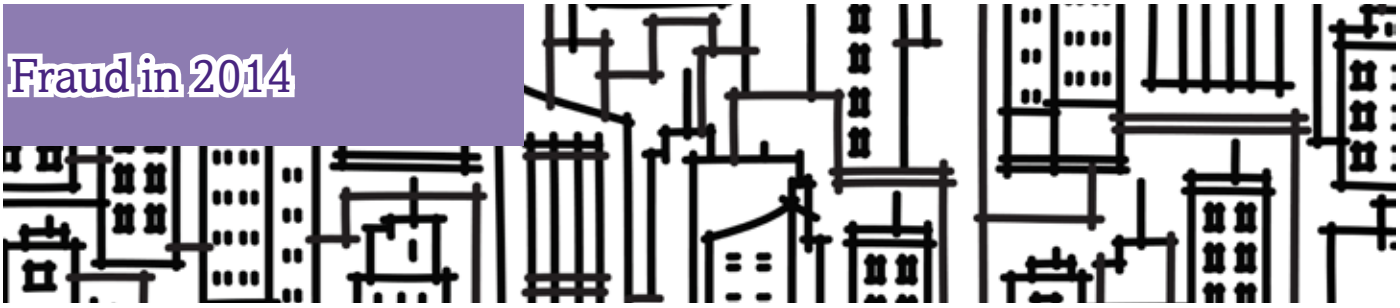
Fraudscape

UK fraud trends

cifas
Leaders in fraud prevention

Fraud in 2014



Introduction

In 2014, there were 276,993 frauds recorded by Cifas Members; an increase of 25% on 2013 levels. While fraud levels often fluctuate year by year, the overall trend is clear – recorded fraud is increasing.

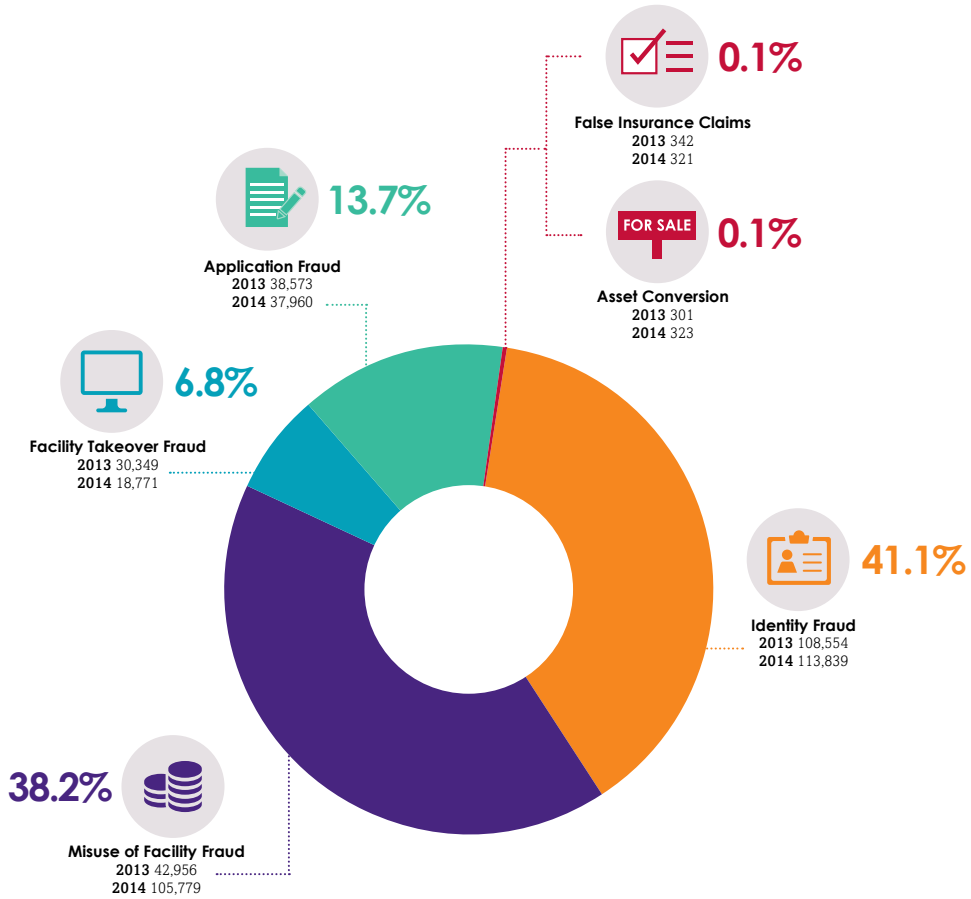
Cifas recorded frauds act as a sound barometer for the fraud landscape of the UK. Cifas Members span a range of sectors, including banking, grant giving, credit card, asset finance, retail credit, mail order and online retailer, insurance, telecommunications and public sector. Members report and share confirmed fraud cases using the Cifas National Fraud Database in order to detect and prevent further fraud. In 2014 Cifas Members prevented an estimated £1 billion of fraud through Cifas systems.

