The Insight Report

Fraud in the private sector - March 2010

Contents

Introduction

Charlotte Hogg, Managing Director, Experian UK & Ireland

Our economy is currently losing an estimated £30.5 billion a year through fraud[1]. That represents 2.2 percent of GDP, 3.5 percent of the national debt, and is more than double the £13.9 billion worth of direct fraud losses identified by the Association of Chief Police Officers in 2007[2].

And that is simply what can be estimated today. By its nature, estimating losses due to fraud is a dark art. But what we do know is that as households face mounting economic pressures, fraud is likely to increase, the nature of it is likely to change, and it is being committed by ordinary people as well as sophisticated criminal gangs.

This report looks at how this is playing out in the private sector, where more than £9.3 billion of fraud is estimated to take place. We review the key trends in fraud, look forward to how they might play out in the future, and what we can do as individuals and organisations to combat it.

What are the shifts? Firstly, a massive increase in first-party fraud; individuals lying or omitting key information on lending or insurance applications, job applications or insurance claims. Those closer to the edge financially are, and will continue to be, where first-party fraud is concentrated, but we see a big increase in wealthier demographic and geographic areas as well.

Third-party fraud is also on the up, and it is moving closer to home. Fraudsters used to travel to commit fraud; today they also focus locally. Once the bane of SW1X and SW3, now postcodes such as E14 are on the target list. Favoured techniques include address forwarding, but we all need to be on our guard against account takeover and identity theft, especially with the increased sharing of career details on the internet.

Fraud is changing as well; with approaches such as 'bust out' becoming more popular as lending applications fall. It is harder to spot, and requires financial institutions to link the activities of individuals and households across current accounts and lending to pre-empt the bust out.

How to combat this rise? As individuals, we need to safeguard our information and ensure that we watch for any activity that appears to take place in our name. As organisations, we need to focus not just on preventing fraud at the front door, but on an ongoing basis as well – both amongst our employees and customers. Culture is key and needs to start from an audit committee constantly asking the question to every employee in the business.

In many cases, we also need to remember that fraud is the result not of an evil gang, but individuals who are financially stressed. Identifying the bad from the pressured is important, and by putting controls in place, it helps those who are facing challenges not to walk down a path it will be harder to come back from.

[1]Source: National Fraud Authority, 21-Jan-10: http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/NewsRelease/Pages/release210110.aspx

[2]Association of Chief Police Officers, 06-Mar-07: http://www.acpo.police.uk/pressrelease.asp?PR_GUID=%7B40F292C5-F97A-4A5B-BCC8-C579F140E01C%7D

2. The changing face of fraud

With fraud an increasingly prominent and costly business issue for many organisations, Nick Mothershaw, Director of Fraud and Identity Solutions at Experian, discusses the changing nature of fraud and the impact it is having, and will continue to have, on private sector organisations.

The recent report from the National Fraud Authority (NFA)[3], based predominantly on 2008 data, estimated that annual losses attributable to fraud in the UK were in excess of £30 billion, with the financial services industry hit to the tune of £3.8 billion. Twelve months later, having experienced even more economic turbulence, losses for 2009 could be much higher, with fraud attempts across insurance and mortgages, for example, up nine percent and six percent respectively. In fact, Experian's projections for 2010 suggest that there could be even worse to come.

Experian works with National Hunter within the financial services industry to provide consortia anti-fraud solutions. This allows organisations to check applications against databases of previous applications and known frauds for inconsistencies and similarities that may indicate application fraud. By analysing the data captured through National Hunter and similar insurance systems, and discussing with a wide range of financial services providers how fraud is impacting them, Experian's team of fraud consultants has identified five key fraud trends that it believes will strongly impact organisations over the next 12 months.

The fraud outlook

Future trend 1: First-party fraud levels will rise, fuelled by financial stress

As a proportion of total fraud, first-party fraud – consumers manipulating their own information attempting to obtain credit and other financial services – accounted for around 28 percent of fraud cases identified by Experian in the first three quarters of 2009.

This figure leapt in the final three months of the year, with first-party frauds accounting for over 46 percent of all fraud attempts, at a time when third-party fraud – organised criminals and opportunists seeking credit and other financial services using the identities of other people – also continued to grow. Experian believes that financial stress brought about by the recession has been a significant driver to cause previously honest consumers to attempt first-party fraud.

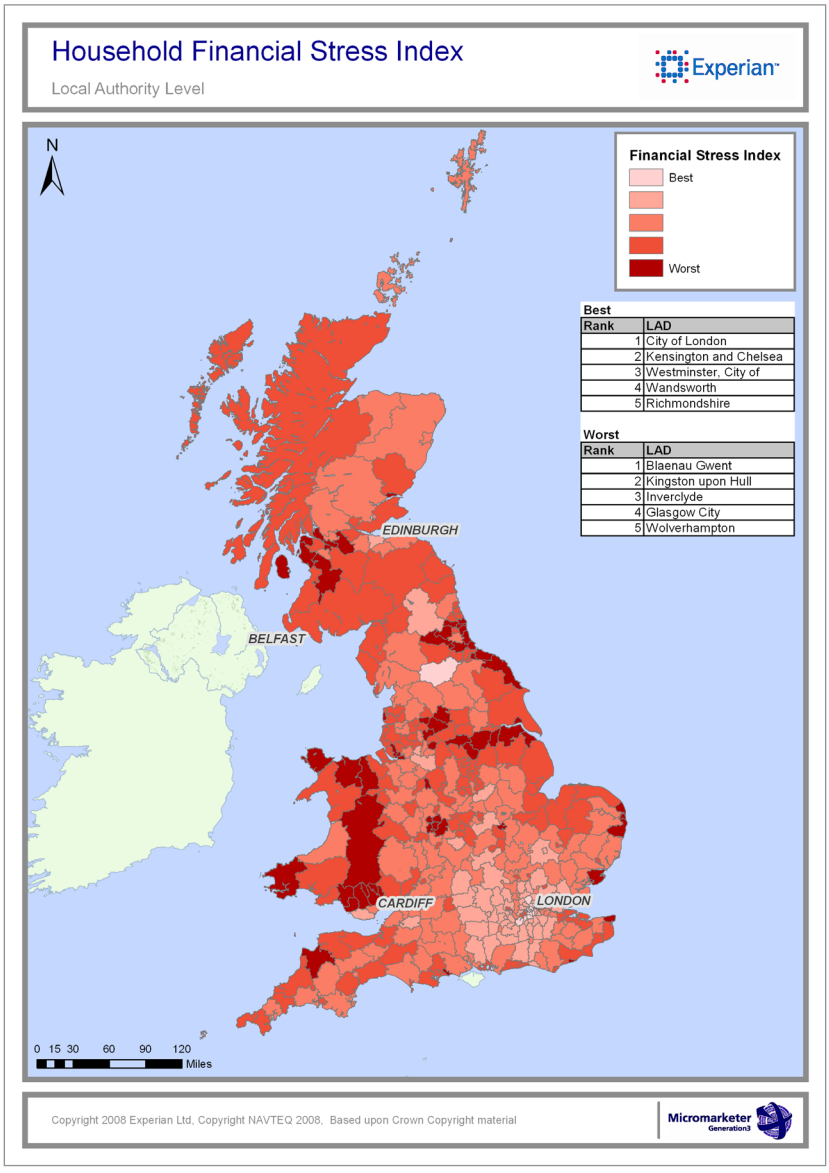
Looking forward, tepid economic growth, with the uncertainties of a "double dip", continued high levels of unemployment and constrained lending could mean that certain household groups will remain vulnerable for longer and potentially more likely to commit first-party fraud. Experian's analysis of fraud data using its Financial Strategy Segments (FSS) classification reveals that those living close to the poverty line, as well as young people in the early stages of setting up home, are most likely to attempt this kind of fraud. Our data shows that these groups are already attempting high amounts of first-party fraud, and financial stress is likely to cause more.

[3] Source: National Fraud Authority, 21-Jan-10: http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/NewsRelease/Pages/release210110.aspx

The Child-raising Challenge demographic – with vulnerable single parents often relying solely on benefits and struggling with debt repayments – makes up less than four percent of the UK population, but is responsible for almost 11 percent of attempted first-party frauds in 2009. Likewise, Looking to the Future – young singles often in shared rented accommodation earning reasonable wages – accounts for less than three percent of the population, but more than eight percent of attempts. This is examined in more detail in section three of this report.

