorised transfers out of accounts that have been taken over. This means that there is a connection between the number of accounts being taken over and the number of accounts that are being fraudulently misused. It should be considered, however, that there are more destinations for a payment from a compromised account than another bank account (paying a bill, for example).

It is interesting that, for the first time, 2009 saw more misuse of bank account frauds than there were application frauds for bank accounts.

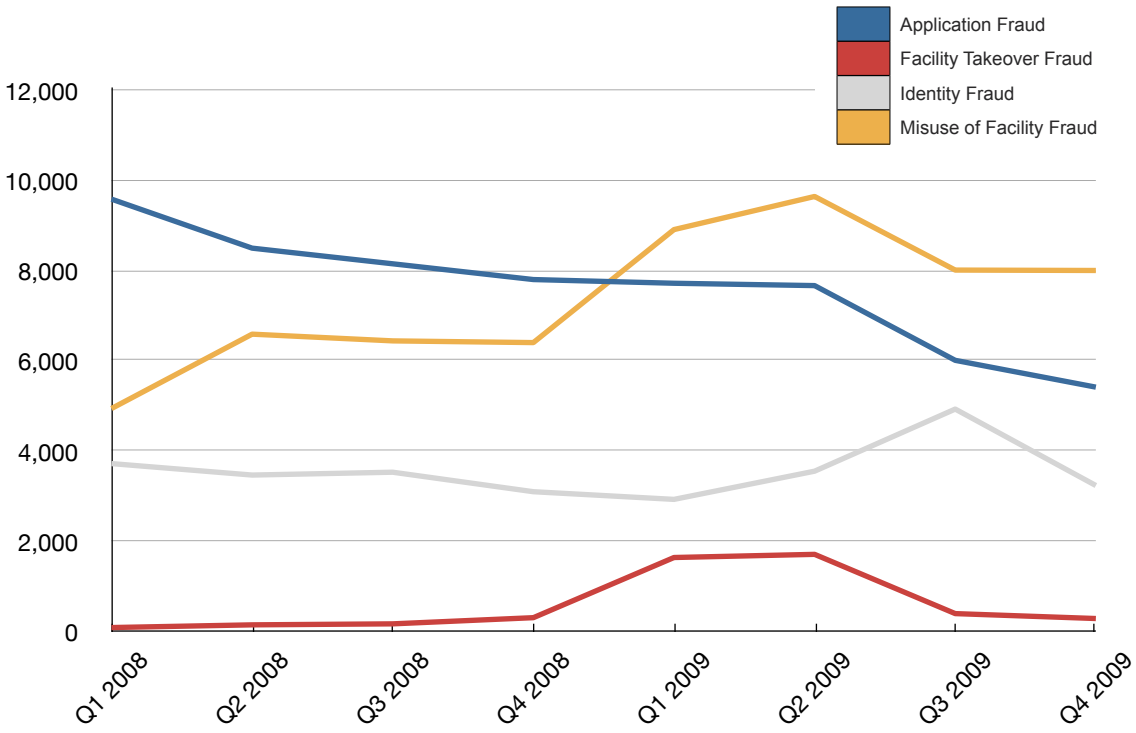
Chart 3.3.1 shows that the decline in bank account application frauds that started at the beginning of 2008 has continued. It is noteworthy that both misuse of facility frauds and facility takeover frauds saw big increases in the first half of 2009, before seeing more 'normal' levels resume in the second half of the year. This reinforces the idea that these two fraud types go hand in hand.

More bank account identity fraudsters target the victim's actual address

The nature of identity fraud cases relating to bank accounts in 2009 was somewhat different from those in 2008. In 2008, the most common identity crime was using an entirely fictitious identity. This accounted for over a quarter of the identity frauds. In 2009, this fell to less than 15% of cases. In its place, the number of current address frauds, using the victim's genuine address, increased from less than 24% of cases to almost 36%. As with other products seeing similar patterns, this can be an indicator of an increase in the organised element due to the sophistication of the crime - especially when the product involved is a bank account. As well as allowing the fraudster to make use of any cheque book and overdraft facilities, bank accounts allow the criminals to move and access the proceeds of other crimes (such as transfers from hi-jacked accounts or benefit fraud) without the trail leading directly to their door. Recent police investigations have brought to light an instance of the proceeds of an elaborate fraud being laundered through hundreds of UK bank accounts.

Bank Account cases by fraud type

Chart 3.3.1



Opportunistic fraud on bank accounts still a threat

The number of previous address frauds (where the fraudster essentially claims the victim has just moved) and previous occupier fraud (where the fraudster makes an application using the address that the victim has just moved out of) both account for a lower proportion of bank account identity fraud cases in 2009 than they did in 2008. Previous address fraud reduced from almost 19% of cases in 2008 to less than 13% in 2009.

The majority of previous occupier frauds tend to be carried out by the new tenants of the property that the victim has just moved out of, and so is very opportunistic: particularly if things like utility bills (a commonly used proof of address) are still in the victim's name. The advantage for the fraudster (of making the application(s) before the victim has had a chance to take themselves off the voters' roll and change addresses on their accounts) is that it still appears to the bank that the victim is living at that address. This explains why this type of fraud, in real terms, increased in number in 2009, even if it accounts for a lower proportion of the total. Previous address fraud, on the other hand, is more premeditated (the fraudster is more likely to select the victim as opposed to having the victim's details fall into their lap) but does not have the advantage of looking realistic to the bank.

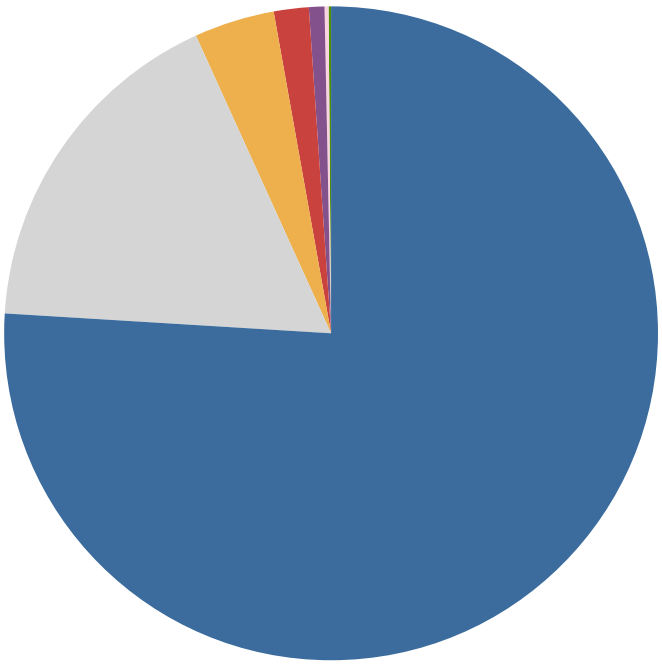
Internet fraud increases

(Please refer to Charts 3.3.2 and 3.3.3)

Identity related bank account frauds (identity fraud and facility takeover fraud) are increasingly perpetrated via the internet. In 2008, 68% of identity frauds and a little over 21% of facility takeovers were perpetrated online. In 2009 this increased to 74% of identity frauds and nearly 76% of facility takeovers. In both of these fraud types, attempts made by telephone have declined - especially in facility takeovers where telephone attempts accounted for over 71% of cases in 2008 but only 17% in 2009. In the past, fraudsters believed that they would be able to talk their way around a telephone operator but, as the knowledge of this type of fraud has increased, so have the controls that prevent it. With attempts over the internet, the likelihood is that the fraudster has obtained the relevant login details from a source outside the bank's control e.g. phishing attacks. Also, as the number of people who have internet access to their accounts has increased, so has the number of potential victims for the fraudsters who specialise in taking over accounts online.