The data included in this report gives a solid indication of the nature and scale of fraud but it is by no means the full picture. It remains the case that there is no one indicator for fraud levels in the UK, meaning that the true levels of fraud will be far higher.

This report explores the key themes and trends from Cifas data in 2014. It is designed to give a simple overview of trends and recommends ideas for further specialist research. Cifas will publish a series of in-depth reports throughout 2015/16.

Contents:

245 organisations, 75% of Cifas Members, have contributed confirmed fraud data to this year's Fraudscape report.



Asset Conversion
The unlawful sale of an asset subject to a credit agreement – for example where a person has bought a car on finance and sold it on before paying it off.

Application Fraud
When an application for a product or service has been made with material falsehoods (lies) using false supporting documentation (but where the name provided has not been identified as false).

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

Facility Takeover Fraud
When a fraudster abuses personal data to hijack the running of an existing account or product.

Identity Fraud
When a fraudster abuses personal data or identity details in order to impersonate an innocent party, or creates a fictitious identity, in order to open a new account or take out a new product.

Misuse of Facility Fraud
The misuse of an account, policy or product, where the identity/owner has not been identified as false. Examples include paying in an altered cheque, knowingly making a payment that will bounce or allowing your account to be used to transfer criminal funds (acting as a 'money mule' to aid money laundering).