Geographically, we would expect first-party fraud to rise strongly in those parts of the UK where financial stress is concentrated. Looking at Figure 1, vulnerable areas could include Blaenau Gwent, Kingston upon Hull, Inverclyde and Glasgow city, where cases could rise as financial stress grips the regions.

Figure 1: Financial Stress levels across the UK



Source: Experian (March 2010)

Future trend 2: Mortgages and sub-prime lending a focus for application frauds

After a sharp rise in fraudulent mortgage fraud applications in the second half of 2007, attempted mortgage fraud has accounted for around 20 in every 10,000 applications ever since (see Figures 2 and 3). The NFA's recent report suggested that mortgage fraud losses materialising during 2008 amounted to around £1 billion. **Experian estimates that mortgage fraud losses amounted to £1.06 billion in 2009 and could well reach £1.17 billion in 2010[4].**

Experian's analysis also reveals that 2009 saw a rise in the use of false documentation to apply for mortgages. Experian predicts that this trend will continue in 2010 with organised criminals using false identity information to gain mortgages, and consumers providing false financial documentation, such as accounts and payslips, to substantiate their income. As a result, lenders should improve their processes for identifying forgeries and false documentation as part of the application process. In particular, a move back to paper verification could actually increase fraud rather than reduce it; the focus has to be on a range of authentication techniques, both automated and manual.

In our view, a shortage of sub-prime and self-certification mortgages will continue to see increasing numbers of consumers turning to deception when attempting to obtain mortgages. 2010 will see the last batch of pre-crunch mortgage holders coming off three-year fixed-term interest deals. Should interest rates start rising again, Experian expects to see a rush of consumers who are currently enjoying low standard variable rates looking to re-mortgage. In our experience, those consumers whose financial fortunes have suffered severely as a result of the recession will potentially be driven to apply using false information in order to gain a fixed interest rate.

Although the majority of attempts will continue to involve false employment and income details, with mortgages requiring at least a five percent deposit, we could well see increasing numbers of consumers attempting to hide personal loans and credit card facilities that they have taken out to raise cash for deposits. This kind of deception can be detected through investigation by using systems that are able to pick up on evidence of recent credit applications.

Experian also expects to see an increase in fraudulent sub-prime applications. As prime finance providers become more effective at weeding out fraud in their open books, fraudsters will be driven to targeting the sub-prime market when it re-emerges from the recession. Sub-prime lenders should ensure that the data supplied by applicants for use in affordability modelling is valid, to ensure that customers are not committing fraud to build what could become an unsustainable credit position.

Likewise, Experian believes that the growing pay day lending business, which is low value but does provide immediate cash, will become a major target for fraud. While much of this threat is likely to come from financially-stressed consumers who may feel that they have nothing to lose, there is also a potential threat from organised fraudsters too. This would, however, require a new level of efficiency in order to commit the higher volumes of low level frauds that organised criminals would be looking to in order to make a decent return. However, with the issue of funds being almost immediate in this type of lending, should organised fraudsters crack this system then they will make hay before the problem is spotted and closed down, with pay day lenders being left with large losses.

---

[4] Figures calculated by extrapolating known growth in fraud attempts against Experian/National Hunter mortgage provider clients in 2009 and fraud expert predictions for 2010 against industry estimates in the National Fraud Authority report on the value of fraud perpetrated against mortgage providers in 2008.

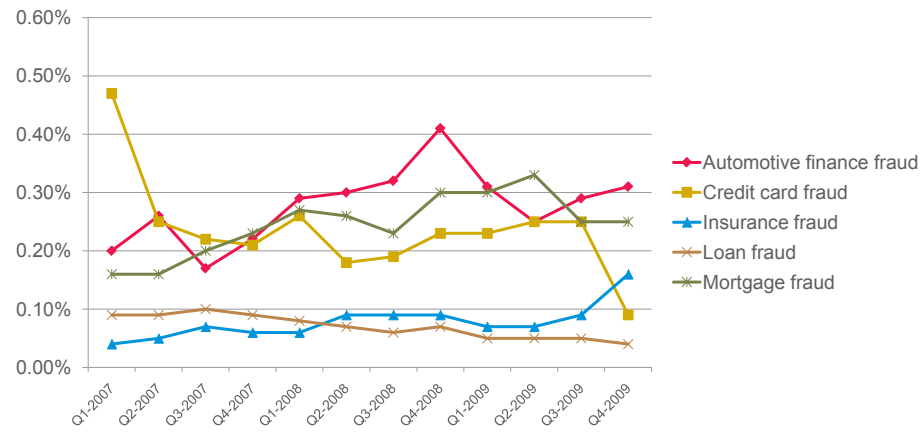
Future trend 3: Insurers face an increase in claims fraud

Insurance fraud will also continue to be a major growth area over the next 12 months. After several quarters of slow but steady growth, it surged in the last three months of 2009 (see Figures 2 and 3), with 16 in every 10,000 insurance claims detected as being fraudulent. As with other forms of first-party fraud, insurance fraud rises in difficult economic times as financially-stressed consumers increasingly claim on home insurance to gain goods which they can no longer afford to replace.

There is also an increasing third-party threat in the insurance sector. As banks increase the sophistication of their fraud prevention systems, fraudsters will turn their attentions to other institutions that they consider to be more vulnerable. Although insurers have taken steps to help them spot organised fraud rings and there are insurers that are incredibly sophisticated in how they detect and prevent fraud, the industry as a whole is still considered an easier target.

By considering the increases in fraud attempted against Experian's insurance clients in 2009, alongside the Association of British Insurers' estimate that fraud cost the general insurance industry £2.08 billion during 2008, **Experian estimates that general insurance fraud losses reached £2.27 billion in 2009, and could reach £2.5 billion during 2010[5].**

Figure 2: Experian Fraud Index: Reported fraud as a proportion of applications [6]



Source: National Hunter and Insurance Hunter (March 2010)

[5] Figures calculated by extrapolating known growth in fraud attempts against Experian/Insurance Hunter clients in 2009 and fraud expert predictions for 2010 against 2008 figures from the Association of British Insurers.

[6] Fraud rate shows the amount of fraudulent applications detected at or within 90 days of the point of application as a percentage of total applications. Experian did not specifically record the total number of applications for credit cards only through National Hunter prior to Q2 2009, and has therefore derived a 'total application' level for credit cards based on trends from applications for credit cards, current accounts and savings accounts combined to allow fraud rate comparisons to be made before this point.

Figure 3: Fraud by product type

		Q1-2009	Q2-2009	Q3-2009	Q4-2009
Automotive finance	Frauds per 10,000 apps.	31	25	29	31
Insurance	Frauds per 10,000 apps.	7	7	9	16
Cards	Frauds per 10,000 apps.	23	25	25	9
Mortgage	Frauds per 10,000 apps.	30	33	25	25
Current account	Frauds per 10,000 apps.	N/A	17	20	18
Loans	Frauds per 10,000 apps.	5	5	5	4

Source: National Hunter and Insurance Hunter (March 2010)

Future trend 4: Organised criminals move from targeting the primarily wealthy to the mass market

