

The Insight Report

Victims of Fraud Survey - March 2010



Contents

1. Introduction	Page 3
2. Executive Summary	Page 4
3. The bigger picture	Page 5
4. The most likely victims	Page 9
5. The UK's identity fraud hotspots	Page 11
6. Victims of fraud case studies	Page 17
7. Top tips for keeping your identity safe	Page 19

Introduction

Pete Turner, Managing Director, Experian Interactive

Identity fraud is often described as a crime that knows no boundaries - one that can be completely devastating for victims. Considered a 'silent crime', because it can take so long to discover, when a fraudster strikes, the victim can be left penniless and, without help, faces an uphill struggle to restore their good name.

The only certainty with fraud is that it is never going away. It is an evolving crime committed by both the opportunist thief and by more sinister, organised criminal gangs.

One of the problems is that danger lurks in the most innocuous of places. Social networking sites, careless friends, unsolicited e-mails, uncollected post and even disgruntled employees can all be valuable sources of information for unscrupulous individuals.

The message to consumers is that they must remain vigilant and take every precaution possible. 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.

One of the biggest difficulties facing consumers is the length of time it can take to discover identity fraud has taken place. In 2009, it took an average of 416 days for fraud victims to realise they had been attacked. This gave fraudsters more than a year to compromise their victims' accounts, build up debts in their names, destroy their credit ratings and then move on to someone else.

Unsurprisingly, Experian's research in this report shows it is the UK's wealthiest citizens who are most likely to be targeted by fraudsters, with the residents of the London Borough of Kensington at greatest risk of an attack. Perhaps more interesting is that younger, less affluent people, who live in rented accommodation and those who change address frequently are increasingly becoming victims. Shared communal halls or a failure to redirect mail make it relatively easy for outsiders to obtain private letters. Fraudsters are going mainstream.

Given that fraud is never going away, and Experian's Insight Report confirms that no one is immune, it's up to all of us to minimise the impact it can have.

The only certainty with fraud is that it is never going away

2. Executive Summary

The key findings from the report are:

- Experian saw a 20 percent increase in the number of victims of identity fraud seeking help reclaiming their identities in 2009 compared to 2008.
- Less affluent people are increasingly more likely to become victims of identity fraud as organised criminals and opportunists turn to the mass market.
- Those people most at risk include people living in flats with communal halls and those who move frequently.
- The two riskiest postcodes are SW1X 8, centred on Kinnerton Street near Knightsbridge in London and W1K 7, centred on Park Street, near London's Park Lane. Residents living in these codes are four times more likely to be a victim of identity fraud than the average resident.
- It is taking people longer to discover they have become a victim of identity fraud. In 2009 it took 416 days, up from 399 days in 2008.
- Most victims, 61 per cent, first discovered their identity had been stolen by checking their credit report.
- The average financial loss per victim is £1,100.
- Criminals are increasingly likely to take over an existing account rather than set up a new one to avoid stringent fraud checks built into the credit application process.
- Criminals redirected their victim's post to another address in almost a third of cases in 2009.

Definition:

Identity fraud (also called third-party fraud) can occur when someone uses another person's identity to commit a crime, either by applying for credit, goods or services in their name ('impersonation') or by fraudulently using ('taking over') their existing accounts. In order to do this, fraudsters often first commit 'identity theft' - obtaining the victim's personal information without their permission.

3. The bigger picture

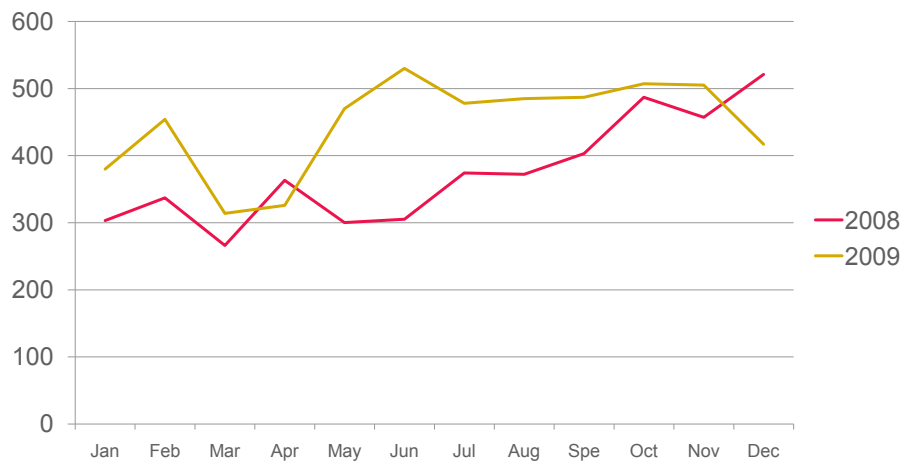
Identity fraud cases

The number of identity fraud victims who sought help from Experian last year was almost 20 percent higher than the year before. In 2009, 5,353 new victims contacted its Victims of Fraud service for help in reclaiming their identities. In 2008, the figure was 4,490.