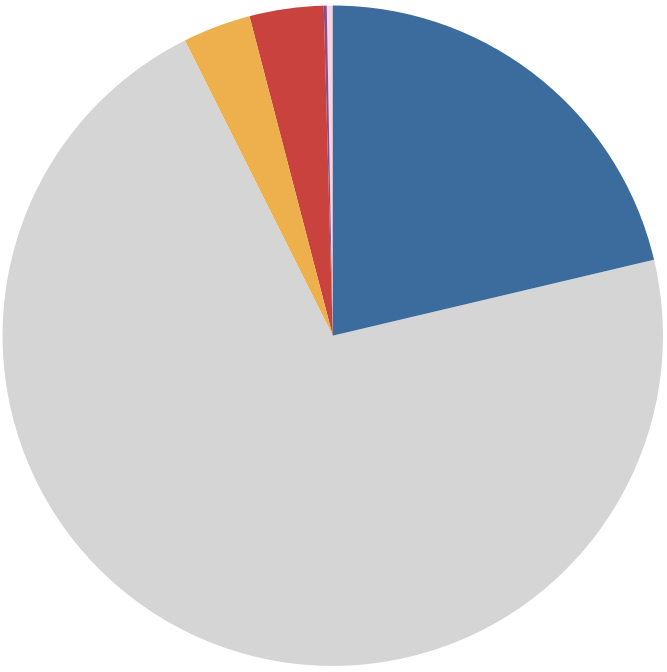
Bank Account Application Channel - Facility Takeover Fraud 2009

Chart 3.3.2



Bank Account Application Channel - Facility Takeover Fraud 2008

Chart 3.3.3



Lies still delivered in person

The delivery channel favoured by bank account application fraudsters continues to be face-to-face, and the proportion of cases this relates to increased in 2009 compared with 2008. Face-to-face application frauds increased from 32% of the total up to nearly 48%, with the proportion of internet and mail application frauds both declining accordingly.

> "The proportion of women involved rose from almost 30% of victims of takeover in 2008, to almost 40% in 2009."

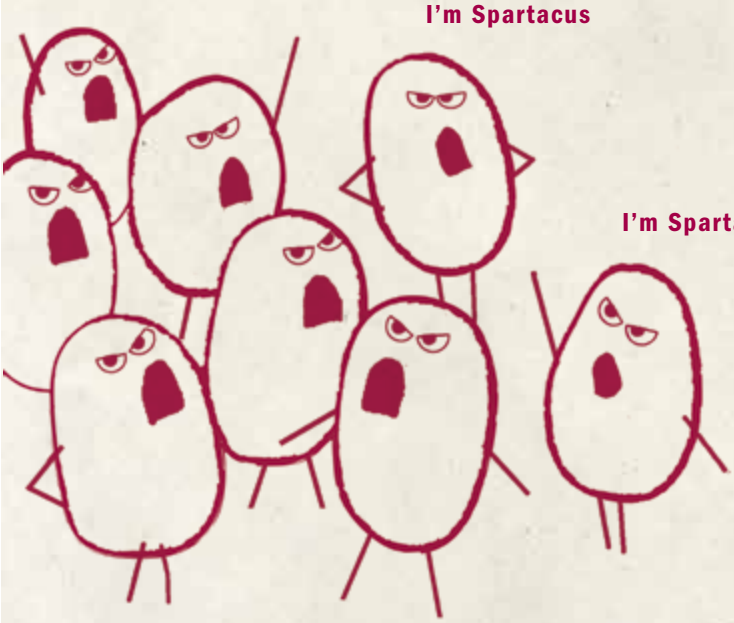
Gender and age only changes in facility takeover fraud

The only type of bank account fraud that saw any significant change in relation to gender distribution was facility takeover fraud: where the proportion of women involved rose from almost 30% of victims of takeover in 2008, to almost 40% in 2009. It is a similar story if average age is considered: with average ages for each gender and type of fraud changing very little, except in cases of facility takeover fraud once again. The average age of male victims of takeover has dropped from 51 to 48 while for women it has dropped from almost 50 to just under 45. This implies a more scatter-gun approach (possibly indicating that the data which has been compromised has come from a more random source, like volume phishing attacks) while still showing that there is a preference for targeting those who are typically more 'affluent'.

I'm Spartacus

I'm Spartacus

I'm Spartacus



Now there's a more secure way to tell who's who and who isn't. Is your business ready?

To find out how identity cards can benefit your business and to secure a free pack, visit **businesslink.gov.uk/idsmart**

Home Office
Identity & Passport Service

idsmart™
ID at your fingertips

Actually I'm Spartacus

3.4 Communications Frauds

The types of communications fraud - frauds committed on an account for a communications product such as a mobile phone - can be seen in Table 3.4.1.

Communications frauds by fraud type

Table 3.4.1

Fraud Type	2008	2009	% Change
Application Fraud	3,911	5,172	32.24%
Facility Takeover Fraud	899	3,879	331.48%
Identity Fraud	6,798	11,511	69.33%
Misuse of Facility Fraud	3,604	3,377	-6.30%
Total Frauds	15,212	23,939	57.37%

Facility takeover fraud rockets

There has been a massive increase in communications related facility takeover frauds in 2009 compared with 2008. This increase is attributable to two factors: (i) an individual taking over an account in order to obtain the genuine account holder's next handset upgrade, providing the fraudster with an expensive item they can either use themselves or sell for cash, or (ii) the unauthorised addition of another number to an account, leaving the victim to pay the fraudster's bill. In 2008, over 96% of facility takeover cases were related to an unauthorised addition of a facility (adding another number to the bill), but in 2009 there was a much more even split between these unauthorised additions of a facility (less than 63% of cases) and unauthorised upgrades (most of the rest). It must be noted, however, that while the proportion of facility takeover cases involving the unauthorised addition of a facility was down, the actual number of cases increased by over 180%.

Similar drivers explain communications application fraud

The desire to get an expensive handset for nothing also extends to taking out an account in someone else's name, or making a fraudulent application in their own name. This is particularly true as handsets become more advanced and expensive. The iPhone, which is now no longer tied to one network, is a particular example of a handset with both high value and high demand. These more expensive, aspirational, devices are also subject to more stringent credit-checking procedures. This increases the temptation for someone who wants one - but won't pass these more stringent checks - either to lie on their application or use someone else's name. The resale value of these items also makes them a highly attractive target for the organised fraudster.

180% = the increase in 2009 in the volume of cases involving the unauthorised addition of a facility (e.g. an extra number) to a communications account.

Unsurprisingly, in cases of communications application fraud, by far the most common offence was the failure to disclose an address where the applicant had accumulated adverse credit information in his or her name. This accounted for just over 90% of such application frauds in 2008, and over 93% in 2009. What is more interesting though, is the decrease in the proportion of cases where the fraudster used an alias

to try and hide adverse credit information. Typically, this relates to women switching between married and maiden names, depending on which one is associated with the adverse credit information. This affected nearly 22% of cases in 2008, but in 2009 this was down to less than 5%.

Boys and their toys?

This decline in the use of aliases can, in part, be aligned with a decline in the proportion of communications related application fraudsters who are women. In 2008, women accounted for just over 50% of application fraudsters where the product was a communications account. In 2009, this is down to 41.5%. This is more to do with an increase in men making fraudulent applications than a decline in women doing so, and is probably an indication that there are more men who feel that they must have the latest gadgets (such as Smartphones), than women.

The theory that the number of communications frauds in 2009 has been pushed up by an increase in men who want to get their hands on the latest high value handset is further reinforced by the nature of the identity fraud cases recorded. Current address fraud, which is more sophisticated and requires a more organised approach, accounts for proportionally fewer cases in 2009 than it did in 2008 (although it is still the most common).

The use of an entirely false identity has increased, which (unless it is perpetrated with a lot of skill, and the fraudster has built an identity 'from the ground up', establishing an address and credit history to go with the name) is an indication that people don't really know the processes and checks involved in the application process. They are essentially just throwing a name at an application and hoping it works.

This lack of sophistication in the attempted fraud is further borne out by the large increase in the number of cases where the 'person' named on the application is not known at the address. The use of a false name occurred in 8% of cases in 2008, but 19% in 2009, while the cases where a name was confirmed as 'not known at the address' accounted for 11% of cases in 2008 and in 25% of cases in 2009. Contrary to the general trend in identity fraud, the proportion of men involved in these cases has increased slightly between 2008 and 2009: from just under 80% of subjects to just over 80% in 2009. The frauds therefore would appear to show nothing more than a growing number of people (increasingly men) who want the latest upgrade but do not want to pay for it.