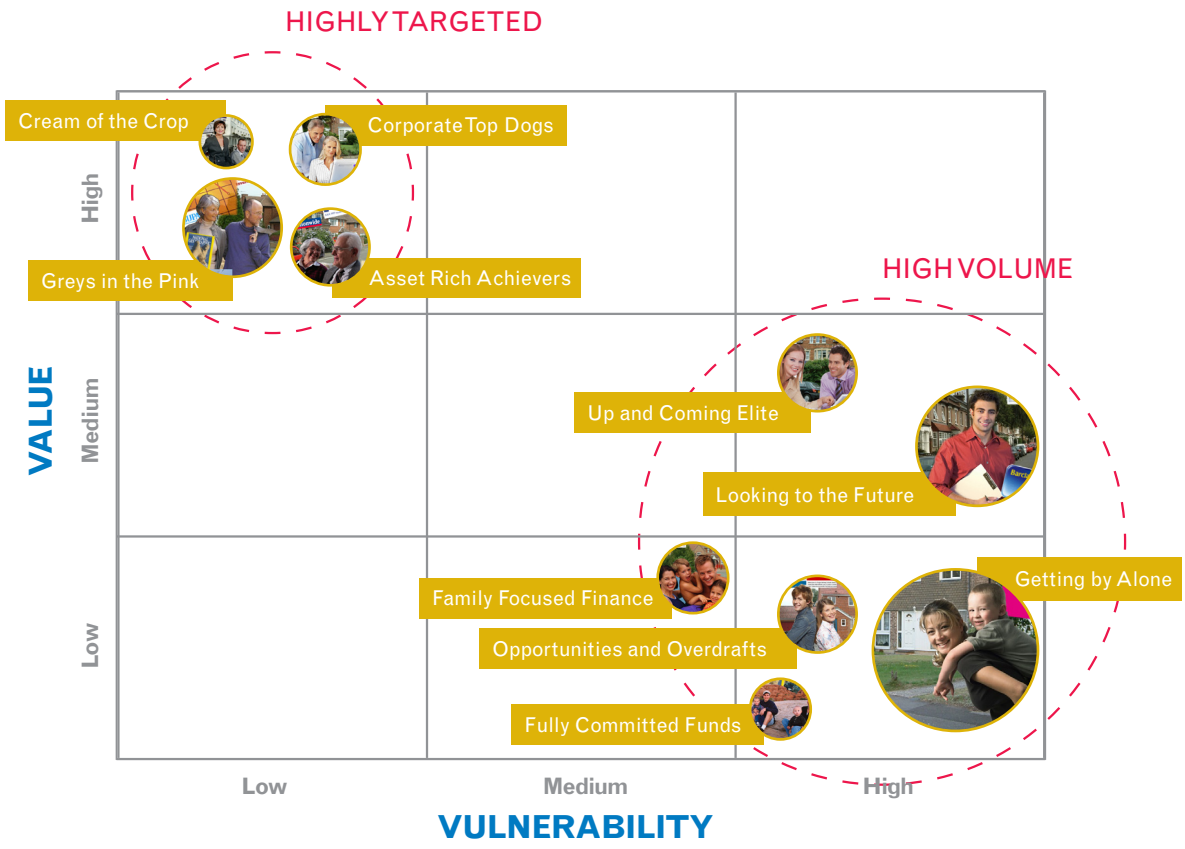
Fraud committed by organised criminals will become even more sophisticated in how victims are selected and targeted in the future. They will increasingly segment their targets according to ease of attack and the ability to accumulate money quickly.

This prediction is based on a new trend that our fraud experts have identified. By mapping suspected frauds to Experian's FSS consumer classification, it reveals that fraudsters are **moving from targeting those with obvious wealth to the mass market, where they are spreading their net far and wide across the population.**

Third-party fraud has started shifting in this direction. Throughout 2009, there was increasing activity in London boroughs closest to a number of areas where fraudsters operate from, primarily targeting lower value victims that fall into the categories described later in this report.

Consumer groups such as Looking to the Future, Up & Coming Elite and Opportunities and Overdrafts – typically young couples, singles and rented home sharers – were most frequently targeted for card application fraud during 2009. Experian expects this trend to permeate through to other product types more regularly in the future. Figure 4 illustrates this new approach, highlighting the most commonly victimised consumer types, the size of its population, the value each target potentially represents to the fraudsters and their relative vulnerability.

Figure 4: Organised criminals' new approach to committing fraud



Source: Experian (March 2010)

Fraudsters have traditionally been keen on postal areas such as SW1X and SW3 – areas with high numbers of affluent households. Experian fraud experts have noticed that fraudsters' attentions are shifting now to new areas in London such as E14, which has greater numbers of lower value, but crucially more vulnerable, victims. With this approach, fraudsters can achieve higher gains for less effort by attacking a larger group of victims.

The trend towards high volumes of vulnerable, lower-value victims is further highlighted by National Hunter data, which identifies increasing targeting of victims in and around London's East End fraud heartland. Areas such as Canning Town, Victoria Docks, Ilford, Woodford, Slade Green, Peckham, Edmonton, Vauxhall, Walthamstow and the Docklands are now at greater risk than in previous years. **Experian expects to see this trend mirrored in other cities around the UK, with fraudsters looking to commit crime in their back yard.**

Future trend 5: Experian expects insider fraud to rise at all levels

Whether from organised criminals, opportunists or simply lying on a CV to get a job, Experian expects to see an unprecedented surge in insider fraud attempts over the next couple of years, as fraudsters seek to obtain assets or battle for work in a depressed job market. Increasing levels of financial stress, uncertainty around job security and pay freezes across many sectors is likely to cause increasing numbers of people, at both junior and managerial levels, to attempt some form of insider fraud. This trend is discussed in further detail in section six of this report.

3. The emerging first-party fraud threat

Chris Farmer, Fraud Product Director at Experian, considers recent increases in first-party fraud and identifies the consumer groups turning to it.

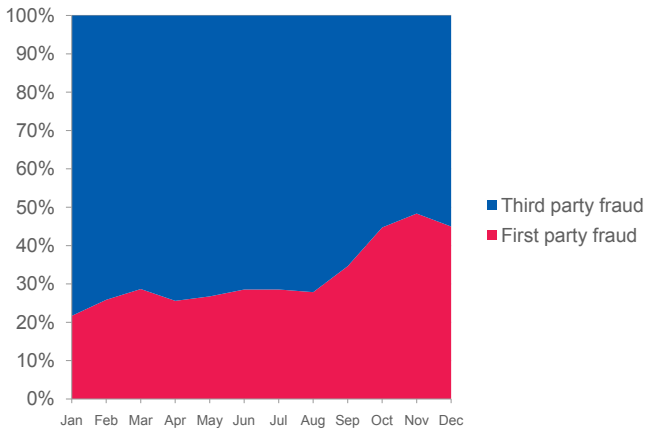
Throughout the recession, UK banks, building societies, mortgage providers and credit card companies have been increasingly targeted by first-party fraudsters. These are consumers manipulating their own information to try and obtain credit and other financial services.

Based on our analysis, this threat has clearly increased as the economic conditions have worsened. In a depressed economic climate, where credit will remain harder to obtain for certain consumer groups, it is highly likely that even more first-party fraud will be committed over the next year.

The first-party fraud shift

It is clear from our analysis that the balance between first-party and third-party fraud shifted dramatically during 2009. As a proportion of total fraud, first-party fraud accounted for around 28 percent of fraud cases identified by Experian in the first three quarters of 2009 (see Figure 5). This figure leapt to over 46 percent in the final three months of the year, while third-party fraud also continued to grow.

Figure 5: Proportion of first-party vs. third-party fraud reported to Experian during 2009



Source: National Hunter and Insurance Hunter / Experian (March 2010)