As shown in Figure 1, year on year, fraud attempts rose most sharply in early summer, rising by 57 percent in May to 470 cases, and by 74 percent in June to 530 cases – the highest number ever reported to Experian in any single month. They had, however, fallen back down to close to 400 a month by December. It remains to be seen if this downward trend continues, or the fraudsters just stopped for a Christmas break.

The number of identity fraud victims who sought help from Experian last year was up almost 20 percent

Figure 1: Volume of cases reported to Experian by victims, 2008 and 2009



Source: Experian Victims of Fraud Survey (March 2010)

The average financial loss per person was £1,100 in 2009, marginally higher than the 2008 figure of £1,040. However, the most extreme loss reported to Experian was for almost £59,000.

Hire purchase saw average losses nearly double in 2009 from £16,544 to £31,112, while credit and store cards, which accounted for 55 percent of identity fraud losses, saw the average loss fall to £1,753 per account, down £154 on 2008. Mail order, which accounted for seven per cent, also saw average losses fall by £31 year on year to £169. Fraud on mobile phone accounts accounted for three per cent, with an average loss of £318, almost the same as last year's £321.

Discovering fraud

Victims of identity fraud typically only discover the fraud when they review their credit reports. In 2009, nearly three in five of victims discovered that their identity had been compromised by checking their credit report.

For one in ten, the first clue they had that they'd become a victim of identity fraud was a notification of fraud from a financial services company or a letter chasing an unknown debt.

Despite consumers being more aware than ever of the risk of identity fraud, it is taking victims longer to discover their identity is being used fraudulently. In 2008, it took victims an average of 399 days to discover they had become a victim of fraud. In 2009, this rose to 416 days, giving criminals more than 13 months to open new lines of credit and destroy an individual's credit rating.

**416: the average number of days
it took someone to discover they
were a victim of identity fraud**

How identity fraud is committed

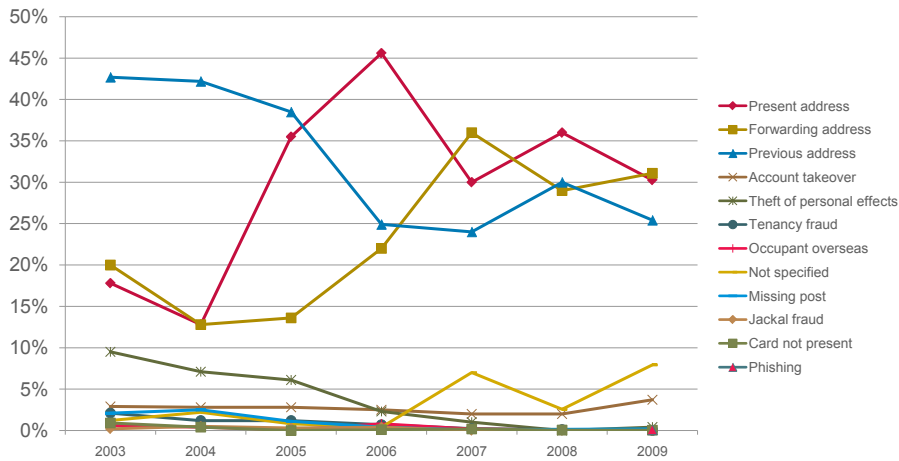
Experian's analysis shows that most identity fraud is premeditated. In 2009, as shown in Figure 2, the most common technique used by criminals was to redirect their victim's post to another address. Known as forwarding-address fraud, it was used in 31 percent of cases. Almost as common was present-address fraud, which typically requires some form of mail interception. It is usually committed by someone living at, or having access to, the victim's current address and often involves a shared mailbox or communal hallway. This method accounted for 30 percent of cases.

Previous-address fraud fell to 25 percent of reported fraud. This is typically an opportunist crime – the victim changes address but fails to redirect their post or does not notify organisations such as banks or credit card companies. Someone with access to the old address then uses the victim's details to open new accounts in their name.

Together, these three types of fraud show why people living in rented accommodation – with shared letterboxes or a communal hall for postal deliveries – and frequent home movers are more at risk of identity fraud than others.