A slight anomaly

The communications product is a rare anomaly in that there was a decline in the number of misuse of facility frauds. This could be a symptom of the increasing reliance on mobile phones in day-to-day life. Even when times get tight, the mobile bill gets paid, and more than that, the bill gets paid with funds that will clear.

Gender distribution for communications fraud subjects

Table 3.4.2

	2008		2009	
Fraud Type	**% Male**	**% Female**	**% Male**	**% Female**
Application Fraud	58.50%	41.50%	49.37%	50.63%
Facility Takeover Fraud	71.07%	28.93%	84.41%	15.59%
Identity Fraud	80.14%	19.86%	79.38%	20.62%
Misuse of Facility Fraud	61.28%	38.72%	61.40%	38.60%
Total Frauds	72.75%	27.25%	69.34%	30.66%

3.5 Plastic Card Frauds

Table 3.5.1 shows the types of fraud that have occurred in 2008 and 2009 when the product involved was a plastic card. This includes store and charge cards as well as credit cards.

Plastic card frauds by fraud type

Table 3.5.1

Fraud Type	2008	2009	% Change
Application Fraud	9,142	5,866	-35.83%
Facility Takeover Fraud	13,273	11,503	-13.34%
Identity Fraud	40,850	39,249	-3.92%
Misuse of Facility Fraud	7,158	6,778	-5.31%
Total Frauds	70,423	63,396	-9.98%

Identity fraud trends bucked?

Unlike other products, frauds involving plastic cards have seen an across-the-board decline in 2009 compared with 2008. The fact that the number of identity frauds has declined is especially surprising; considering that this is by far the most common type of fraud involving plastic cards and that identity frauds have increased so much over all other products collectively. It can only be assumed that in a period when there is a lot more scrutiny paid to applications, and where 2 out of 3 credit card applications are rejected, other products are considered an 'easier target' and so the fraudsters' attention has been deflected elsewhere. The takeover of bank accounts would seem to be an area which has been the target of this off-setting, as this type of fraud has seen a substantial increase: fraudsters trying to siphon off funds that are already in circulation rather than attempting to gain new funds.

Application fraud decreases but follows pattern

Application fraud in relation to plastic cards has seen the greatest proportionate decline; down almost 36% in 2009 compared with 2008. It is likely that this will be due to a combination of factors. First, if there is a perception that card issuers are just not issuing cards, then the number of applications goes down. Even if the proportion of frauds within applications increases, this is unlikely to offset the total drop in applications. Second, because lenders are being more cautious, the number of applications that are declined will have increased. Within this number there will be a proportion of applications that are fraudulent, but although the fraudster has lied to increase their chances of being approved, they haven't told enough lies to pass the credit score. This means that these applications will never reach the fraud team's desk, and so will never be identified as frauds.

There has been very little change in the nature of plastic card application frauds taking place. They're still predominantly attempts by the fraudster to hide adverse credit information (61% of cases in 2008 and 59% in 2009) followed by the use of false bank details and the provision of false employment details (14% and 12% respectively in 2008, and 13% and 15% in 2009). This increase in false employment details provided is likely to be a reflection of the increased levels of unemployment in the UK due to the recession.

A slightly higher proportion of women committed application fraud in 2009 compared with 2008, with women accounting for 47% of fraudsters in 2009 compared with 45% in 2008, and those women were on average about a year older (36 years old in 2008 up to 37 in 2009). Apart from these minor changes, the nature of application frauds for plastic cards remained unchanged - there were just fewer of them identified.

Reasons for recording the fraud

The proportion of cases that would seem to be opportunistic, the previous occupier frauds, was unchanged. This can be seen in the table below. The increase in the more sophisticated current address fraud is more worrying.

Reason for recording fraud	2008	2009
Current address fraud	39.14%	50.71%
Previous occupier fraud	20.56%	20.56%
Previous address fraud	19.52%	12.43%

Some uncomfortable possibilities

The increase in the minimum lending requirements used by lenders can also partially explain the reduction in the number of card-related identity fraud cases recorded. Using someone else's identity is one thing, but if that identity is not deemed to be 'creditworthy' in the current conditions, then it's still not going to be approved - never mind appear on the fraud team's desk to be investigated and recorded. Where identity fraud has been identified, there has been an increase in the proportion of current address frauds in 2009 compared with 2008, while the proportion of previous address frauds has declined.

Once again, this could be a symptom of organised criminals making the frauds more difficult to identify by using more sophisticated techniques. It could also, however, be an unfortunate side-effect of greater public awareness of identity fraud and that the victim will not be held liable. Some people may be more willing to impersonate someone they live with when they know that his or her victim will not be liable for any debts accrued as a result of the impersonation. Added to this, a fraudster who lives with the victim is more likely to know all the relevant personal details, making the chances of a successful application greater (assuming the victim is sufficiently 'creditworthy', of course).

There is also the chance that some of these frauds are not cases of impersonation at all, but cases where the 'victim' did actually apply for the card themselves; building up a debt on that card, then claiming that they were impersonated and never made the application in order to avoid repaying that debt. This type of fraud is very difficult for the card issuer to identify, but becomes a greater fear. It could well lead to genuine victims of impersonation finding it more difficult to prove that they are victims as any organisation that could be prey to this sort of fraud becomes more suspicious of those who say they have been impersonated.

Why have takeovers declined?

It could be said that, in 2008, plastic cards were the facility takeover fraudsters' product of choice. The decline in facility takeover frauds in 2009, therefore, is noteworthy. The technique generally centres upon changing the address on the account, in order to be able to obtain replacement cards. Part of the decline in this type of fraud is due to card issuers responding to this threat and making it more difficult by improving the checks around these requests.

Another possible reason for this decline is that one of the main channels where fraudsters are likely to want to use these fraudulently obtained cards, the internet, has also improved security.

The internet has traditionally allowed criminals to use their fraudulently obtained cards facelessly, and does not require the fraudster to have also obtained the PIN, when a request for a replacement PIN might trigger more concerns with the card issuer. Increasingly, however, eRetailers are using such additional security as the Verified by VISA and MasterCard SecureCode systems. As these systems require a password at the point of transaction, it presents another - more impenetrable - barrier for the fraudster. If fraudsters are finding it more difficult to take over the card accounts successfully, and more difficult to use the cards when they do, then it is unsurprising that they will be attempting to find a new 'path of least resistance' and will be focussing their efforts elsewhere.

"Some people may be more willing to impersonate someone they live with when they know that his or her victim will not be liable for any debts accrued."

3.6 Insurance Frauds

Volumes of the different types of insurance fraud can be seen in Table 3.6.1.

Insurance frauds by fraud type

Table 3.6.1

Fraud Type	2008	2009	% Change
Application Fraud	4,675	4,284	-8.36%
False Insurance Claim	433	670	54.73%
Facility Takeover Fraud	0	2	-
Identity Fraud	601	1,046	74.04%
Misuse of Facility Fraud	269	104	-61.34%
Total Frauds	5,978	6,106	2.14%

There has been an increase in the number of false insurance claims being identified by CIFAS insurance Members. Economic conditions are a major contributory factor to this increase. An argument frequently put forward by the fraud prevention community is that desperate individuals are likely to see making a false claim as a 'morally acceptable' fraud: feeling that they are entitled to a pay-out for all the years that they've paid in without claiming. The claim that they are making, however, breaches the terms of their policy.

Another explanation?

It is possible that some of these false claims mask a different problem: that some people are seeking to avoid finance payments for a car that they can no longer afford. Claiming that the car was stolen, they believe, is one way to avoid having to make any further monthly payments.

If someone is willing to make a false claim because they are desperate, however, they may not be averse to trying the same trick again. They may feel that they 'need' to make a false claim the first time, and then feel more inclined to make further false claims - even if they are subsequently much less 'necessary'.

Why in a false name?

The number of identity fraud cases in relation to insurance has increased significantly in 2009. There are two possible reasons why someone may wish to commit identity fraud in order to obtain insurance. First, if someone takes out an insurance policy with the express intention of making a false claim, then using someone else's, or an entirely fictitious, name distances the fraudster from the crime. An example would be the use of false identities in staged or induced road accidents - a crime that puts all road users in danger.