276,993

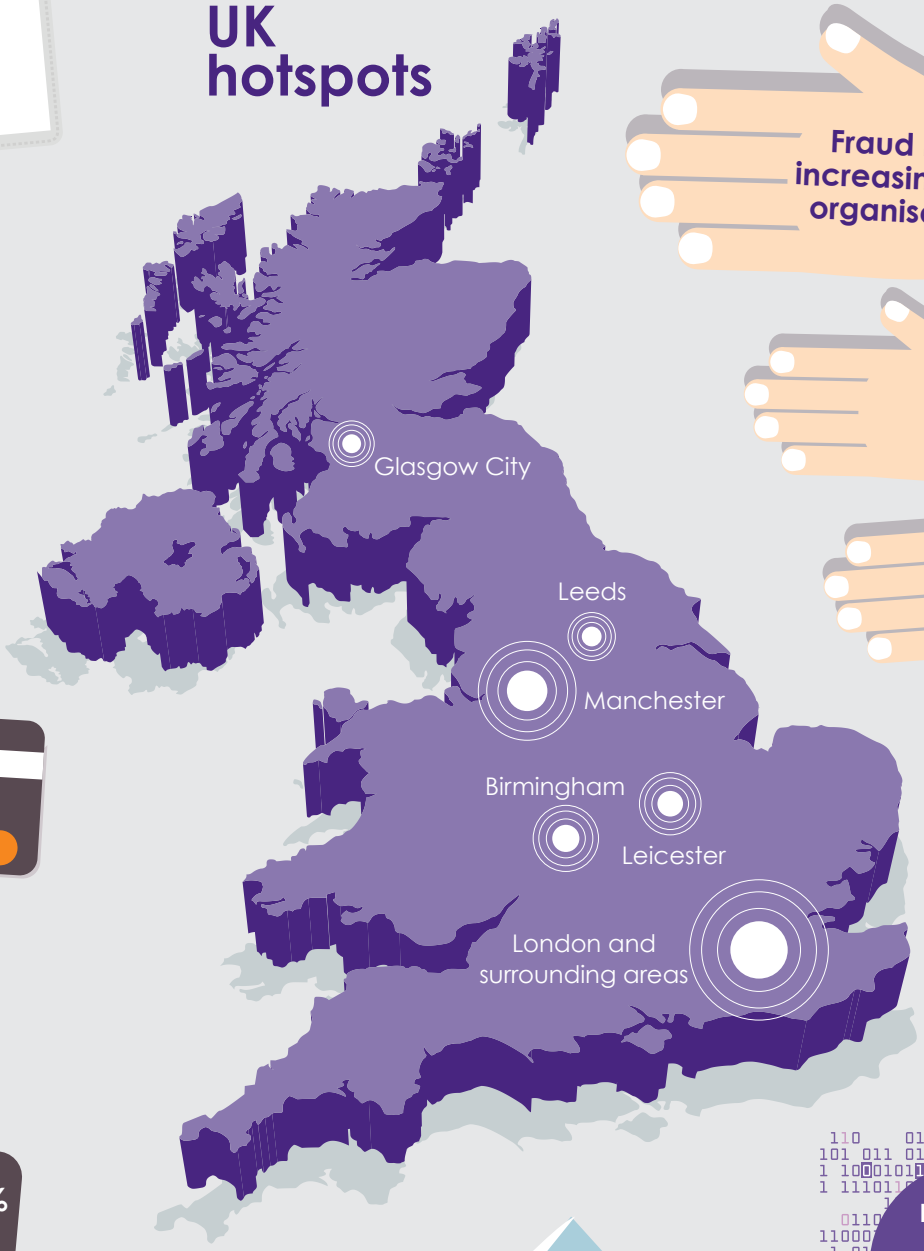
Cifas recorded frauds in 2014

Identity fraud dominates

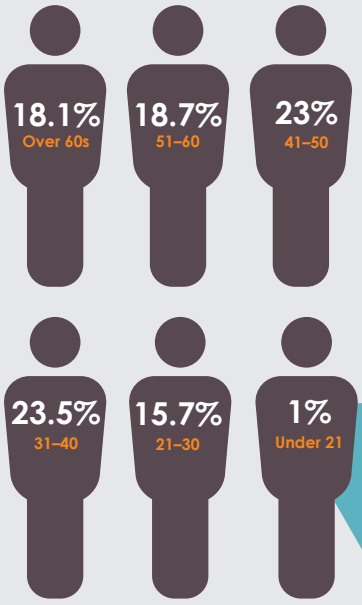
41% of fraud was identity fraud.

Almost **114,000** instances of identity fraud were recorded: representing a **5% increase**

UK hotspots



Fraud victims



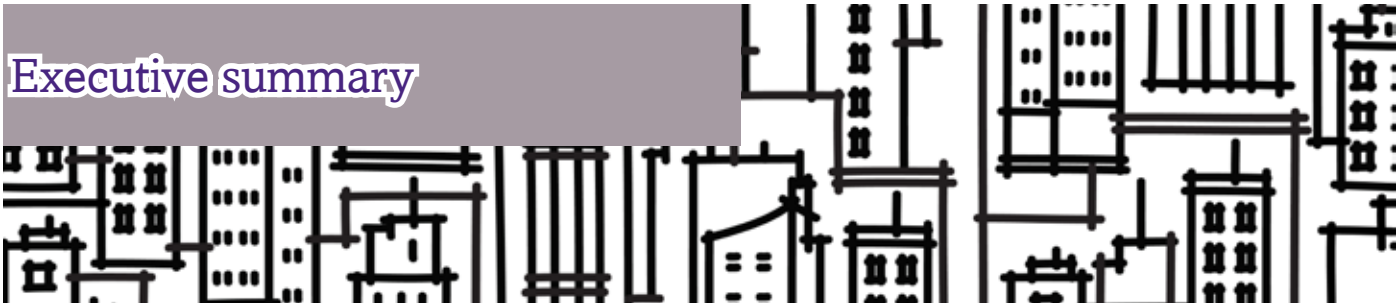
758 frauds every day

31 per hour

from Cifas members alone

The true scale of fraud is unknown

Executive summary



Analysis of the frauds recorded to the Cifas National Fraud Database in 2014 reveals a number of key trends and challenges:

1

Recorded fraud levels increased by 25% in 2014. Better reporting has contributed to the increase and provided a more accurate picture of the fraud landscape.