Account takeover fraud, where criminals take over a victim's existing bank or credit card account, doubled to four percent of cases. Internet fraud phishing, through which account details are obtained via false e-mails or a fake website, made its appearance for the first time this year.

Figure 2: Fraud type trends, 2009



Source: Experian Victims of Fraud Survey (March 2010)

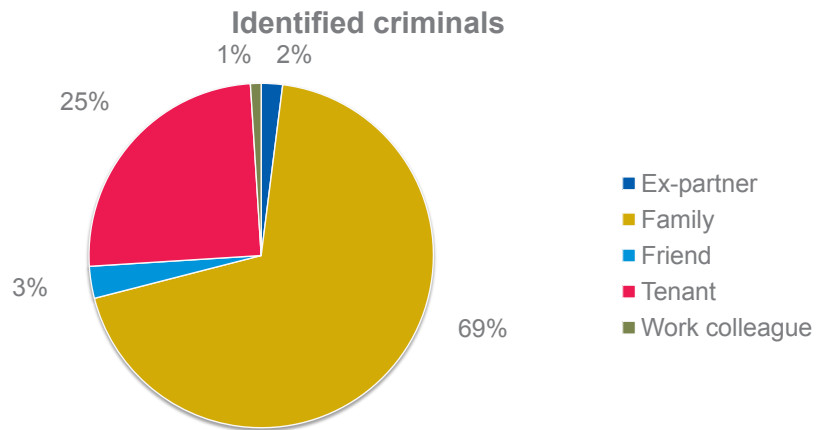
The prime suspects

In the majority of cases, victims were unaware or unwilling to disclose who they believed had hijacked their identities. Only 31 percent were aware and prepared to disclose who they believed had committed the fraud.

Of those who believed that they knew the perpetrator, the majority suspected a family member or a tenant. Family members – the people most likely to have easy access to personal details – are cited by over two-thirds of those who believe they know who carried out the crime. Tenants are suspected of being the guilty party by a quarter of victims, and of committing previous-address fraud.

Friends represent three percent of suspected identity fraudsters, followed by ex-partners (two per cent). This year, for the first time, work colleagues have been identified in one percent of cases where the perpetrator is known or suspected. All of these groups are in a position to know a lot about their victims – and to take advantage of that knowledge.

Figure 3: Suspected fraudsters (where opinion given)



Source: Experian Victims of Fraud Survey (March 2010)

Of those who believed that they knew the perpetrator, the majority suspected a family member

4. The most likely victims

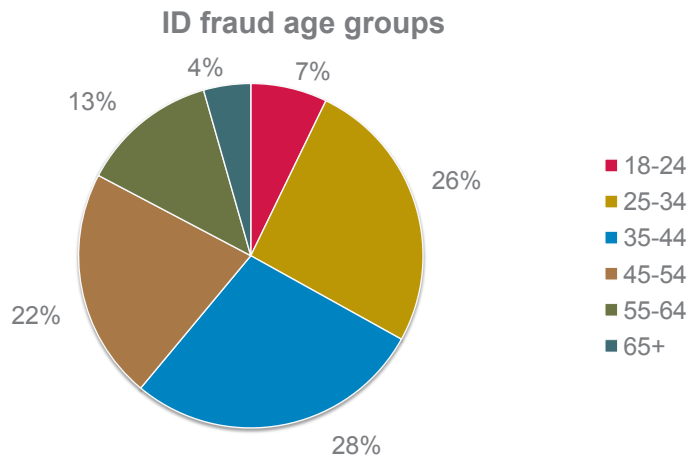
Age and gender of victims

The age of fraud victims has changed and younger people are more likely to suffer than ever before.

2009 saw a three percent increase in the number of 18 - 34 year olds affected by identity fraud. This age group now accounts for a third of all those affected. However, in tandem, the absolute number of older people being targeted has also risen with, in particular, an increase in the number of those near or at retirement becoming victims.

The typical identity fraud victim in 2009 was more likely to be male than female (60:40) and in his late 30s or early 40s. The average age of a victim was 42, and more than three-quarters of all victims were aged between 25 and 54.

Age and gender of victims



Source: Experian Victims of Fraud Survey (March 2010)

Victim classification

As part of this year's Victims of Fraud Survey, a detailed analysis of new cases of identity fraud has allowed Experian to identify who is most likely to be targeted.

Mapping frauds to Experian's Financial Strategy Segments (FSS) consumer classification, which groups people according to their financial behaviour, reveals that there has been a shift to less wealthy consumers, from those with obvious wealth. These people still have a good credit history but are less likely to actively manage their finances and notice quickly if their identity has been stolen.