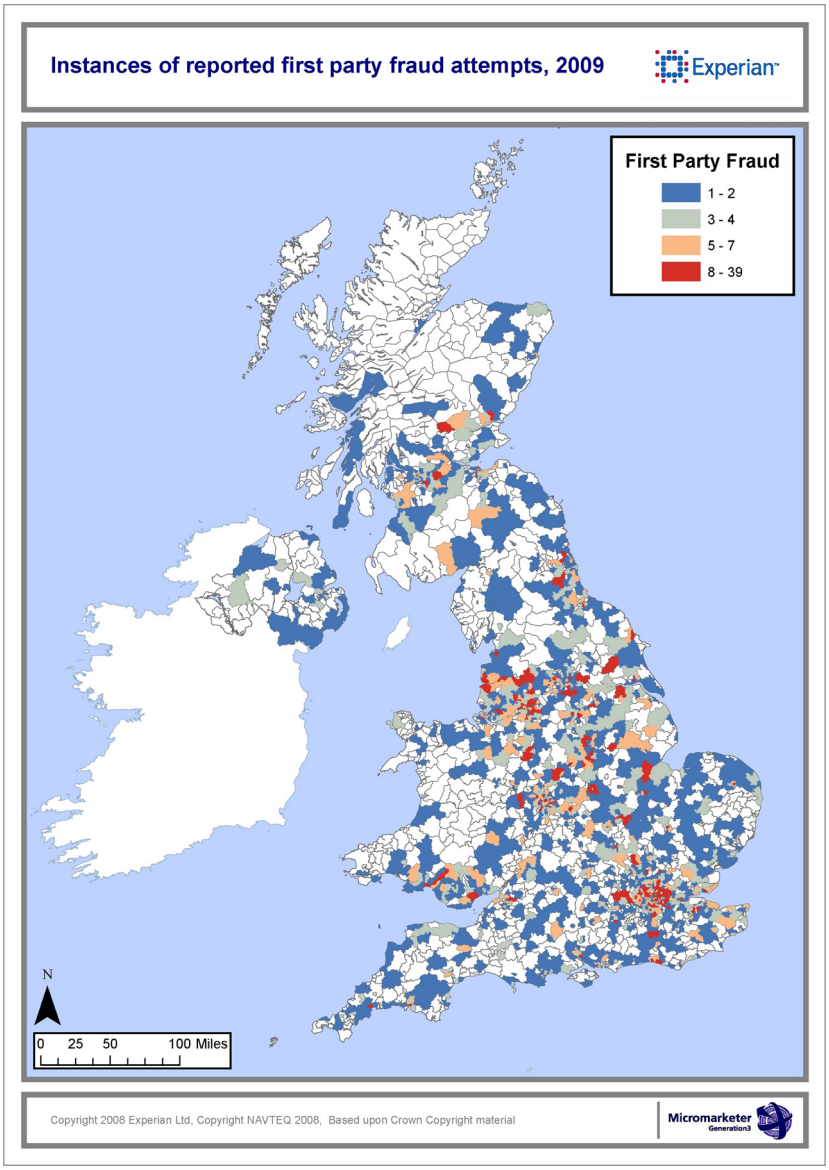
Looking across all sectors, **the main trend Experian identified was a rise in applicants with adverse credit histories at a previous address which they had not disclosed**. By omitting the address from an application, 'hidden adverse' fraud went from accounting for 13 percent of frauds recorded to 30 percent during the course of 2009.

With tighter lending criteria being applied, high levels of financial stress and a shortage of sub-prime credit, many consumers who would traditionally have applied to this sector are now omitting information when applying for prime sector credit and being detected as fraudsters.

Geographic analysis of first-party fraud

Examining the locations where Experian knows first-party fraud is perpetrated reveals a cluster of fraud hotspots around the East End of London. Analysis of data collected through the National Hunter fraud data sharing scheme shows that Shadwell, Stepney, East Ham, Walthamstow, Woolwich, Peckham and Barking saw far higher than average instances of first-party fraud attempts, as did other London districts such as Streatham and Willesden. Outside of London, there were hotspots in the less affluent parts of Chatham, Leicester, Birmingham and Bolton (see Figure 6).

Figure 6: Reported instances of first-party fraud attempts by postal district in 2009



Source: National Hunter and Insurance Hunter / Experian (March 2010)

First-party fraud perpetrators

Our data highlights that most first-party frauds are perpetrated by individuals aged 23 to 27, and these people represent a quarter of all cases. However, even greater insight can be gained by analysing cases reported to Experian by financial institutions and other creditors using Experian's Financial Strategy Segments (FSS) classification.

This level of analysis shows that three key groups of individuals emerge as the most likely to attempt first-party fraud:

- **Those living close to the poverty line – singles and lone parents with very poor means living in the lowest quality housing – were responsible for one in five attempts in 2009.** Responsible for almost 11 percent of cases, the Child Raising Challenge demographic, within which there are many who rely solely on benefits, was the most prolific offender.
- Young people in the early stages of establishing careers and setting up home also feature highly. Groups such as Looking to the Future – young house sharers who, although earning reasonable wages, are not immune to money problems – and Limited Livelihoods – singles in their 30s in mostly council-rented flats – were responsible for around nine percent and four percent of attempts respectively.
- Finally, young credit-hungry families, that previously spent beyond their means and became reliant on credit, also featured strongly amongst the most active first-party fraudsters. These include groups such as Hocked to the Hilt, where incomes are not enough to cover daily expenditures and Downscale Mortgagees, mortgaged families who have struggled onto the property ladder by buying the lowest value terraces and flats.
- **Mapping these groups across the UK shows that there are high concentrations in Northern Ireland, the central areas of Birmingham, Manchester, Nottingham and London's East End**, as indicated in more detail in Figure 7.

Figure 7: FSS consumer types most associated with first-party fraud attempts in 2009

2009 rank	Type	Description	% of frauds responsible for	% of population
1	Child-raising Challenge	Vulnerable single parents often relying solely on benefits and struggling with debt repayments. Central Manchester, Birmingham and Nottingham all have high populations of this consumer type.	10.62%	3.76%
2	Looking to the Future	Young singles often in shared rented accommodation earning reasonable wages and optimistic for the future. These groups are commonly found in the Wood Green, Queensway and Harrow areas of London.	8.83%	2.62%
3	Hocked to the Hilt	Young families with low income with credit from many sources to sustain their lifestyle. There are high concentrations of such types in Northern Ireland and central Nottingham.	6.53%	3.59%
4	Straining the Budget	Young singles, often with children, on low income in rented council properties. West Bromwich and central Nottingham have large populations of this group.	5.84%	3.32%
5	Getting by Alone	Young singles and single parents getting by with limited income in low value properties. Both Colchester and the Broadmead area of Bristol have large numbers of such types.	5.36%	3.44%
6	Limited Livelihoods	Singles in their 30s in mostly council-rented flats. Unemployment is a problem but debts are usually controlled. There are high proportions of this type in the Stratford and Lewisham areas of London.	4.40%	1.75%
7	Poor Prospects	Very poor singles with few prospects living in council flats; many are unemployed or have only part time, low paid work. The central areas of Manchester and Newcastle upon Tyne have large populations of such groups.	3.84%	2.35%
8	Carefree Kick-off	Home sharers making the most of their youth in small, private rented flats. This group is often found in the Princes Street area of Edinburgh as well as central Brighton and Glasgow.	3.78%	2.36%
9	Savvy Big Spenders	Young families with big mortgages for their income; they take advantage of deals to save money but have a high level of spending. There are high populations of this group in Norwich and the Broadmead area of Bristol.	3.57%	3.05%
10	Downscale Mortgagees	Young mortgaged families in the lowest value properties. Low earning power, loans and no savings mean finances can be stretched. Central Nottingham and Mansfield have large populations of this group.	3.51%	1.80%

Source: National Hunter and Insurance Hunter / Experian (March 2010)

First-party fraud in 2010

The increases seen in first-party fraud have undoubtedly been exacerbated due to the recession. Those people perpetrating it tend to come from financially-stressed, low income households. With peaks in unemployment typically lagging overall economic performance, there is no reason why this trend will not continue.

As a result, Experian expects to see first-party fraud attempts, which leapt in Q4 2009, to continue growing throughout 2010, particularly across mortgages and insurance. With a shortage of sub-prime and self-certification mortgages, it is realistic to expect increasing numbers of applicants attempting to obtain mortgages through deception. Furthermore, insurance fraud also rises in difficult economic times as financially-stressed consumers increasingly claim on home insurance to gain goods which they can no longer afford to replace.

These lessons learnt in 2009 simply underline that, in order to combat first-party fraud effectively, it is vital that organisations validate all details of an application. Address history and employment details should also be subject to thorough, automated checks and any suspicious elements flagged for further investigation.

While the majority of first-party fraud is concentrated amongst the most financially stressed, more affluent segments are far from immune. Demographics such as Confident Consumers – young, thriving families with high outgoings – Independent Investors – successful families with good incomes – and Professional Solos – successful professionals or managers who are mostly living alone – each saw first-party fraud attempts increase more than seven-fold in the second half of 2009.