This year's report has seen considerable increases. 245 organisations from a range of sectors have contributed to this year's report. Cifas data acts as a good barometer, yet it is only part of the picture.

Fraud is like an iceberg. Fraud that is undetected (for example, the false insurance claim that is paid out in full by the insurer, or the tax refund that was never due) is a more insidious threat than fraud that is uncovered and reported. Without accurate reporting, a true sense of the fraud problem is impossible. Stronger reporting levels this year are a positive step.

The UK does not have a single measure for fraud. Collating reports of fraud across all 5.4 million organisations and identifying how many of the 60 million plus people in the UK have suffered fraud will be a challenging task, but it is a vital one.

2

Identity crimes remain the biggest challenge for both organisations and consumers.

As taking over existing accounts has become more difficult, criminals have focused on using other people's identities to open new ones. Identity Fraud continues to be the biggest issue. Almost 114,000 instances of Identity Fraud were recorded: representing a 5% increase from 2013 and constituting 41% of all fraud recorded through Cifas in 2014. The need to protect personal data is stronger than ever.

With almost 125,000 recorded victims of fraud, this is having a damaging impact on society. During the past five years, identity crime has fluctuated year on year, but has consistently remained the biggest fraud threat.

2014 saw increases in all victim age groups over 21. The average age of an Identity Fraud victim is 46. However the group that has seen the most consistent year-on-year rise is young adults between 21 and 30 years of age. This suggests that as digitally savvy young people enter their twenties and increase their access to financial products, they are increasingly becoming targets.

3

In the internet age, fraud and technology are intimately linked. Several variations in fraud levels can all be attributed to technology either as an enabler or prevention measure.

With data driven fraud like Identity Fraud dominating, it is unsurprising that technology played a major role in 2014. While the internet offers a fantastic opportunity for fraudsters to attempt fraud on an industrial scale, technology is also the reason behind several successes in preventing fraud.

The introduction of enhanced security procedures has made it far more difficult for fraudsters to take over existing accounts – demonstrated by the reduction in Facility Takeover Fraud, which is down by 38%. In addition, technological enhancements used by organisations have enabled them to record frauds that previously were not able to be recorded; for example, the increase in Misuse of Facility Frauds, where frauds are committed using genuine identities. This will help to identify and prevent further fraud.

These technological enhancements help to improve protection and understanding, enabling organisations to focus their efforts further. In a society where technology is constantly changing, criminals will continue to adopt new techniques. In 2014 approximately 82% of Identity Frauds were committed online rather than face-to-face. As long as fraudsters are able to obtain data, technology will both aid and prevent fraudulent activity.

4

Education and awareness are key in the fight against fraud.

Criminals change their fraud tactics on a regular basis, adapting their approach as needed. This can make education complex. A lot of prevention advice is tried and tested, but as threats evolve advice must also change.

Awareness is not just about scams. It is also important that people know what constitutes fraud. Increased reporting in 2014 reveals growing cases where individuals appear to be committing frauds themselves, or acting as money mules. The extent to which ignorance plays a part in this behaviour is not clear. Greater education is needed to ensure that ignorance can never be an excuse.

The customer can often be seen as the weakest link in the fraud prevention chain by many – organisations however can do much to ensure that their customers become the first line in effective defence.

5

Criminals continue to adapt - and fraud looks increasingly organised

Identity Fraud is an organised process. It takes time and effort to commit. Criminals must set up operations and obtain data before using identities to steal money or goods. These crimes are not committed by individuals working in isolation. Technology is crucial to ensuring the smooth running of these operations. The continuing rise in Identity Fraud is further evidence of the increasingly organised nature of fraud.