To provide a comparative indication of risk, each group is given a risk index score, with the average risk being 100. The higher the score, the greater the risk. For example, a score of 300 means those in this group are three times more likely to be a victim than the average UK resident.

The analysis shows the Up and Coming Elite and Looking to the Future groups, with scores of 293 and 268 respectively, are high-risk groups. These two groups represent young singles and high-flying graduates who are likely to rent and are therefore at greater risk of fraud. They are attractive to criminals because they often work in professional occupations and are relatively wealthy.

While fraudsters' attentions may be moving around, affluent people still continue to be at high risk. Corporate Top Dogs – wealthy directors and business owners – were the most commonly targeted group in 2009, rising from fourth place in 2008. With a risk score of 306, this group has more than treble the average risk of having their identities stolen. Another well-off grouping, Cream of the Crop, with high incomes and living in the best parts of the UK's largest cities, are in this year's fourth place, with a score of 265.

Pensioners make it into the top ten this year, an increase noted in the average age of victims. Greys in the Pink, wealthy retired couples with a high disposable income, were frequently targeted in 2009 resulting in a risk score of 192. This group typically has many investments which generate paperwork that can be intercepted and used to commit fraud. They might also be more vulnerable to scams such as phishing e-mails.

It's not only the affluent who are at risk. Young people living alone and single parents, both on limited incomes and likely to rent, make the top ten as well. People who are Getting by Alone have a risk score of 162. Again the dangers of communal hallways and postal deliveries contribute to their overall risk of becoming a victim of identity fraud.

Other groups at risk include Opportunities and Overdrafts – again a younger-than-average group – with a risk score of 188. The Family Focused Finance group, who have high child-related costs and few savings, and Fully Committed Funds, who may have big incomes often with big mortgages to match, score 190 and 167 respectively.

Figure 5: Top 10 FSS consumer types at risk from identity fraud

Index shows level of risk, where 100 = UK average

2009 rank	Type	Description	Risk index score
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 and 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 Victims of Fraud Survey (March 2010)

5. The UK's identity fraud hotspots

Alongside research into the types of people most likely to become victims, the UK's identity fraud hotspots – the areas containing the highest proportions of most-at-risk residents – can also be identified.

The analysis looks at the towns, territories and individual postal sectors most at risk. Again, analysis of locations is comparable against a national average of 100.

Most-at-risk towns/territories

London remains the UK's overall fraud hotspot – residents have an average risk score of 260. Well-off districts such as Kensington and Chelsea dominate the capital's top ten, with index scores of 370 and 366 respectively – and almost four times the risk of the average address.

Figure 6: Top ten most-at-risk territories within London

Index shows level of risk, where 100 = UK average

2009 rank	Territory	Risk index score
1	Kensington	370
2	Chelsea – Kings Road	366
3	Victoria – Victoria Street area	354
4	Liverpool Street & Bishopsgate	350
5	London West End	350
6	Hammersmith – King Street	346
7	Stratford	346
8	Queensway	344
9	Cheapside	341
10	Wandsworth – Clapham Junction	340

Source: Experian Victims of Fraud Survey (March 2010)

Outside London, commuter belts and affluent areas with a high proportion of rental properties are especially vulnerable. They include St Albans (211), Guildford (201) and Epsom (198).