4. The Experian victims of fraud survey

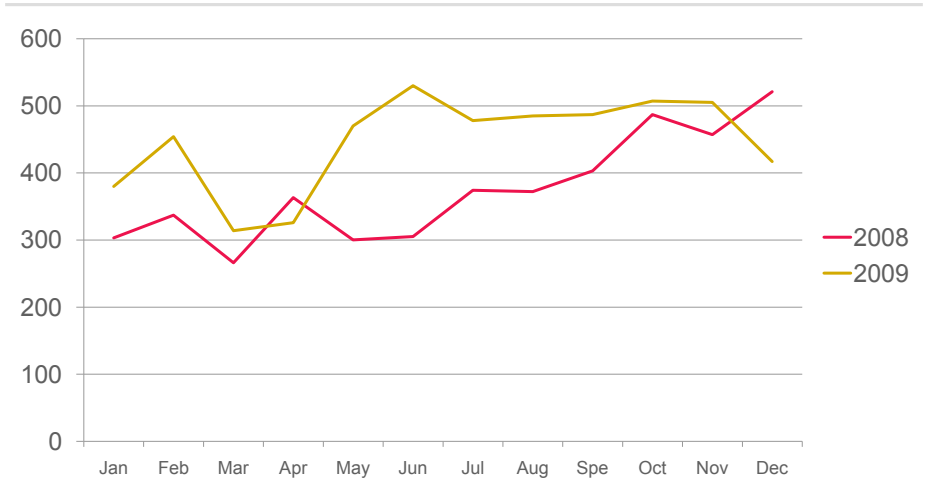
Experian operates a victim of fraud support service that helps consumers impacted by third-party / identity fraud to reclaim their identities and put right the damage done to their credit reports. Nick Mothershaw looks at the victims' experiences.

Victim volumes

Experian uses a range of measures to track identity fraud. Traditionally, this has centred on victims of fraud survey data, although this has recently been supplemented with additional data now being collected through National Hunter.

Over 5,000 identity fraud victims sought help from Experian in reclaiming their identities in 2009 – an increase of 20 percent on 2008 (Figure 8). Experian surveys the experiences of each of the victims it helps, providing valuable additional insight into the evolving nature of identity fraud. These findings are backed up by National Hunter data from 2009. Just 10 percent of attempted identity frauds reported to Experian during the period were in the first quarter of the year. This rose to reach 38 percent of cases in the final quarter.

Figure 8: Volume of cases reported to Experian by victims, 2008 and 2009



Source: Experian Victims of Fraud Survey (March 2010)

Younger groups more at risk

2009 saw a marked shift in the age of victims, with the 18 to 30 age group being increasingly targeted (up seven percent) and the 50+ age group dropping by a similar amount.

A detailed analysis of cases reported to Experian in 2009 using the Financial Strategy Segments (FSS) classification has revealed that both wealth and lifestyle attributes make consumers attractive to fraudsters. Figure 9 details the 10 most commonly-targeted groups in 2009, which are each given a risk score based on this propensity.

While the wealthiest sections of society continue to be at high risk of identity fraud attack, as mentioned earlier, fraudsters are now targeting the mass market (Figure 9).

For example, more affluent younger people feature prominently amongst the highest risk groups. Solid credit ratings and renting mean that groups such as the Up & Coming Elite – high-flying graduates privately renting in good areas – and those Looking to the Future – young singles in shared rented accommodation earning reasonable wages – are firmly on the fraudsters' radars, with risk scores of 293 and 268 respectively. With the average risk score for UK consumers being 100, these scores indicate that both groups are more than two-and-a-half times more likely to be targeted by fraudsters. Analysis of cases filed by lenders through the National Hunter fraud data sharing scheme confirms that fraudsters increasingly targeted younger groups throughout 2009.

Older and wealthier victims also feature strongly. Corporate Top Dogs – wealthy company directors and business owners – were the most at-risk group for identity fraud in 2009. A risk score of 306 signals this group as being more than three times more likely than the average UK consumer to fall victim to identity fraud. The Cream of the Crop – the highest income earners in premium price city flats and residences– with a risk score of 265, we're the fourth most at-risk group.

Likewise, Greys in the Pink – wealthy retired couples with high disposable incomes – were victims in 2009. This group has many investments, creating income and also paperwork which can be intercepted and the details used to commit fraud.

Figure 9: Top 10 FSS consumer types most at risk from identity fraud in 2009

2009 rank	Type	Description	Risk index score [7]
1	Corporate Top Dogs	Company directors and business owners. Very wealthy individuals at the pinnacle of successful careers	306
2	Up & Coming Elite	High-flying graduates privately renting in good areas while they pay off student debts and save for a mortgage deposit	293
3	Looking to the Future	Young singles often in shared rented accommodation earning reasonable wages and optimistic for the future	268
4	Cream of the Crop	Highest income earners in premium price city flats and residences	265
5	Greys in the Pink	Wealthy retired couples with high disposable income generated from their investments	192
6	Family Focused Finance	Busy, young families doing well. They have high child-related costs, little time for financial planning, a few savings and some debts	190
7	Opportunities & Overdrafts	Young, cohabiting couples and friends currently relying on overdrafts but with future potential	188
8	Asset-rich Achievers	Professionals who have had successful careers and are now approaching retirement. Likely to be in a senior management position with the salary to match	172
9	Fully Committed Funds	Heads of families with considerable incomes but with a very large mortgage leaving little spare to save	167
10	Getting by Alone	Young singles and single parents getting by with limited income in low value properties	162

Source: Experian (March 2010)

Identity fraud hotspots

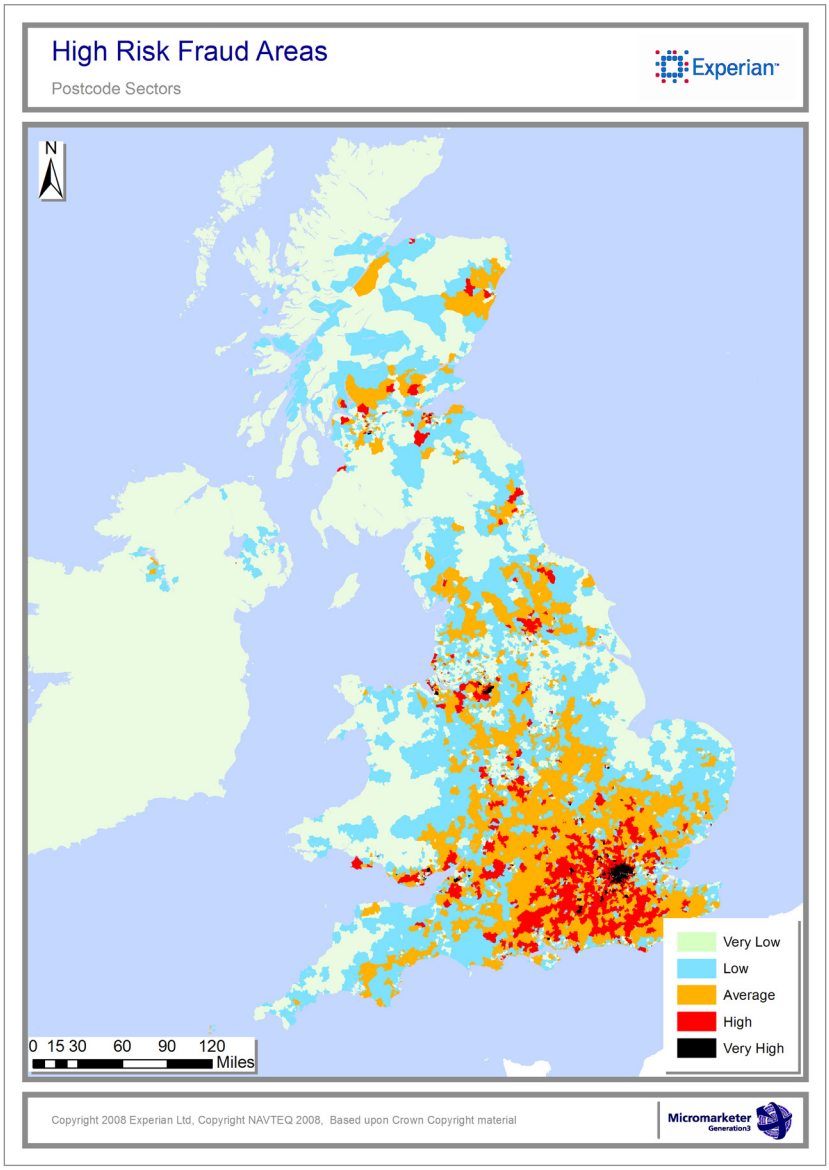
Using its research into the types of people most likely to become victims, Experian has been able to identify the UK's identity fraud hot spots – the areas that contain the highest proportions of most-at-risk residents. As seen in Figure 10, London remains the UK's overall fraud hotspot. Across the UK, districts with a high proportion of rental properties were especially vulnerable.