Fraudsters also look more willing to involve others in their criminal enterprises. Enlisting individuals to be money mules and launder their illicit gains has long been understood to be a problem and there were more cases of these frauds in 2014.

6

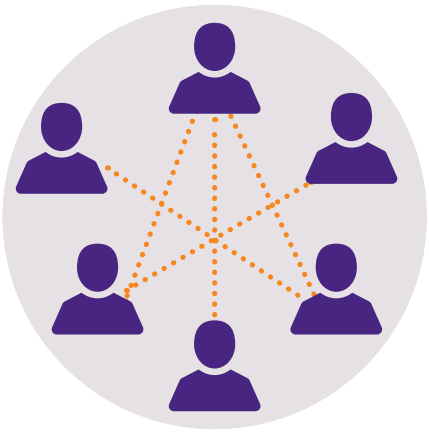
Prevention works better together

Large scale fraud operations are not limited to individual sectors. Criminals will target insurance as well as banking, the public sector as well as the charity sector. 2014 provides further evidence that cross sector prevention approaches work. An estimated £1 billion of fraud was prevented through Cifas National Fraud Database in 2014. 63% of fraud detected through Cifas systems was identified by matching data across different sectors.

These are significant successes and demonstrate the power of a joined-up approach.

Fraud prevention is most effective cross-sector

63% of fraud detected through Cifas systems was identified by matching data across different sectors.



Fraudsters don't work in silos, neither can we.

Working across sectors, Cifas members prevented over £1bn of fraud last year.

Recommendations for 2015/16

1

The UK needs a national measure of fraud losses and fraud levels

Government needs to work with industry to re-establish this measure. Until we understand the scale of the loss, society cannot truly tackle it. This year's Fraudscape shows what an impact better reporting can have on our understanding of trends and patterns.

2

Greater research is needed into the exact point at which data is compromised

Cifas Members cannot always know at what point their customers' identities have been compromised, and individuals often do not know themselves. This kind of information is vital in focusing prevention efforts and messages. Society as a whole could then focus on designing fraud out at an early stage – for example, through tighter mail security at flats where mail could be intercepted.

3

Further research into the involvement of organised criminals in fraud

This year's data provides further evidence that organised criminals are behind numerous fraud trends. More research is needed to verify and better understand the nature of this involvement of organised criminals in fraud and the extent to which money obtained through fraud is used to fund further criminal activity.

4

A co-ordinated education and awareness campaign on fraud, led jointly by Government and industry

People of all ages need to be savvier to frauds, and fraudsters, in order to protect themselves better. This year's data also suggests that some may be allowing their details and accounts to be used by criminals, without a full understanding of the seriousness of the crime.

5

A comprehensive review of the sentencing guidelines for fraud

Fraud is a serious crime. The public must have faith that when frauds are reported, criminals are punished appropriately. This will also encourage people to report fraud, adding to our overall understanding of the UK's fraud profile.

The persistent rise of identity crime

Identity crimes are cases where a fraudster has abused personal data or identity details in order to carry out the fraud: this can be through the creation of an identity, or impersonation of an innocent party (Identity Fraud) or making use of personal data to hijack the running of an account (Facility Takeover Fraud).

Number of Victims of Identity Fraud in 2014: 105,500 (6% increase on 2013)

Number of Victims of Takeover in 2014: 18,873 (38% decrease on 2013)

Identity Fraud (using either stolen or fictitious identities) was the most commonly recorded type of fraud in 2014 and accounted for over 41% of all frauds identified. Table 1 opposite shows the products targeted by those committing Identity Fraud.

Identity Frauds are not unique to the internet, but the reality is that the internet has allowed the fraudsters to attempt the fraud on a scale that would have been otherwise impossible. Examples include when fraudsters obtain personal data in large quantities, the sale or purchase of personal information, and the use of online applications or channels to use the data. Experian estimates that there are 25 million unique strains of malware, resulting in an 80 % annual increase in phishing attacks and 600 million customer information records hacked*.

The figures are large and the threat shows no signs of abating.