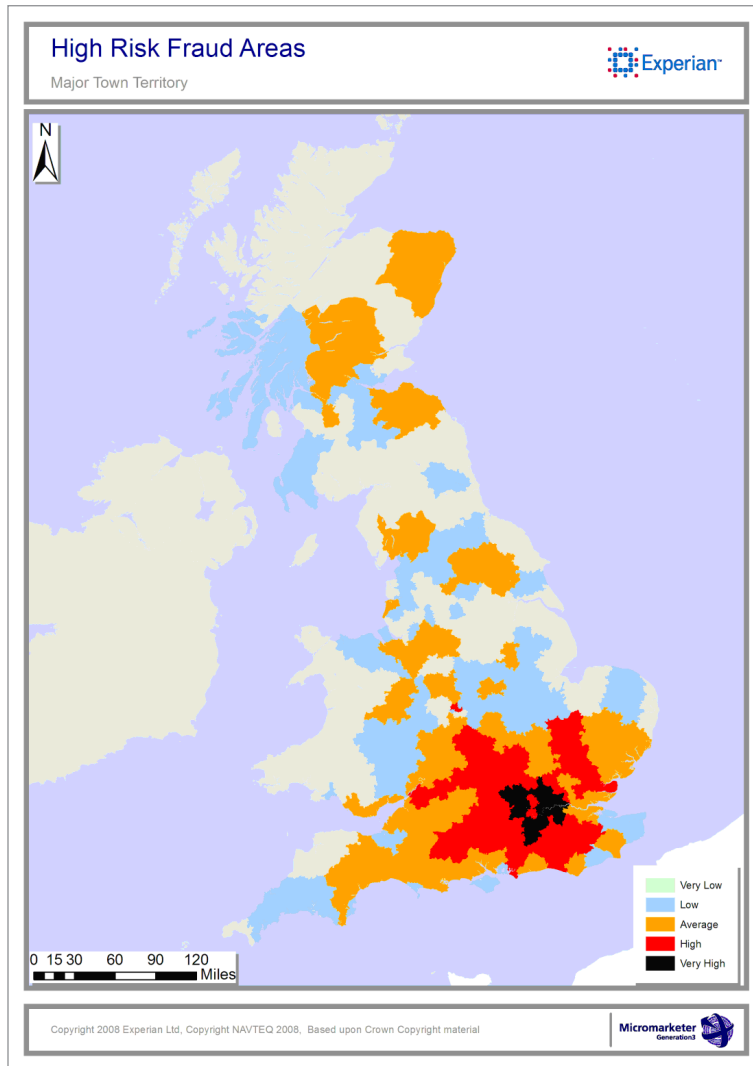
Scotland is less risky, with Edinburgh's Princes Street scoring 117 and its Gyle area 116, while Glasgow Central is just above average at 106.

Figure 7: Top ten most-at-risk territories excluding London

2009 rank	Territory	Risk index score
1	St Albans	211
2	Guildford	201
3	Epsom	198
4	Woking	195
5	Maidenhead	195
6	High Wycombe	190
7	Bromley	181
8	Slough	179
9	Watford – Central	178
10	Bracknell	177

Source: Experian Victims of Fraud Survey (March 2010)

Figure 8: UK high-risk fraud areas



Source: Experian Victims of Fraud Survey (March 2010)

The country's most vulnerable location is SW1X 8, centred on Kinnerton Street near Knightsbridge

Postal sector analysis

At a postal sector level – which brings the analysis down to individual neighbourhoods – the ten most at risk postcodes are all in affluent parts of London, including parts of Chelsea and Knightsbridge, as well as up-and-coming areas within Canary Wharf and Blackwall.

The country's most vulnerable location is SW1X 8, centred on Kinnerton Street near Knightsbridge in London, with a score of 408. This is closely followed by W1K 7, centred on Park Street, near London's Park Lane, with a score of 407. Knightsbridge itself, postal code SW1X 7 weighed in at 401. Residents of all three postal sectors are some four times more likely to have their identity cloned than the average person.

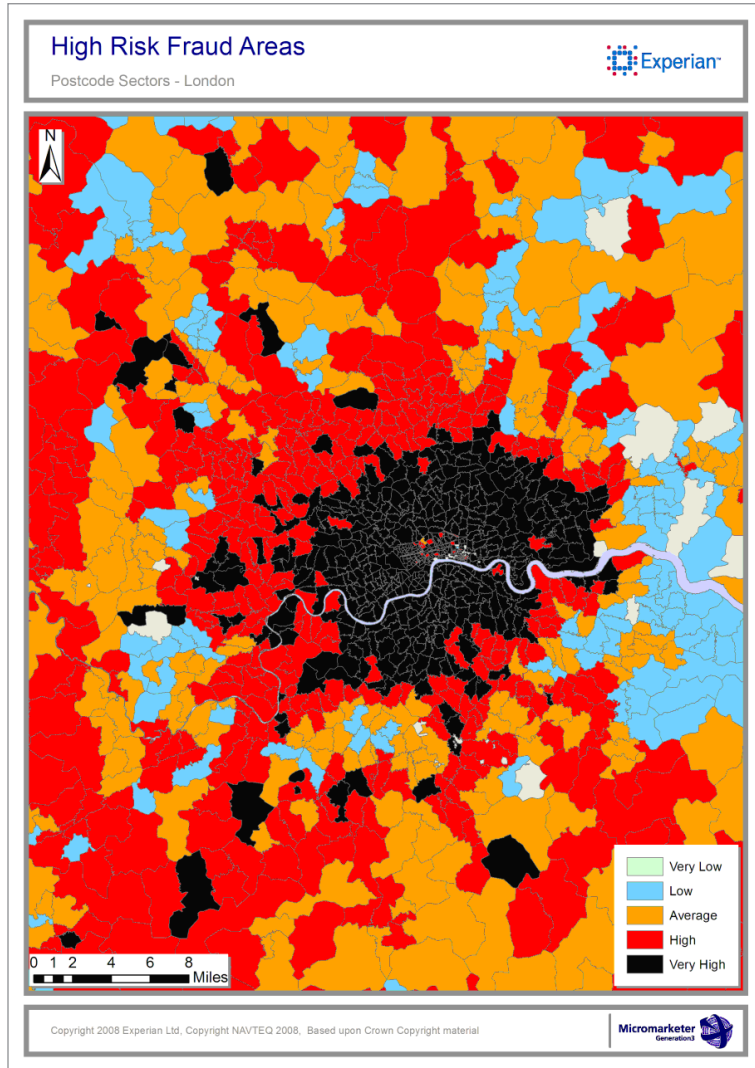
Figure 9: Top ten most-at-risk postal sectors within London