With high concentrations of the most targeted groups, London's Knightsbridge, Docklands and Blackwall districts are prime locations for identity fraud activity. This is consistent with our earlier observations about fraudsters attacking within striking distance of where they are based.

Outside of the capital, new-build locations with a large rental sector dominate. The Quays development in Salford, Liverpool Street in Manchester and Cardiff's dockside regeneration area also feature highly on Experian's risk indices.

[7] Risk indices show how much more or less likely individuals within a certain demographic group or location are to be impersonated by identity fraudsters, compared to a national average of 100. A score of 300 indicates that constituents are three times more likely to be targeted than the national average.

Figure 10: High risk fraud areas in 2009

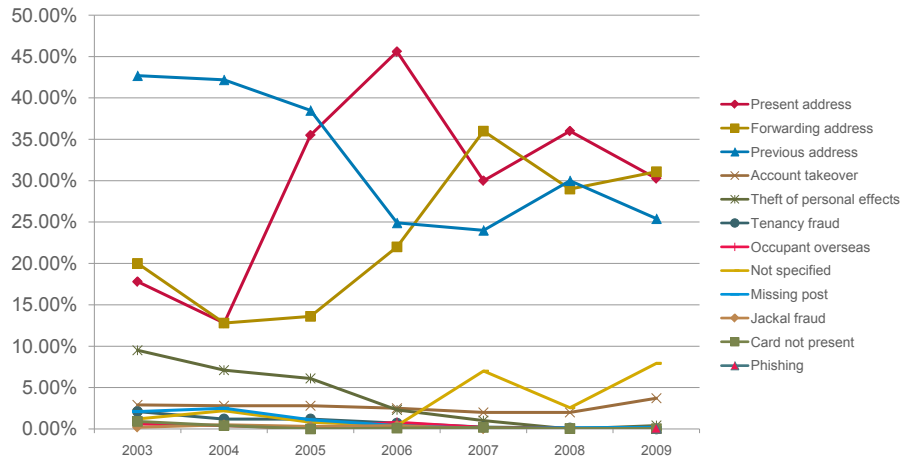


Source: Experian (March 2010)

Identity fraud modus operandi

Based on Experian's analysis, forwarding address fraud – where the fraudster redirects the victim's post to another address – was used in 31 percent of cases, suggesting the ongoing involvement of organised crime in this area. Present address fraud – a more opportunistic crime perpetrated by someone living at, or having access to the victim's current address – increased in 2009: this accounted for 30 percent of cases. Present address fraud often requires access to mail delivered to the address through collusion, interception or redirection.

Figure 11: Fraud type trends, 2009



Source: Experian Victims of Fraud Survey (March 2010)

Furthermore, National Hunter data supports this view (Figure 11). Across all product areas during 2009, the current address – which would include present address and forwarding address frauds – was used in 61 percent of cases of attempted fraud reported by organisations. Previous addresses accounted for 11 percent of fraud attempts.

Consumers must remain vigilant and take every precaution possible to protect their identities. It is important to be careful not to share personal information online and to shred sensitive documents, such as financial statements, before throwing them away. Regular credit report monitoring – so individuals can reassure themselves that no one has gained unauthorised access to their personal information and is abusing it to commit crime – offers the best level of protection.

5. Addressing the fraud cycle

Rising fraud levels mean that it has never been more important to ensure that applications for new credit facilities are analysed for signs of fraud. Graham Pitt, General Manager, Fraud and Identity Solutions at Experian, explains why it is critical that these capabilities are extended throughout the customer lifecycle, and that organisations start monitoring for suspicious activity and new frauds within their existing customer base.

Fraud in the open book

While much attention over recent years has focused on combating fraud at the point of application, less has been placed on looking for fraud within an organisation's open book. While efforts have quite rightly been focused on keeping the enemy from the gates, there is a significant threat posed by those that are already inside the castle.

Put into context, **Experian analysis of live data across a range of organisations indicates that, on average, around two percent of accounts in a portfolio show signs of suspicious activity and warrant further investigation**. There are potentially millions of open accounts with UK financial institutions that could expose the organisations to significant financial loss.

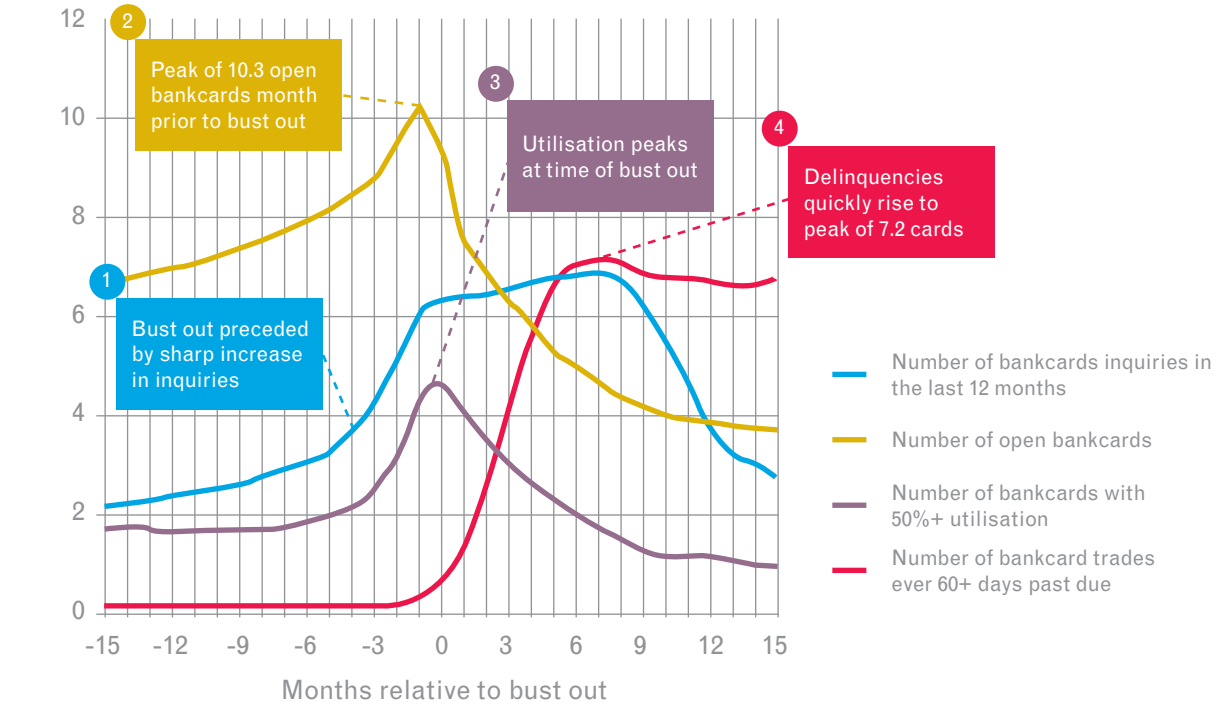
Sleeper / bust-out fraud

There are many reasons why a financial institution should monitor for signs of fraud in its open account book. The first and perhaps most pressing is the threat of sleeper / bust-out fraud, a growing area of concern for the industry.

Frauds of this type usually involve an organised fraudster who may start by opening a new savings or current account. Over a period of time, typically two years, the fraudster will operate the account in the manner of a good customer, in order to build a good credit history with the organisation. Typically, customers of this nature will be attractive prospects for the organisation's credit products and they may well be offered pre-approved credit facilities and generous credit payment terms.

At a point in time, the fraudster will suddenly increase their spending and acquire additional credit facilities, which they will then max out, and they will most likely withdraw all funds from the original accounts. They will also use all stockpiled cheques. Often this is the last activity the organisation might see.