Second, an insurance document could be used as a stepping stone to creating an identity in order to commit further identity fraud. General insurance policies do not require identity checks in the same way as finance, and are therefore easier to obtain. When someone has an insurance document in a name that is not their own, they can then use this (in some cases) as a proof of identity or address to obtain further goods and services. In that way, a certificate of insurance can be considered a potential 'breeder document' for fraud.

17.5% = The proportion of false insurance claims in 2009 for events that NEVER took place.

A first for insurance fraud

It is interesting to note that 2009 saw the first cases of takeover of an insurance policy. Although this has only been recorded on 2 occasions, this could be the start of a new avenue that fraudsters attempt to exploit. In the first instance, the policy was taken over to add another vehicle fraudulently to the policy - free insurance for the fraudster. The fraudster also attempted to change the address on the policy to keep the new documentation out of the genuine policyholder's hands. In the other instance, the policy was taken over in order to attempt to steal the proceeds of a claim by providing an unauthorised payment instruction for the proceeds of that claim - trying to get the payout sent to an account that was not the policyholder's.

More than just false identities being used

The number of insurance application fraud cases decreased by 8% in 2009 compared with 2008 but, unlike the application frauds seen by other business sectors, the application frauds identified for insurance revolve around the provision of false payment details or the use of false documents. The use of false documents (specifically the provision of false proofs of no claims bonus entitlement) increased from less than 3% of cases in 2008 to just over 9% in 2009. This is obviously a fraud designed to reduce the premium that is charged for insurance - unsurprising in the current economic conditions. What is more surprising is that there haven't been more of the lies that would reduce premiums; like failing to declare convictions or previous claims. Undeclared convictions accounted for a little more than 7% of cases in both 2008 and 2009, while undeclared claims accounted for a little less than 5% of cases in both years. This may not, however, be so surprising in the context that most insurers do not check claims records until they receive a claim. So many people who lie about their claims history, are driving with insurance that would be invalidated should they claim.

Fraud becomes more brazen

With false insurance claims, the number of more blatant frauds appears to have increased in 2009. In 2008, it was most likely that the false claim would be an inflated claim - so the accident took place, but the fraudster has tried to take advantage of the situation to make more out of it. In 2009, however, the most common type of false claim was for a staged accident - the fraudster deliberately engineering the accident with the express intention of making a false claim. In the same vein, 2009 has also seen an increase in the proportion of cases where the fraudster has made a claim when the event did not take place.

Staged events accounted for 16.5% of false claims in 2008 while claims when the event did not take place accounted for 11%. In 2009 this has increased to 23% for staged events and 17.5% for events that did not take place. There has also been an increase in the proportion of cases where the fraudster has made a claim for an event that happened before the cover was in place. So, the fraudster is trying to ensure that an insurance company picks up the cost of an event that they are either unwilling or unable to cover themselves.

A male preserve

In 2009, more than 4 in 5 people involved in insurance fraud were male. This is up from just under 3 in 4 during 2008. This is mostly due to the increase in the proportion of men involved in insurance application fraud in 2009. This is up to more than 83% of cases compared with under 75% the year before. The proportion of men involved in false claims has also increased slightly. In 2008, 62% were male, rising to 65% in 2009. This increase in men making false claims can be somewhat aligned to the increase in the number of premeditated false claims - implying that men are more likely than women to stage an event and/or claim that one took place when it didn't.

3.7 Loan Frauds

The number of frauds identified on secured and unsecured loans has continued to decline.

Loan frauds by fraud type

Table 3.7.1

Fraud Type	2008	2009	% Change
Asset Conversion	0	1	-
Application Fraud	9,981	4,198	-57.94%
Facility Takeover Fraud	2	17	750.00%
Identity Fraud	3,500	2,093	-40.20%
Misuse of Facility Fraud	807	344	-57.37%
Total Frauds	14,290	6,653	-53.44%

The decline easily explained

The decline of over 50% in loan fraud in 2009 compared with 2008 comes on the back of a near 25% decline in 2008, compared with 2007, with facility takeover fraud being the only type of fraud to go against this trend.

The most obvious reason for this is that the current economic climate makes lenders reticent about lending. The instigation of tighter lending criteria has created an environment where people are not considered a sound credit risk, even when they've committed application fraud to hide such things as defaults and other adverse credit information. In many organisations, this will lead to the application being rejected before any fraud investigation could take place, leaving the attempted fraud unrecorded.

The same applies to identity fraud. Just because a fraudster has found a victim, this does not mean that the victim is going to be considered a good enough credit risk. The lender's fraud team therefore has no chance to identify the impersonation.

This decrease in the volume of business being underwritten will be leading to smaller lending books as older loans are paid off. Fewer active loans will mean that there are fewer in a position to be misused. This could well be contributing to the decrease in misuse of facility fraud in relation to loan accounts. Additionally, misuse of facility frauds tend to be identified very quickly: the fraudster not bothering to keep up initial repayments being the strongest of indications that there was never any intention to repay.

53% = the overall decrease in 2009 of frauds relating to loan accounts.

A new trend?

As previously stated, the only type of fraud to increase with regard to loans was facility takeover fraud. The number of these frauds is low, but could this be a type of fraud that could have a greater impact in the future? Where a fraudster has attempted to take over a loan facility, they have attempted to change the address on the account. It is believed that this attempt is a precursor to getting additional funds extended under the original agreement, but the address change means that this will happen without the knowledge of the innocent victim. The fraudster is essentially considering that it is more likely that a lender will extend further funds to an individual whom they have previously identified, and whom they know to be a low risk borrower than someone who has to go through the entire application process from the beginning.

Same old lies

Unsurprisingly, the most common application fraud when applying for a loan is the attempt to hide adverse credit information by failing to disclose a previous address at which the adverse credit information is registered. In 2009, this accounted for over 80% of cases - up from 77% the year before. The proportion of cases where false employment details were supplied has also increased, up to nearly 11% in 2009 compared with less than 7.5% the year before.

The proportionate increase in the attempts to hide adverse credit information is most obviously due to the indebtedness of the UK population. If people owe more, it is likely that they will have more trouble paying it back (especially in times of recession). Repayment problems will lead to adverse credit information and for some, therefore, the belief that they need to hide that adverse information in order to obtain another loan successfully. The increasing number of unemployed in the UK may also explain the increased proportion of application frauds that include false employment details.

Current address fraud increases for loans too

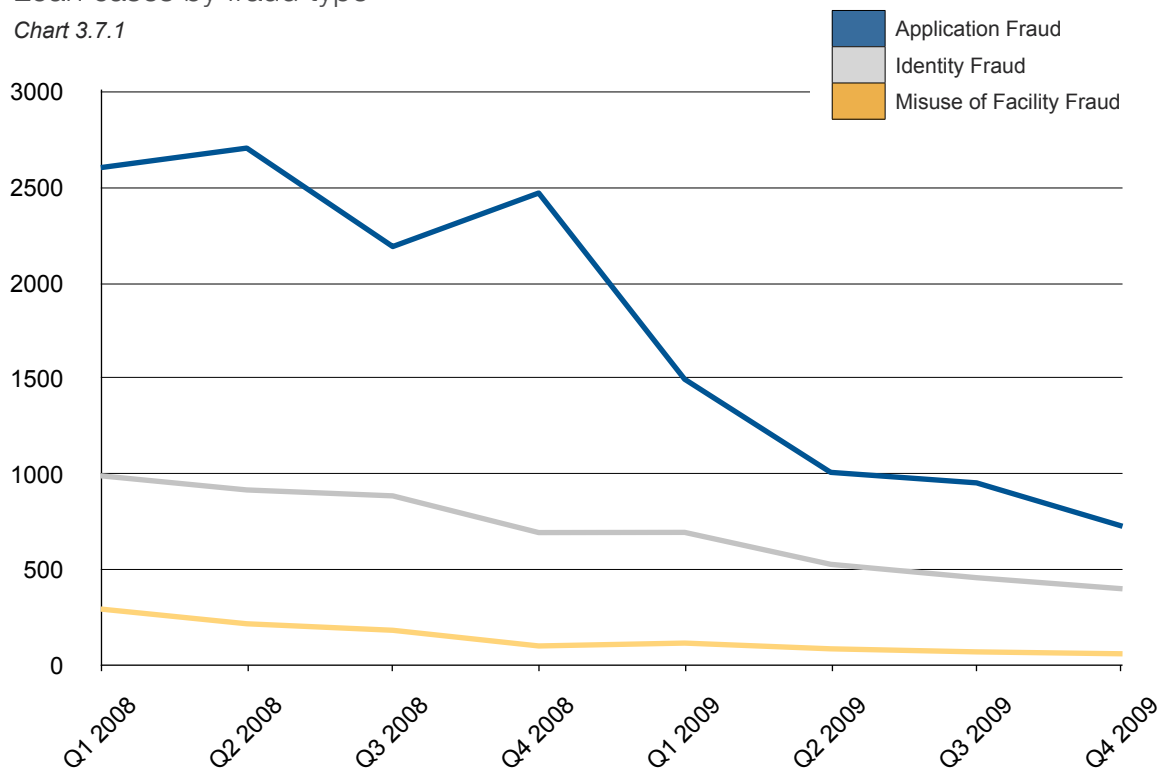
Although the number of cases of identity fraud decreased in 2009, the proportion of those centred upon current address fraud increased. Cases of impersonation where the fraudster used the victim's current address increased from 57% to over 63% of cases in 2009. The proportion of cases that involved the fraudster claiming that the victim has just moved (previous address fraud) reduced from almost 22% to just over 16% in 2009. The opportunistic previous occupier fraud (generally the new resident of a property applying in the name of the last resident) has remained relatively constant - just over 7% of cases in 2008 and just less than 7% in 2009.