Index shows level of risk, where 100 = UK average.

2009 rank	Postal sector	Risk index score
1	SW1X 8 – Kinnerton Street, London	408
2	W1K 7 – Park Street, London	407
3	SW1X 7 – Knightsbridge, London	401
4	W1J 5 – Hill Street, London	400
5	SW3 1 – Brompton Road, London	398
6	SW17 6 – Macmillan Way, London	397
7	E14 5 – Chancellor Passage, Canary Wharf, London	396
8	SW1X 0 – Lennox Gardens, London	396
9	W1K 2 – South Audley Street, London	395
10	E14 2 – Blackwall, London	393

Source: Experian Victims of Fraud Survey (March 2010)

Figure 10: London high-risk fraud areas



Source: Experian Victims of Fraud Survey (March 2010)

Outside London, new-build locations with a large rental sector and flats with shared letterboxes or hallways dominate the at-risk top ten. It is interesting to note, however, that nowhere outside London presents as high a risk of identity fraud as the top ten within the capital.

Top, excluding London, with a risk score of 390, is the Quays development in Salford M50 3, which comprises blocks of new property, creating a classic rental zone occupied by relatively well-off younger people.

The next riskiest place is Liverpool Road in Manchester M3 4 – another location with a high proportion of new-build houses and flats. Many are rented and the area scores 352, making its residents three-and-a-half times more likely to be a victim of identity fraud than the national average.

Further new-build locations follow. Fell Road in Westbury, Wiltshire, BA13 2, scores 350, closely followed by Morrison Street in Glasgow G5 8 at 348. Liverpool's L3 4 regeneration sector and new business park by the Mersey has a risk score of 343, and Cardiff's regeneration area around the docks at CF10 4 comes in at 334. Leafy Maple Road in Surbiton KT6 4, meanwhile, offers residents more than three times the average chance of having their identity stolen, with a risk score of 333.

Living in a relatively new property need not be an indicator of high risk. The safest postal sectors in the country are recent estates in Gateshead at NE10 8 and East Denton, Newcastle upon Tyne NE5 2, both with a risk score of 18, less than a fifth of the national average. Joining them on 18 is the Cathays area of Cardiff CF24 4, a well-preserved Victorian area just three miles from the high-ranking docks with almost 19 times less risk of identity fraud.

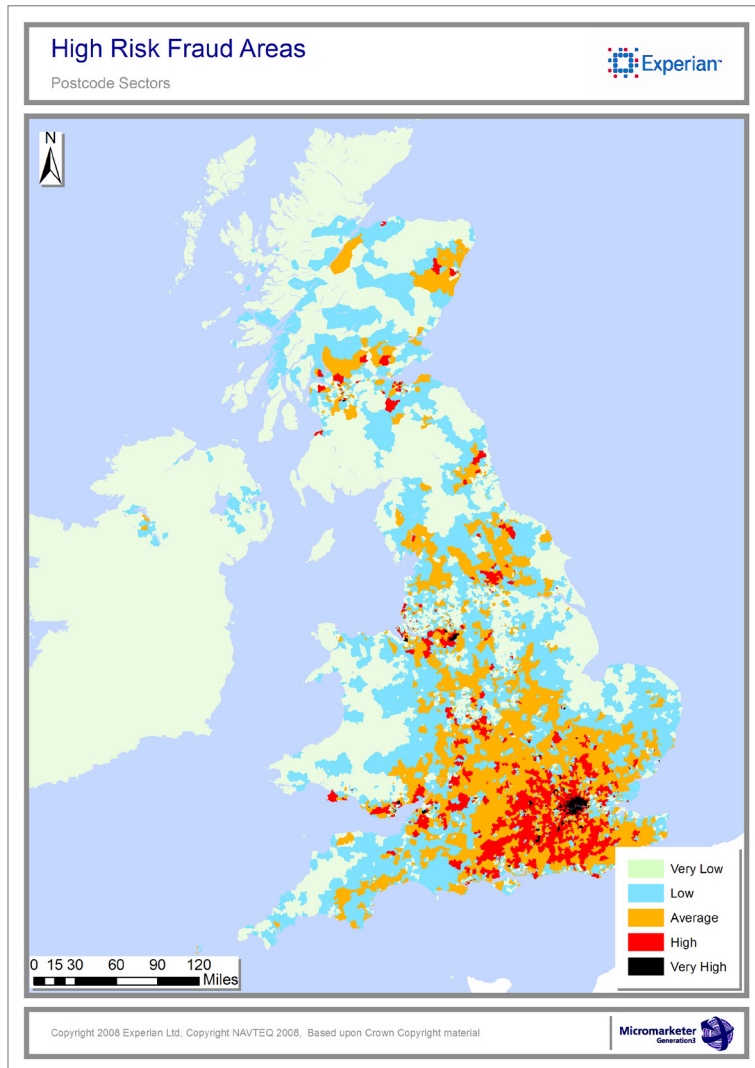
Figure 11: Top ten most-at-risk postal sectors excluding London