Product	2013	2014	% Change
All-in-one	121	146	+20.7%
Asset Finance	300	439	+46.3%
Bank Account	12,544	23,686	+88.8%
Communications	16,129	9,323	-42.2%
Plastic card	41,887	49,318	+17.7%
Insurance	43	33	-23.3%
Loan	12,862	13,956	+8.5%
Online retail	19,110	6,898	-63.9%
Mortgage	33	45	+36.4%
Other	5,525	9,995	+80.9%
Total	108,554	113,839	+4.9%

Table 1: Identity Fraud by product 2013-14

* www.experianplc.com/media/news/2014/one-in-six-adults-has-fallen-victim-to-cybercrime-according-to-research-out-today-by-experian/

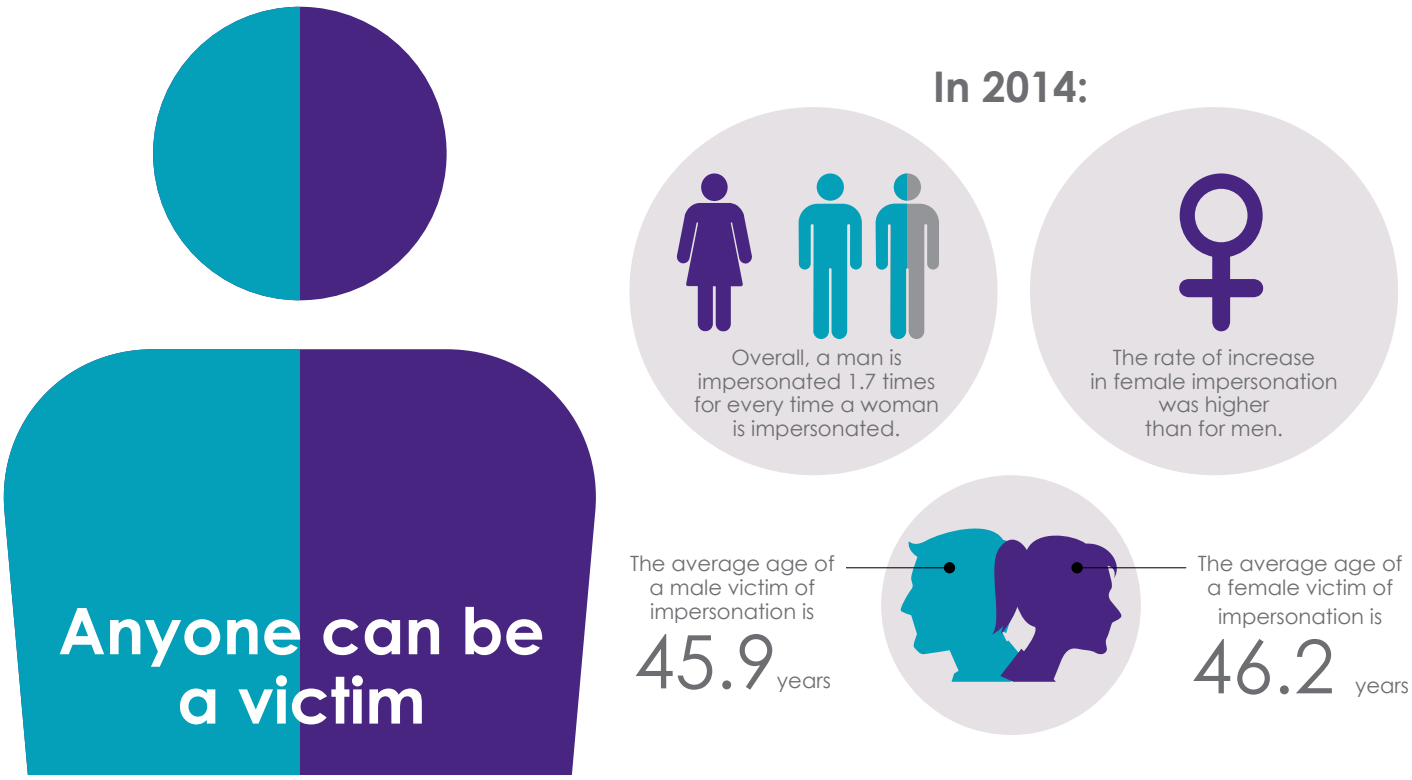
In contrast to the continuing rise in Identity Fraud, Facility Takeover Fraud decreased abruptly. Facility Takeover Fraud, also known as Account Takeover Fraud, is an identity crime which occurs where a person (the facility hijacker) unlawfully obtains access to the details of their victim (namely an existing account holder or policy holder) and fraudulently operates the account or policy for his or her (or someone else's) benefit. This decrease is explained in the next section. Table 2 opposite shows the products targeted by those committing Facility Takeover Fraud.