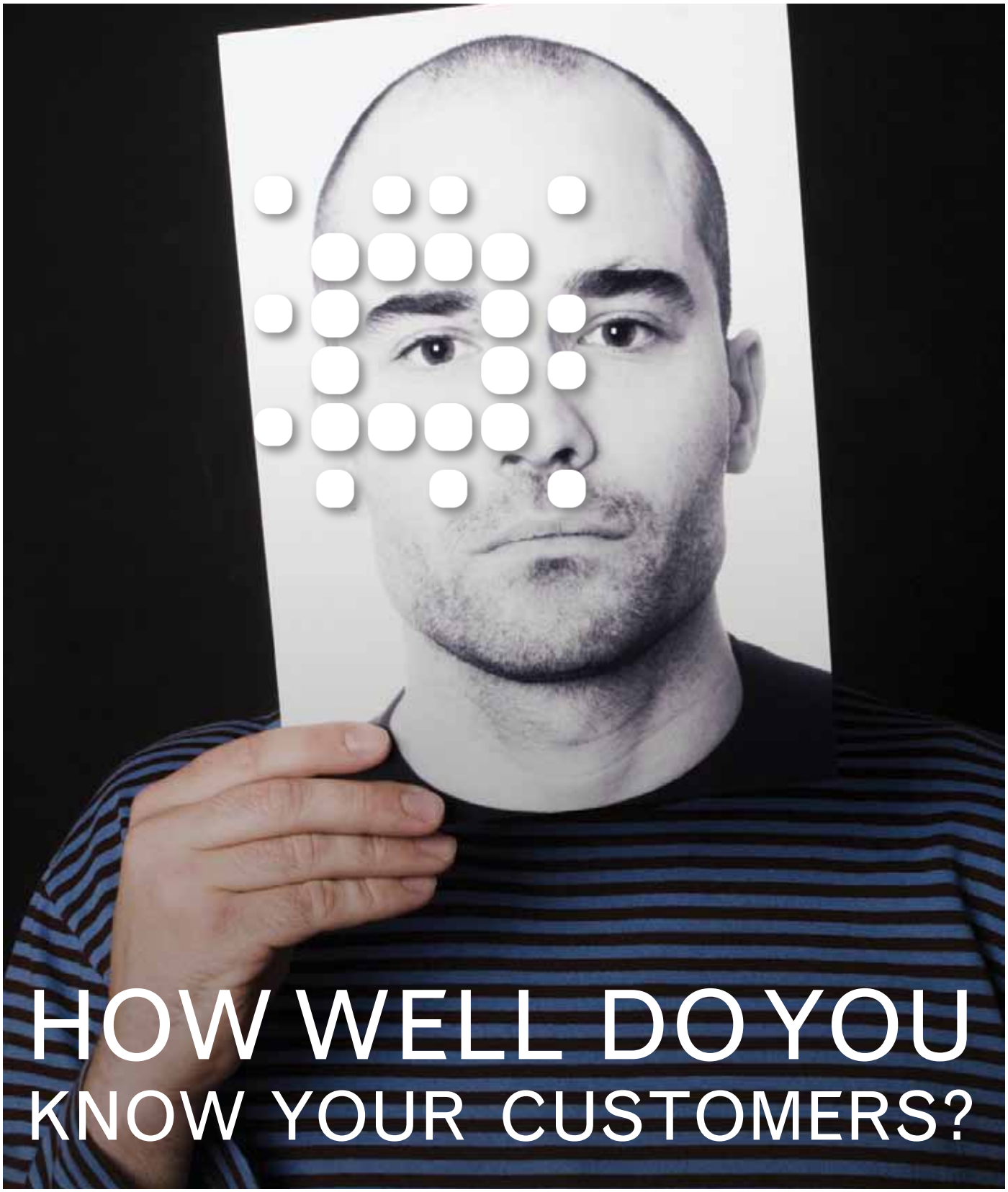
Loan fraud increasingly involves women

The proportion of women involved in loan frauds has increased slightly - from 31% in 2008 to one third in 2009. This increase applied to all types of loan fraud, apart from the few cases of facility takeover fraud. As with other products, identity fraud saw the biggest increase in the proportion of women involved, which may be to do with women being perceived by fraudsters as good targets for impersonation, as well as possibly being a symptom of organised fraudsters using a less targeted approach by using details that they have acquired in bulk through avenues like phishing attacks or purchased from other criminals.

Loan cases by fraud type

Chart 3.7.1





Experian's new Fraud Open Account Monitoring service screens the accounts of existing customers against a unique range of data sources to identify suspicious activity and information. The tool can uncover multiple fraud types including Account Takeover and Sleeper Fraud.

Find out for FREE how well you know your customers with our unique screening service. For more information contact: fraud@uk.experian.com

Experian™
A world of insight

3.8 Mail Order Frauds

Table 3.8.1 shows the mail order frauds that have been identified in 2008 and 2009.

Mail Order frauds by fraud type

Table 3.8.1

Fraud Type	2008	2009	% Change
Application Fraud	641	280	-56.32%
Facility Takeover Fraud	4,351	2,816	-35.28%
Identity Fraud	9,830	30,920	214.55%
Misuse of Facility Fraud	2,740	4,702	71.61%
Total Frauds	17,562	38,718	120.46%

Identity fraud rockets

There has been a massive increase in identity frauds that have been recorded on mail order accounts in 2009 compared with 2008. This may indicate that fraudsters are preferring to go for a 'low value, high volume' route: by using identity fraud to obtain mail order accounts and, therefore, goods that can be sold on. In the present climate, a fraudster may feel that their chances of a successful application for a traditional credit product, like a credit card, are low; especially if the identity details are from criminal online sources and potentially incomplete. This means that fraudsters may be more willing to use those details for mail order applications where the checking procedures may prove to be less exacting.