Index shows level of risk, where 100 = UK average.

2009 rank	Postal sector	Risk index score
1	M50 3 – The Quays, Salford	390
2	M3 4 – Liverpool Road, Manchester	352
3	BA13 2 - Fell Road, Westbury	350
4	G5 8 – Morrison Street, Glasgow	348
5	L3 4 – Liverpool (inc Brunswick Business Park)	343
6	CR3 7 – Woldingham	340
7	CF10 4 – Cardiff (inc Docks)	334
8	KT6 4 – Maple Road, Surbiton	333
9	WD18 8 – Greenhill Crescent, Watford	330
10	EH3 6 – Cumberland Street, Edinburgh	328

Source: Experian Victims of Fraud Survey (March 2010)

Figure 12: Identity fraud risk across the UK



Source: Experian Victims of Fraud Survey (March 2010)

6. Victims of fraud case studies

Sirisha Kodakandla

After working a 12 hour day, checking her post was not high on Sirisha Kodakandla's list of priorities, which is why she didn't notice post was going missing. Since she lived in rented accommodation with a shared hall, it allowed someone to intercept and try to open credit accounts in her name, using her date of birth, work number, work address and other details stolen from the mail.

"When I was studying for exams in 2007, I got my credit report and found that 32 credit applications had been made in my name but none of them had been successful, so I thought nothing of it," says Sirisha, 27, a care home officer. "It was by chance, after seeing an advert, I signed up for CreditExpert in January 2008."

A few weeks after signing up, more false applications started appearing on her report and Sirisha started to receive e-mail alerts from CreditExpert.co.uk flagging significant changes to her credit report. There were multiple credit card and store card applications, a catalogue and even mobile phones. She contacted Experian's Victims of Fraud team which contacted all the lenders who received false applications, to have them removed from her report. She now has a flag on her account telling lenders to contact her and ask for a password when they check her report as part of their credit application process.

"I am really glad I joined CreditExpert," says Sirisha. "If it hadn't been for them, I wouldn't have known about these applications until it was too late and I could have lost thousands. Instead, I've lost nothing."

Amy Gibbons

Amy Gibbons checks all her statements regularly, shreds sensitive documents and joined Experian's CreditExpert service when she was due to remortgage, so she could see whether her credit report needed improving before she made any applications.

So when several statements for one of her credit cards went astray, she swung into action.

"I kept it for emergencies and it should have had a zero balance, which is probably why it initially slipped my mind," says Amy, a 29-year-old quality assurance manager from Spalding, Lincolnshire. "I went online to find the electronic statements and couldn't believe it when I saw a couple of cash transfers, one for £500 and the other for £2,300.

"I called the card issuer, which claimed I'd transferred the money to my bank account – but it was a bank I've never used. Then I asked where the statements had gone, and was told I'd changed my address from Spalding to Dagenham, Essex. I've never even been to Dagenham. They said it looked as if I was the victim of identity fraud and cancelled the card."

The question was how anyone had managed to take over the password-protected account. It turned out that, if a cardholder forgot his or her password, they could also get online access by using their date of birth and mother's maiden name.

"The card fraud department said it looked as if someone had got hold of my full name and address, and then bought a copy of my birth certificate, which would have contained enough information to take over my account," says Amy.