Figure 12: Activity prior to bust-out fraud



Source: Experian (March 2010)

Figure 12, which is based on Experian analysis of bust-out frauds in the US, demonstrates how bust-out occurs over time and shows some of the attributes that are correlated to bust-out behaviour. It also shows how these attributes change significantly right before the bust-out behaviour occurs.

1. The number of bankcard inquiries increases steadily over time and about three months before bust out, they increase sharply.
2. The number of open bankcards also increases steadily over time and about three months before bust out, the number of open accounts increases sharply. The fraudsters are ramping up all the credit they can get prior to bust out.
3. Utilisation also remains steady until three months before bust out and then it increases significantly.
4. No delinquencies occur until the point of bust out and then they increase dramatically. They behave like good customers in order to receive the highest credit limits and maximum number of lines of credits.

After the bust out and delinquency occurs, the fraudsters are still trying to get more bankcards, but they can no longer get credit (as evident by the number of inquiries continuing to increase, but the number of bankcards decreasing). The number of open bankcards and the utilisation level also drop after the bust out because the accounts are being closed by the issuer or charged off.

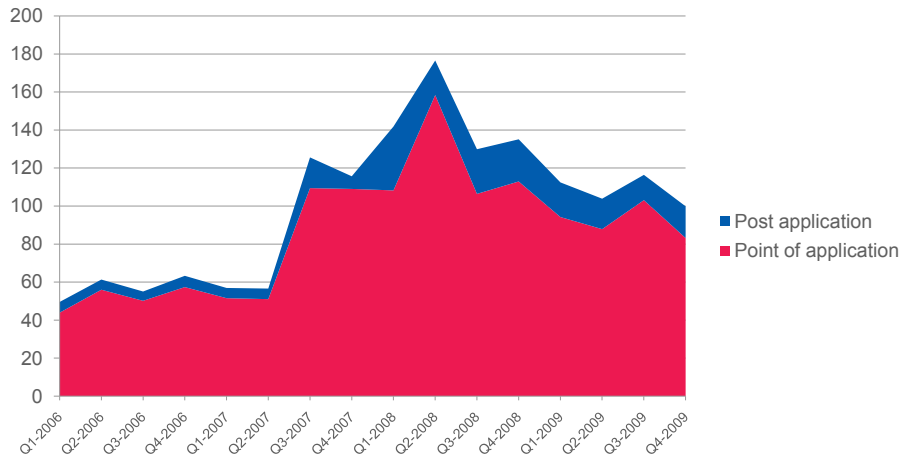
Within the retail banking environment, sleeper / bust-out fraud involves a deliberate manipulation of current account behaviour. The fraudster simulates normal banking activities in order to inflate credit scores and in turn, fool credit systems and behavioural scores into granting additional lending.

The identification of sleeper / bust-out is difficult for many organisations; however, there are often signs indicating that an account may be suspicious, if the organisation is looking for them. Organised fraudsters will often run multiple scams at the same time, which provides an opportunity for organisations that share data on these matters to alert, or possibly be alerted by, its peers.

This was a threat that relatively few organisations had actually anticipated, and, as such, these facilities have historically not had the same level of checks as credit accounts.

Fraud data compiled around the point of application does not tell the full story in this area; however, it is potentially indicative of a shift towards more sleeper / bust-out fraud. Experian has witnessed a doubling of fraudulent current account applications since 2006 (Figure 13), with an increasing proportion being spotted post-application. Experian is seeing many more organisations looking to boost their defences in this area.

Figure 13: Reported current account fraud 2006 – 2009



Index based on average number of all current account fraud reported to Experian each quarter over the period. Source: National Hunter (March 2010)

When first parties go bad

A second threat comes from first-party fraud. As previously mentioned, increasing numbers of consumers are inclined to 'go bad' when the economy takes a turn for the worse. Individuals who passed all checks when they first became a customer of an organisation may well have been honest at that point in time, however, if they later turned to fraud, the organisation would not have a clue. The use of shared data can help greatly. Should an individual try at first-party fraud against one bank, sharing that information with other organisations would limit their exposure and vice versa.

Money laundering and terrorist financing

A third reason for monitoring for signs of fraud in the open account base is to satisfy anti-money laundering and anti-terrorist financing obligations. Organisations that take money on deposit are obliged to confirm the identity of potential customers in order to ensure that they are not unwittingly hiding a trail of ill gotten gains, or acting as a conduit for putting money in the hands of terrorists. Establishing a customer's true identity at the point of application is absolutely vital. It is also good practice to ensure that regular checks are done to spot cases where new information becomes available, such as when an address or telephone number is flagged as being potentially suspicious by other organisations.

Account takeover

Finally, organised fraudsters are increasingly seeking to take over existing credit facilities to circumvent checks at the point of application. Organisations should not be reliant on their customers to spot unexplained items on their credit card or bank account statement – particularly in these days of paperless billing – and should be on the lookout for suspicious activity that suggests account takeover may have taken place. This includes the use of common addresses as takeover hubs, use of common contact details and sudden changes in account use behaviour.

Detecting fraud in the open account base

With account takeover on the increase and millions of accounts showing signs of suspicious activity, the industry should ensure that it is focused on addressing the potential ticking time bomb within the open account base.

It is as vital to monitor for signs of fraud in deposit-taking accounts as it is for credit accounts, and in the open account base as it is at the point of application. By sharing data as widely as possible on a regular basis, organisations can ensure their records are up to date and that any potentially fraudulent accounts are flagged as soon as possible.

6. Combating the threat from within

Louise Brown, General Manager, Experian Background Checking, discusses insider fraud, its typologies and how organisations should look to combat it.

Insider fraud – the theft of an organisation's assets by those it has placed in a position of trust – is an issue that affects almost all organisations. While, for many, the problem may be isolated to cases of expenses fiddling, there are organisations whose assets make them a prime target for fraudsters.

Companies more aware to insider fraud

Experian's own data suggests that companies are starting to become more aware of the threat posed from within, and are actively gearing up their processes to ensure they can combat it more effectively in the future. The volume of background checks carried out by Experian for clients increased by four percent in 2009, against a backdrop of depressed recruitment activity. This demonstrates a tightening of vetting practices across all sectors and company sizes.

Whether from organised criminals, opportunists or simply candidates lying on a CV to get a job, **Experian expects to see an unprecedented surge in fraud attempts over the next couple of years, as fraudsters seek to obtain assets or battle for work in a depressed job market.**

This trend is echoed by other sources of data. Fraud prevention service CIFAS reported that dishonest actions by staff to obtain benefits by theft and deception increased by 69 percent in the first half of 2009, compared with the last half of 2008[8]. KPMG, which analyses major fraud cases heard by UK Crown Courts, reported that staff accounted for £228 million worth of fraud across the private and public sectors in 2008, up from £81 million in 2007[9].

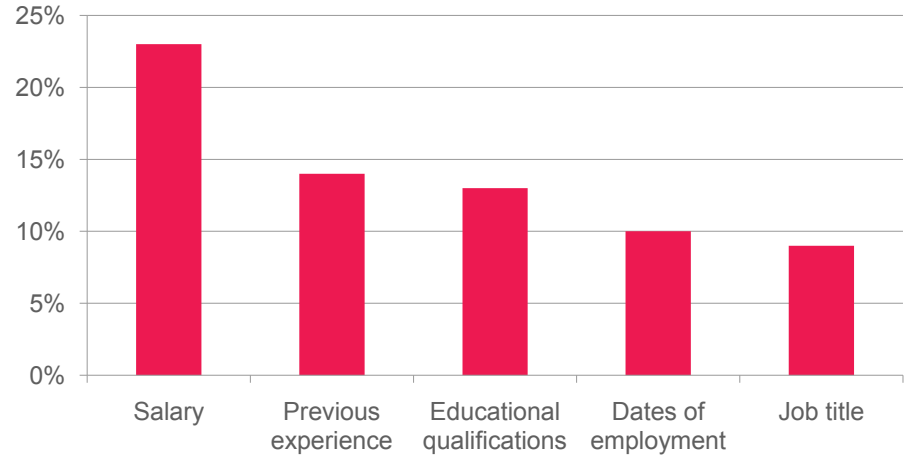
Insider fraud can originate in a number of areas from within an organisation, and from a range of different types of people. While many of those responsible are individual opportunists, looking to obtain assets or gain employment that they are not necessarily suitable for, improvements in anti-fraud measures designed to protect organisations from external threats have pushed an organised criminal element to consider new approaches. These include infiltrating the organisation themselves or coercing existing employees to act on their behalf.