Mail Order fraud cases by fraud type

Chart 3.8.1

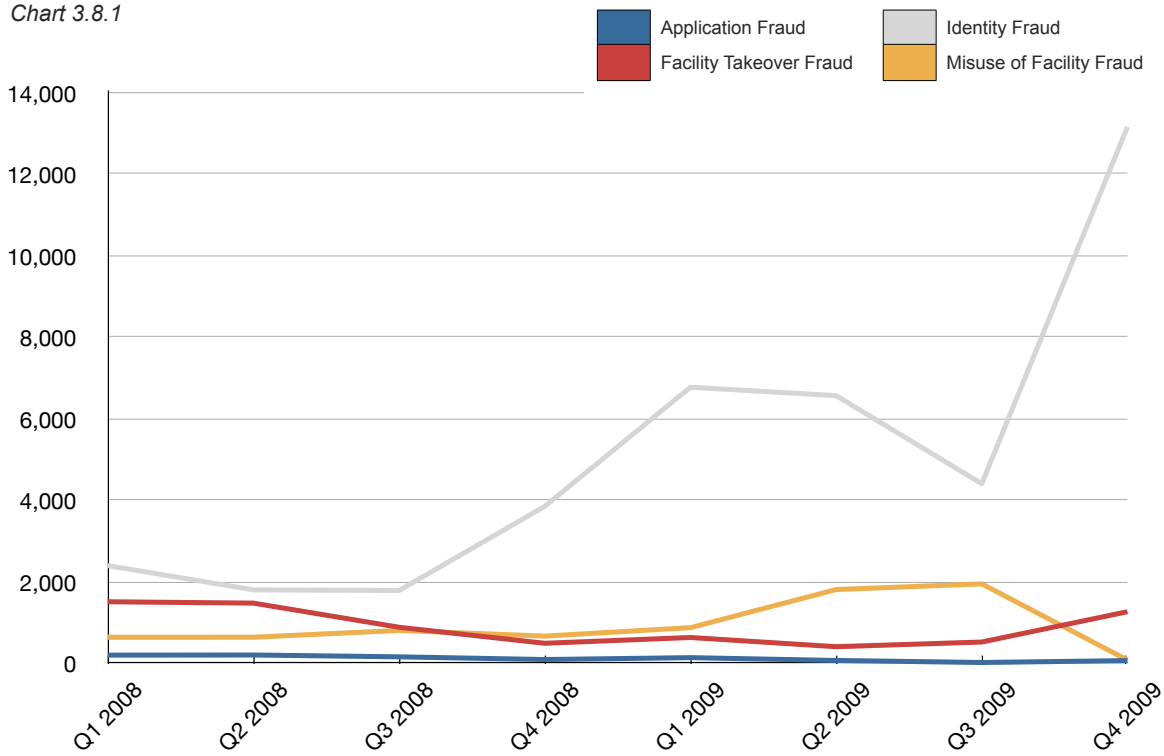


Chart 3.8.1 shows that the number of mail order identity fraud cases spiked dramatically in the last quarter of the year - coinciding with Christmas. This would be an optimal time for a fraudster to be able to sell on goods that they have obtained fraudulently. People who are struggling financially may be more inclined to buy from the stereotypical 'man in a pub' in order to provide for Christmas.

The 'Christmas Effect' does appear to strike the world of mail order on an annual basis. As well as the big spike in 2009, the last quarters of 2007 and 2008 also saw considerable increases over the levels seen in the preceding quarters.

Proof of incomplete datasets

The link between the mail order frauds and organised criminals, particularly those using datasets of compromised identity details, appears to be supported by the types of identity fraud recorded.

In 2008, 68% of cases involved current address fraud, but in 2009 this figure was up to 85% of cases. It is also likely that a proportion of this will relate to people impersonating those they live with as they know that - in general - the victim is not liable for fraud losses. In over 45% of cases, however, a false birth date has been provided, implying that fraudsters are making a high number of attacks but that the datasets they have are not always complete.

Facility takeover fraud figures display changing business practices

It is curious that, in relation to mail order accounts, the number of cases of facility takeover fraud declined over 2009 compared with 2008, as in 2008 there was an increase of over 500% compared with 2007 (albeit from a fairly low base). Most probably, this is due to mail order organisations catching on to the tactics used by the fraudsters to perpetrate the takeovers. Instances of this type of fraud increased rapidly in 2008, necessitating that those organisations put processes in place to block the fraudsters' attempts; such as contacting their genuine customer to check any address changes. As fraudsters realise that the techniques they are using are no longer so successful, they will migrate to other avenues. In this case it would appear that they have moved to attempting to open completely new accounts.

A new gender distribution

(See Table 3.8.2)

It is noticeable that the proportion of men involved in mail order fraud has increased significantly in 2009 compared with 2008. As asset finance fraud is generally the preserve of men, so mail order fraud has been considered a more female fraud. 2009, however, saw more men than women involved - particularly in cases of identity fraud. Other products have seen the proportion of women involved in identity fraud increase, but this is not the case here. It is, however, bringing this particular gender distribution more into line with those seen for other products.

Gender distribution for mail order frauds

Table 3.8.2

	2008		2009	
Fraud Type	**% Male**	**% Female**	**% Male**	**% Female**
Application Fraud	41.31%	58.69%	45.96%	54.04%
Facility Takeover Fraud	18.25%	81.75%	27.44%	72.56%
Identity Fraud	58.56%	41.44%	61.47%	38.53%
Misuse of Facility Fraud	42.76%	57.24%	47.83%	52.17%
Total Frauds	45.77%	54.23%	57.75%	42.25%

Method is everything

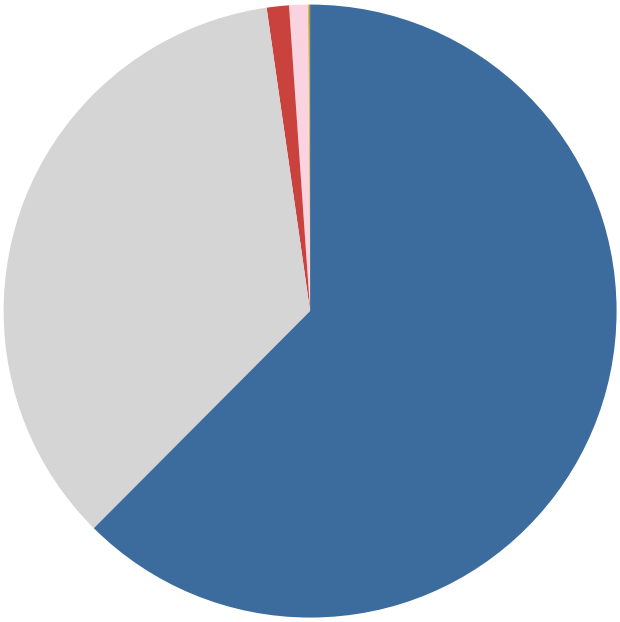
Mail order fraud is another product where the delivery channel of choice for fraudsters, particularly in areas where they are using another person's identity, is the internet. The proportion of facility takeovers that were attempted online increased from 62% in 2008 up to 92% in 2009, with the proportion of online identity frauds up from 86% to 98%. (see Charts 3.8.2 to 3.8.5)

This clearly illustrates that, more than ever, distance and facelessness is of primary importance to a fraudster using someone else's identity. Even in cases of facility takeover (where it was previously believed that fraudsters were happy to try and use the gift of the gab to take over accounts), the anonymity provided by the internet is paramount. This increase in the use of the internet could also be a symptom of an increase in the number of people's login details that have been compromised by attacks like phishing or the use of spyware; coupled with fraudsters finding it increasingly difficult to talk their way past call centre staff.

If the call centre uses a system that takes decisions out of the hands of staff (i.e. the correct answer to security questions must be entered into the system before proceeding) then the criminal cannot convince the operator that it's OK to do what the criminal wants without them having provided the right answer. This also reduces the potential for staff collusion in the fraud. This does not mean that all call centre operators who may have allowed these takeovers to take place were collusive in the fraud. It is saying that, in attempting to offer good customer service, some staff will have allowed the criminal to bypass the security questions because the criminal sounded honest and believable, and they would have felt like a 'jobsworth' if they had refused.