The greatest decrease in real terms was seen in the number of takeovers of plastic card accounts. This type of fraud decreased by 48 % in 2014 compared to 2013. Also decreasing, but not as substantially, were the number of attempted takeovers of bank accounts (down 2 %). Decreases in these areas can be seen as a considerable success for the organisations offering these accounts, which often have similar security features. Enhanced security features are helping to reduce the number of people who have had their existing accounts plundered by fraudsters.

Product	2013	2014	% Change
All-in-one	432	303	-29.9%
Asset Finance	0	2	–
Bank Account	5,476	5,386	-1.6%
Communications	4,379	3,198	-27.0%
Plastic card	16,089	8,353	-48.1%
Insurance	0	1	–
Loan	14	30	+114.3%
Online Retail	3,939	1,458	-63.0%
Mortgage	1	0	-100.0%
Other	19	40	+110.5%
Total	30,349	18,771	-38.1%

Table 2: Facility Takeover Fraud by product 2013-14

Victims



Fraudsters adapt and change their methods

Cifas has previously likened Facility Takeover Fraud to stealing someone's house keys in order to rob their house. This analogy still holds true, it is just that the locks have become more complicated and the burglar alarms more effective. The number of pieces of information that a fraudster now needs to be able to gain access to someone else's account, particularly a bank account or credit card account, are numerous. These could include any or all of:

- Customer number;
- Memorable date(s) or information;
- Passwords; and
- One time codes from a card reader.

This clearly makes that fraudster's life much more difficult. Other security issues (around what devices can access an account, or entering security numbers by clicking on randomly ordered keypads and so on) all contribute to reducing the fraudster's opportunities.

When fraudsters are being successful they are most commonly using online channels, often facilitated by a phone call. Banks and plastic card issuers have reported that some fraudsters have accessed customer accounts by phoning the customer directly and talking them through the logon process. They purport to be calling from the bank or card issuer, and claim that in order to be able to verify that they are talking to the right person, they need them to confirm their customer number, and so on. The fraudster will then be logging onto their victim's account as they are talking to them and entering the security details as they are read out. In this way, the fraudster can even obtain one time only passcodes from card readers.

Fraudsters adapt their methods – as one becomes more difficult, a number of other avenues open up. The increased difficulty in gaining access to existing accounts has occurred at the same time that Identity Frauds are increasing. This suggests that as fraudsters find it more difficult to access existing accounts they have focused on opening new ones instead. Additionally, their attention has been turning to convincing their victims to just give them the money directly. This kind of fraud is often called 'vishing'.

The rise of the vishing scam (or how fraudsters convince you to give them your money)

It is difficult to takeover someone's account; so how does a fraudster continue to commit fraud successfully? Increasingly, instead of trying to access their victim's account in order to steal money, the fraudster simply asks the victim to give it to them.

A common method of doing this (but by no means the only one) is for the fraudster to ring their victim, purporting to be from their bank or the police. The fraudster will say that their account is at risk: but not to worry, a new, safe, one has been set up for them, and all they need to do is transfer everything from their existing account to this new account. But they need to do it immediately. The victim trusts what the fraudster has told them, transfers the money and (in most cases) never sees it again.

This change of tactic from the fraudsters has created a social problem beyond the issue of money falling into criminal hands. If a fraudster gains access to a bank account and transfers the balance to another account, then the bank is required to reimburse their customer. If, however, the customer voluntarily transfers their own money to the fraudster, then the bank has done nothing wrong and is under no legal obligation to repay the customer. Once alerted to the fraud, the banks will work together to follow the money and (where possible) recover as much as possible and return it to the account holder – but there is no legal obligation for any shortfall to be reimbursed.