The fraud department also advised her to check her credit report in case the criminals had done anything else. Luckily, the card fraud was the only illicit activity on record.

Her credit report is now flagged so that new applications for credit are not processed until Amy has been contacted by the lender.

Andy Hindmarch

Computer programmer Andy Hindmarch didn't owe a penny to anyone back in June 2009, when he decided to buy a new car. But when he tried to get credit to finance the vehicle, he was turned down.

"I was stunned," says Andy, 32. "I'd never been refused credit and hadn't even applied for any for years."

He decided to find out why and looked at his credit report via CreditExpert.co.uk. There he found an address linked to his own, hundreds of miles away from his home in Newcastle upon Tyne.

"Somehow, criminals had got hold of some of my details back in 2006 and had used an address very similar to mine but in a different city. They'd run up a credit card debt of around £22,000, including interest, over three years. I was therefore seen as a bad risk," he says.

Andy called the credit card company, only to find the card and its debts had been sold. "The new company passed the buck back to the old one. I was getting nowhere."

He called Experian's Victims of Fraud team. "They were brilliant," says Andy. "I got a crime report number from the police and Experian did the rest. The linked address was removed from my credit report and with it, the criminals' debt."

The process took ten weeks and Andy now checks his credit report regularly and shreds all post showing his name and address before throwing it away.

Robin Storer

When Robin Storer moved from the North West to Swindon, Wiltshire in February 2009, he gave his new address to the utility companies, financial providers and friends, rather than redirect his mail.

"I received a letter from a credit card company," says Robin, a civil servant. "It asked me to contact them urgently and I was suspicious. I'd heard of phishing letters and thought this could be one of them, so I got my credit report, just to check."

His credit report revealed a catalogue of fraud. Not only was the original credit card listed, but there were six other unfamiliar accounts, including a further credit card, store cards and catalogue accounts with outstanding debt totalling £10,000. And there had been 17 searches of his report, relating to more applications for credit.

"Initially, I went into shock," says Robin, 44. "I didn't know what to do. Somebody had taken out all this credit pretending to be me. The record showed that, at first, they'd made regular payments and then slipped behind until they defaulted."

Robin called Experian's CreditExpert service for advice. He was advised to write to each creditor, explain what had happened and enclose proof that he had moved. CreditExpert also contacted the creditors.

"Within a few weeks, it had all been sorted out and the items were removed from my credit report, thanks to the advice I received from CreditExpert," says Robin, who is planning to move house again later this year. "This time I will have all my post redirected and I now keep an eye on my credit report."

7. Top tips for keeping your identity safe

- **Shred sensitive documents, such as financial statements, before throwing them away.** Delete your name, address and account number from catalogues and direct mail offers too – or shred those pages as well.
- **Never share passwords or PINs and don't write them down.** Don't use the same PINs and passwords for multiple accounts – if one account is compromised, you've given away the keys to all your financial affairs.
- **Redirect your post for at least six months after you move house.** Give your new address to any organisations who regularly contact you.
- **Ask the Post Office to investigate if important mail does not arrive.** It could have been intercepted or redirected. If you have a shared letterbox or communal hallway where post could be taken, ask for secure, individual facilities.
- **Keep hackers and viruses out of your computer.** Install the latest security software on your computer and update these programs regularly. Only use secure websites for online shopping – look for the closed padlock symbol or https:// at the start of the address.
- **Never reply to e-mails asking for information such as account numbers, passwords and PINs.** Don't click through to any website they direct you to. Check with the organisation the e-mail appears to come from, using an existing number or e-mail address, the phone book or a directory enquiries service. Never use the number given on the e-mail.
- **Don't give personal information to cold callers.** This applies to the phone, the internet and face to face.
- **Limit the information you share on social networks.** Be especially careful of giving details such as dates of birth or children's names that you may use as PINs or passwords.
- **Check your credit report regularly.** It lists your credit accounts, recent applications and your repayment history. If you see anything you don't recognise, contact the relevant lender immediately.
- **Go through your bank, card and other statements carefully.** Look for unfamiliar transactions that could indicate identity fraud.
- **Investigate unexpected credit refusals.** Your credit rating could have been ruined by a criminal borrowing money in your name and running up debts.
- **Always tell the police and any organisations that might be affected if you suffer a theft of potentially sensitive items.** For example, let your card issuer know if you've lost a credit card.

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



© Experian Limited 2010.

The word "EXPERIAN" and the graphical device are trade marks of Experian and/or its associated companies and may be registered in the EU, USA and other countries. The graphical device is a registered Community design in the EU.

All rights reserved.