CV misrepresentation

Certainly it would seem that lying on CVs is on the increase. Surveys suggest that as many as a quarter of job seekers deviate from the truth on their CV. Experian's own research finds that the most common distortions include salary (23 percent), level of previous experience (14 percent) and educational qualifications (13 percent), followed by dates of employment (10 percent) and job title (nine percent).

[8] Source: CIFAS, 27-Aug-09. http://www.cifas.org.uk/default.asp?edit_id=926-57
[9] Source: KPMG, 02-Feb-09. http://rd.kpmg.co.uk/mediareleases/15782.htm

Figure 14: Most common areas of CV misrepresentation



Source: Experian (March 2010)

Career cloning

In a survey last year, Experian found that 63 percent of professionals include career details in their personal profiles online and as many as one in 10 people now publish their whole CV on social networking sites such as LinkedIn, leaving themselves at risk of 'career cloning.' It is likely that fraudsters will increasingly look to take on the identities and career histories of third parties to secure employment within companies for the purposes of committing fraud.

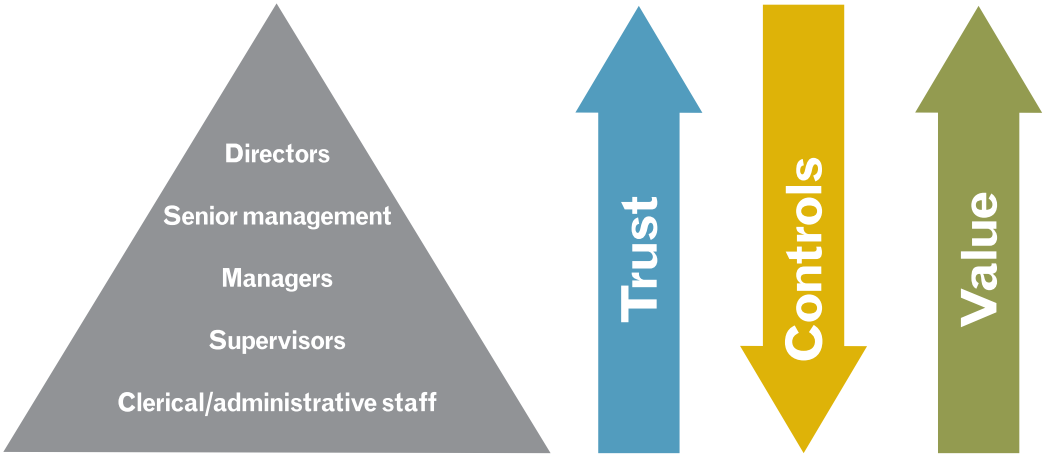
Recruiting an insider

Despite the best company security systems, criminals will find the weakest link, which more often than not is a person. Criminals have been known to hang around pubs and cafes near target organisations, seeking out disgruntled employees and those fearful of job losses and unemployment, who may be vulnerable to manipulation. Once targeted, the gangs will then attempt to bully or bribe employees to give up sensitive data that could be used to steal money or other assets. Threats of violence or blackmail may be extended to employees and their families if the orders of the gangs are not undertaken.

A more senior threat

It is not just those on lower pay grades that commit fraud. The threat includes senior level employees, who may well have implemented – or fall outside – the controls in place to monitor those deemed as higher-risk personnel. Senior personnel who deal with external suppliers, procurement and acquisitions have greater opportunities and a lower risk of detection as the focus in most organisations is elsewhere. Figures from BDO (79 percent) and KPMG (56 percent) indicate that the majority of financial losses attributable to insider fraud in 2008 were down to those in managerial positions. **With tighter economic conditions resulting in pay freezes and relatively low wage increases where they are granted, we could well see increasing numbers of those higher up the organisational pyramid looking to commit insider fraud to maintain their lifestyles.**

Figure 15: Insider fraud pyramid



Source: Experian (March 2010)

Frauds more commonly committed by more senior personnel within organisations include: setting up false suppliers to purchase goods and services that are over-priced or never received; sanctioning contracts to companies for goods and services in exchange for kickbacks; embezzlement of company funds; false cheque / electronic payments; placing fictitious staff on the payroll; and falsifying sales figures to increase bonus payments.

Combating insider fraud

The best way to combat the insider fraud threat is through a multi-stage employee vetting process that enables the organisation to have a clear picture of the candidate from a variety of data sources.

At the recruitment stage, organisations need to be sure they know the true identity of the candidate and whether they have any criminal convictions, as well as an understanding of the individual's financial picture. Client experience has also shown that there is a 15 percent drop-out rate when applicants are made aware that background checking is involved in the recruitment process, highlighting the strength of robust checking procedures in deterring time wasters and potential fraudsters.

Criminal records and financial data should play a key role in the recruitment process as they can highlight red flags such as convictions, bankruptcies and other adverse data, which are valuable warning signs into a candidate's character and suitability, as well as those potentially most vulnerable to coercion from the criminal element.

While organisations may not wish to appear to doubt the word of the candidate, the importance of criminal records checks should not be underestimated. They can protect an organisation from hiring someone who may be unsuitable or even dangerous to the organisation's staff and reputation.

Traditional CV checks should also be undertaken. Discrepancies and falsehoods on CVs and job applications provide an indication into the character of a candidate. If a person is willing to deceive on a CV, then they do not possess the integrity that employers expect.

Employee vetting should not, however, stop at the point of recruitment. Monitoring of existing staff is just as important, and many of the checks used in the recruitment process are valid for existing employees too. There are a number of early warning signs that may be indicators of staff fraud including employees living beyond their means, employees under financial pressure, and employees not wanting time off or being unwilling to change jobs which should be considered as part of an effective monitoring system.

There are a wide range of tools and techniques at employers' disposal for deterring and detecting insider fraud. These can range from CCTV, to protect against physical losses, through to complex software analytics that can highlight unusual patterns of behaviour on systems that hold commercially sensitive and proprietary information. It is important, however, to balance privacy rights of employees with the need to protect the business. Clear and well-communicated policies that set out the organisation's stance on fraud and its approach to tackling it also provide an opportunity to explain to employees why anti-fraud measures are so important.

Organisations are increasingly waking up to the threat from within. While much of the effort should go into the recruitment process, to **truly safeguard against insider fraud it is important to maintain an element of screening throughout the employment contract.**

7. Experian's fraud prevention expertise

Fraud is an increasingly prominent and costly business issue for many organisations. Experian's data assets and fraud products are unique and over 300 blue-chip clients across many market sectors help prevent fraud. Experian is constantly investing in new products and working with organisations and industry bodies to stay one step ahead of the fraudsters.

Application fraud
Fraud is the biggest cause of revenue loss for financial, telecommunications and insurance organisations and the resulting losses always affect profitability. Our software and information will help you to detect potentially fraudulent applications even before a customer is accepted, in a speedy and efficient way.

Authentication
Experian can provide you with instant verification, validation and authentication tools for preventing fraud in real time, while conducting secure online and call centre transactions. Experian can also provide you with the confidence that employees are who they say they are and are qualified to do the job with its Background Checking services.

Open account fraud
Experian can monitor account patterns and assess customer behaviour based on the likelihood of them committing 'open account fraud' and preventing 'bust-out' or 'sleeper' fraud.

Claims
Experian develops products specifically for the insurance industry that verify information, quantify risk and investigate and prevent fraudulent claims.

Identity fraud protection
Experian can validate a customer's bank account details to confirm that the person that you are interacting with is who they say they are. Experian can also help your organisation to protect your customers and staff in the event of ID fraud.

Data breach response management
Experian provides data breach response management to protect customers and staff in the event of a data breach, for example through unauthorised access to personal information such as bank account details.

Vehicle history
Experian's range of vehicle history products and services are specifically developed for the automotive industry and help to protect your business and your brand by reducing your exposure to risk.

Landmark House
Experian Way
NG2 Business Park
Nottingham
NG80 1ZZ
United Kingdom
www.experian.co.uk