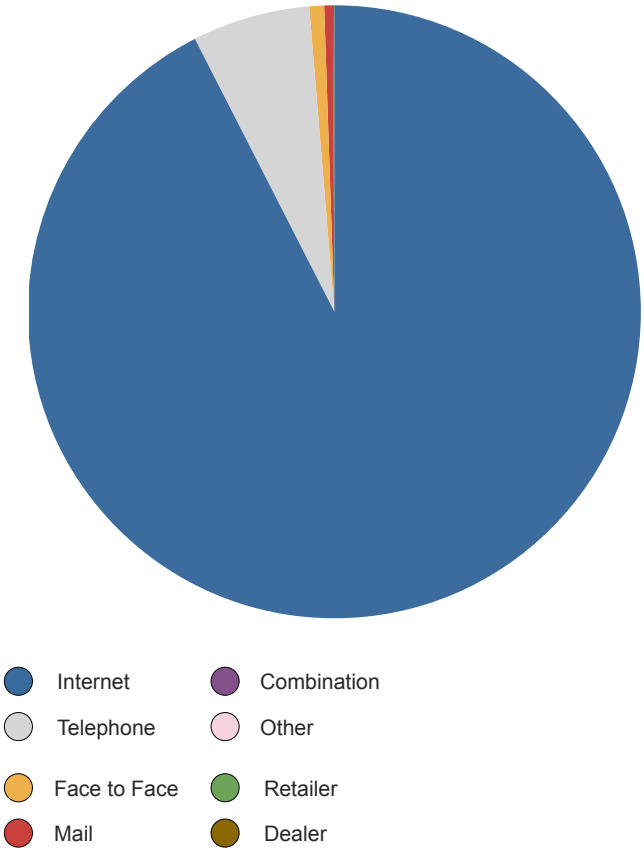
Mail Order Application Channel - Facility Takeover Fraud 2008

Chart 3.8.2



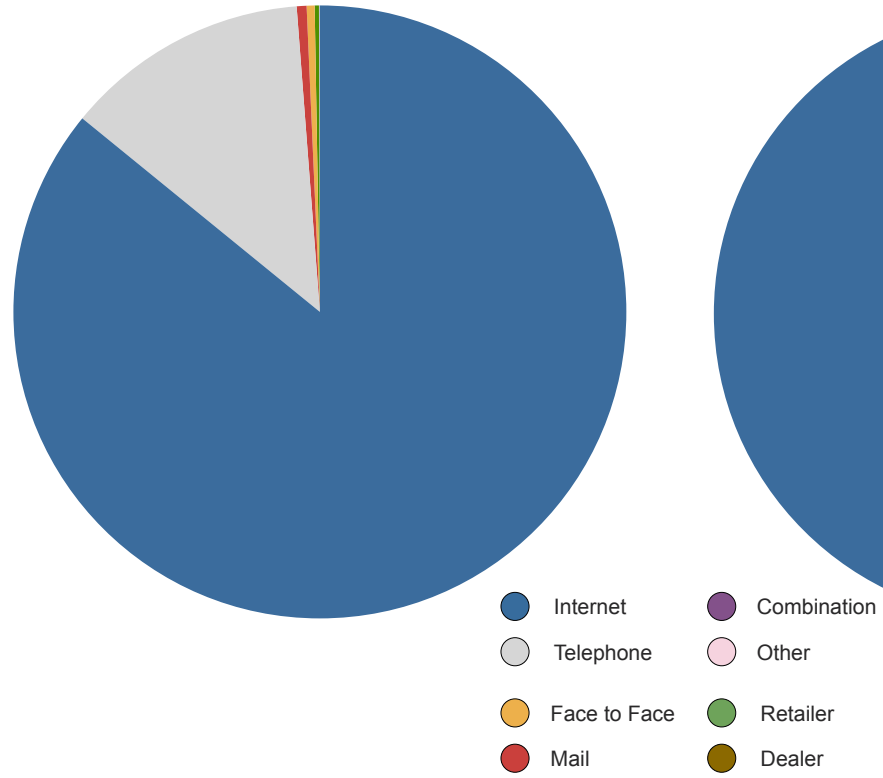
Mail Order Application Channel - Facility Takeover Fraud 2009

Chart 3.8.3



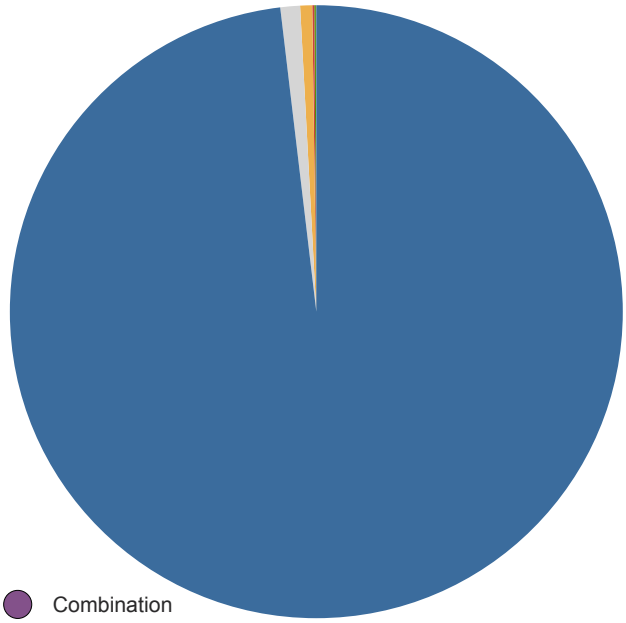
Mail Order Application Channel - Identity Fraud 2008

Chart 3.8.4



Mail Order Application Channel - Identity Fraud 2009

Chart 3.8.5



3.9 Mortgage Frauds

Table 3.9.1 shows the mortgage frauds that have been identified in 2008 and 2009.

Mortgage fraud by fraud type

Table 3.9.1

Fraud Type	2008	2009	% Change
Application Fraud	2,824	2,677	-5.21%
Facility Takeover Fraud	0	6	-
Identity Fraud	92	161	75.00%
Misuse of Facility Fraud	82	160	95.12%
Total Frauds	2,998	3,004	0.20%

Mortgage (fraud) market recovers!

The last few years have seen a steady decline in the number of mortgage fraud cases that have been identified. This coincided with the decline in the housing market, one of the most prominent features of the recession. Declining house prices had the effect of deterring serious fraudsters from attempting to obtain property for profit and those individual fraudsters attempting to obtain a mortgage that they may not be able to afford (fraud for property). 2009, however, has seen an increase in the number of mortgage frauds attempted. Notably, the increases are in identity fraud and misuse of facility fraud, while application fraud continues to decline.

The implication of the reduction in application fraud is that the opportunist (property) fraudsters are still hesitant about over-stretching themselves in the current climate. But examination of the number of cases recorded in each quarter clearly shows that those identified have been increasing as confidence begins to return to the housing market. (See Chart 3.9.1 overleaf)

Surge in forged documents

The supply of false documentation was the most common form of mortgage application fraud committed in 2009. It accounted for 33% of cases in 2009, up from 22% in 2008. In 2008, those false documents were most often bank statements, but in 2009 the most commonly presented false document was a P60. It accounted for less than 9% of the false documents presented in 2008, but almost 35% in 2009. The most obvious explanation for this is that the fraudster may no longer have a job, and so forges or doctors a P60 in order to try and prove both income and employment. The next most common form of application fraud after the supply of false supporting documents was the attempt to hide adverse credit information by failing to disclose an address. This accounted for 30% of cases in 2009, with a further 16% failing to disclose adverse credit information without actually trying to hide it by not mentioning the address it's recorded at.

Are organised fraudsters being assisted?

The increase in identity fraud indicates that serious organised fraudsters see a recovering housing market as an attractive proposition. In turn, they are making more attempts to profit by using deception to purchase a property and then sell it on at a higher price. A very real problem is that this is with the assistance of intermediaries like valuers to help make sure that they buy low and sell high.

There are elements of organised mortgage fraud that are not specifically related to the value of the property being mortgaged. These frauds can involve the use of corrupt solicitors, and revolve around the mortgage lender releasing the funds, which are then pocketed by the criminal. While not tied to house prices specifically, these frauds are made more difficult to perpetrate when credit is hard to come by. The recovery of the housing market has the unfortunate side effect of, once again, making this type of fraud a more realistic proposition for the serious organised criminal.

> "In 2009, 35% of application frauds using forged documents used a fake P60 - up from less than 9% in 2008."

Bucking the current address fraud trend

Curiously, the most common mortgage related identity fraud perpetrated in 2009 was not current address fraud, but previous address fraud. In fact, there were also more false identity cases identified in 2009 than current address frauds. Nonetheless, there were more current address frauds recorded in 2009 than there were in 2008. In 2008, current address frauds accounted for over 31% of the mortgage identity frauds recorded, with previous address fraud and false identities accounting for 20% each. In 2009, previous address fraud was up to almost 40%, false identities accounted for 25%, and current address fraud was down to 20%.

This implies that, while the number of cases that appear to be perpetrated by serious organised fraudsters has increased, they have been proportionately outweighed by less sophisticated frauds. This is most likely a case of people with little knowledge of the processes and checks involved in the application process trying to take advantage of what they believe to be rising property prices. They wish to make a relatively quick profit, but without the danger of using their own name to do it.

Fraud motivated by fear

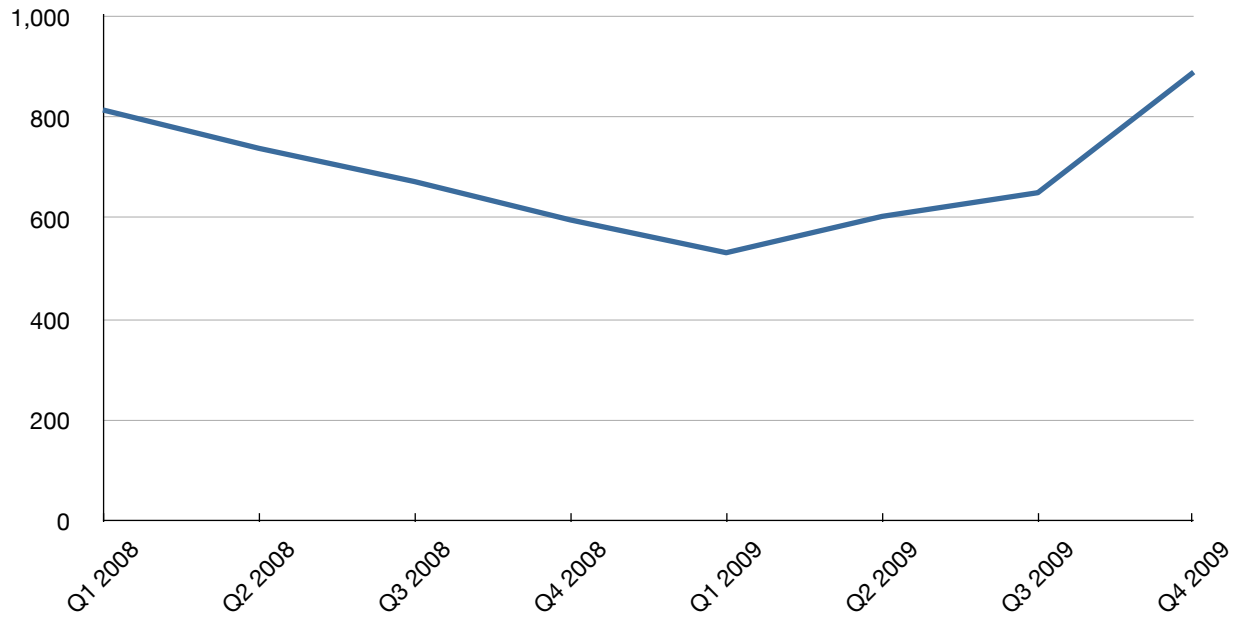
The increase in the number of misuse of facility cases indicates that making mortgage payments has become a struggle for more people. The most common offence relating to misuse of facility fraud is the paying in of false instruments such as cheques that they know will bounce and electronic payments that they know will be recalled. These are clearly frauds perpetrated by people who are worried that their home may be repossessed if they do not continue with repayments. In many cases these concerns could be unfounded as lenders are, frequently, reluctant to repossess homes where the payment problems are likely to be only temporary. This means that in at least some of these cases, the homeowner would not have needed to commit the fraud if they had just spoken to their mortgage provider and come to an arrangement.

Another first

As with loan frauds (Section 3.7), 2009 has seen the first takeovers of mortgage accounts. The reasoning behind this is similar: the fraudster wishes to get the mortgage lender to advance them funds based on the security provided by the innocent party's home and their payment record.

Mortgage application fraud cases

Chart 3.9.1



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.

We help you **discover** more

Ordnance Survey®

www.ordnancesurvey.co.uk/cifas

4. The fraudscape of the UK: Conclusions

An age-old comment is that fraud rises to the surface during times of recession. It certainly goes without saying that a substantial number of the frauds identified in 2009 have been driven by the current economic conditions, particularly those around misusing existing facilities by making false payments and making false claims on insurance. These conditions, while helping to push up the numbers of these types of fraud, will also be masking some others. Another age-old comment is that when the tide goes out, the wrecks become visible. So - it is likely that the recession will have uncovered historic frauds. It will also have masked attempted frauds that have not been identified by the fraud departments of an organisation, as they failed to get past the tighter lending controls currently in place.

The fraudsters may be telling lies to hide adverse credit information, but that may not be sufficient to make them creditworthy in the present lending conditions. They may have used the identity of someone else, but that does not mean that their potential victim is sufficiently creditworthy either. These fraudulent applications, which are rejected, may never reach the fraud team for investigation, so remain unidentified and uncounted. Similarly, with less new business coming in, fraud departments have more time to scrutinise the existing books more scrupulously to identify frauds that have previously slipped through the net.

Most worrying is the increase in the number of current address identity frauds that have been recorded. These are frauds likely to have been perpetrated either by a person living with the victim, or the so-called victim themselves (when they falsely claim to have been impersonated in order to evade a debt). More disturbingly they may have been perpetrated by serious organised criminals with in depth knowledge of the systems that they are trying to subvert and a large toolkit at their disposal for the effective perpetration of the crime.

2009 saw fraudsters increase the amount of 'piggybacking' taking place - taking over mobile phone accounts and insurance policies in order to get their phone number or car added to someone else's bill.

2009 would appear to be the year that the fraudster started to take "the road less travelled". The figures suggest that those areas that have, over the last couple of years, been the fraudster's bread and butter are increasingly being closed off and so they are looking for alternatives. One of these alternatives is to take over an account that is not immediately an obvious target (loan accounts and mortgage accounts). Another alternative is to cut out the middle man: instead of fraudulently obtaining credit cards to make purchases, set up fraudulent mail order accounts to obtain goods direct.

Is facility takeover fraud a flash in the pan? It is noticeable that the products that saw the highest volumes of facility takeover fraud in 2008, plastic cards and mail order, actually saw declines in this type of fraud in 2009. This could indicate that fraudsters are now finding this type of fraud more difficult to perpetrate as the organisations that hold the accounts have become more alive to the threat. This increased awareness and ability to combat the fraud may mean that the less skilled fraudsters are moving away from these products and leaving such takeovers to the organised fraudsters who could possibly be operating with the assistance of collusive members of staff within the organisations.

Women account for a higher proportion of victims of impersonation than seen previously, which could be an indication that fraudsters, particularly organised fraudsters, are moving away from their traditional target demographic. This is possibly because there is a greater perception of parity between the genders now, and that a woman is just as likely to be a 'good' victim. Or it may indicate that fraudsters are increasingly using a less targeted approach, and are willing to try and use anybody's data that they are able to compromise, be that through the use of spyware, phishing, bulk data theft or any other means. Although it is not possible to say precisely which, the likelihood is that it is a combination of both.

Not only has the quantifiable fraud that has been identified and recorded by CIFAS Member organisations increased, but so has the probability that the amount of fraud that has been attempted but remains unidentified (lost in the sea of rejected applications) has also increased. A proportion of this increase will be attributable to desperate people taking increasingly desperate measures as a result of the recession. An example of this increasing desperation may be the rise in the number of false insurance claims that are a result of pre-planned, staged events as opposed to inflating the claim on a genuine accident. There is also an unknown but worrying proportion of this increase that will be a direct result of organised criminals involved in fraud, especially those frauds that involve the abuse of the identities of innocent members of the public.

So, overall, fraud is on the up. If, as recent figures suggest, the worst of the recession is really over, will the fraud trends identified here disappear, or will they simply change once again?

For further information, please contact our Research Manager and the Communications Team.

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

press@cifas.org.uk

CIFAS

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

www.cifas.org.uk