This has provoked some debate, with some of the opinion that banks should reimburse the customer and do more to prevent the transactions being processed in the first place. The counter argument, however, questions why a bank should shoulder the financial burden of a poor decision by their customer (which will, of course, ultimately be passed on to all customers) and highlights that banks are legally obliged to carry out the wishes of their customer.

Plastic cards continue to dominate

Plastic cards, especially credit cards, have always been attractive to identity criminals. Figure 1, below, shows that this continued in 2014. In the last quarter of 2014 there were over 14,000 cases alone. In these cases, fraudsters are applying for cards using either stolen or fictitious identities.

During times of economic gloom, these kinds of fraud had reduced because as a general rule it was harder to get credit. This made it more difficult for fraudsters to find victims who were creditworthy. As lenders' appetite to lend has increased in recent years this has widened the pool of creditworthy victims and contributed to the increase in this fraud type.

An additional factor is that improved security measures have made taking over existing, genuine credit cards more difficult. If a fraudster cannot gain access to existing accounts in order to perpetrate their frauds, then the next option is to start from scratch and open a fresh account or card in someone else's name.

Over three quarters of the Identity Fraud cases to obtain a plastic card involved the use of the victim's genuine current address – up from just under three quarters of cases in 2013, but equating to another 6,500 cases. There is a particularly high level of use of genuine addresses when it comes to Identity Fraud against plastic cards. This is notable because it means the fraudster will have to intercept the mail of their victim in some way in order to get their hands on the card and stop it from reaching their victim. While other products can be delivered electronically without necessarily needing mail interception, with plastic cards we can say that (in 2014) 37,500 frauds occurred that will have involved mail tampering – 6,500 more than the previous year. That means that the victim's identity was stolen, used to order a credit card and then the credit card was intercepted either at the victim's own address or along the way.

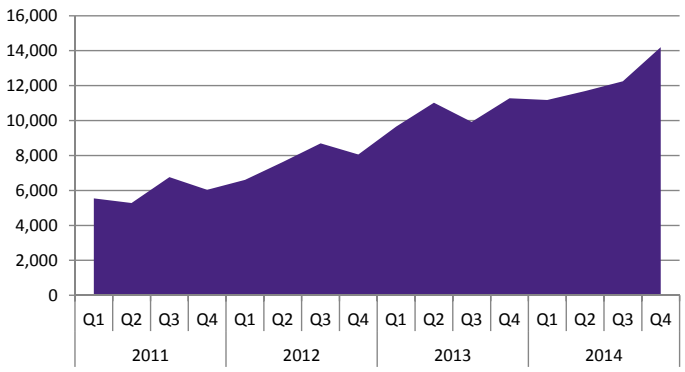


Figure 1: Identity Frauds on plastic cards 2011-14

How safe is your mail?

Research has shown that, overall, the type of building you live in has no bearing on the chances of you being impersonated – unless the identity fraudster wants credit cards. In those instances, living in flats increases your chances of being impersonated. Flats often have less secure mail facilities, giving fraudsters a greater chance of intercepting the mail before the victim sees it. If you live in flats with communal mail areas and you want to reduce your fraud risk, you may wish to consider:

- Does each flat have a separate mail box?
- Are these boxes lockable?
- Does the shape of the box prevent someone putting their hand through the slot and just pulling the mail out?

Online retail and communications see decreases in identity fraud

While the overall number of Identity Frauds increased by 5% in 2014 compared with 2013, Identity Fraud in online retail and communications decreased. Figure 2 below shows the decline in fraudulent retail accounts over the last two years following the very high levels seen in 2012. The strongest explanation for this remains that the implementation of device recognition software has prevented this type of fraud. 2014's data shows that this barrier continues to hold firm and previous concerns that the more technologically advanced fraudsters would quickly figure out a way to circumvent this software have not been realised yet. The continued success of this preventative measure, however, does not mean that the online retail sector is now immune from fraud. Far from it. The British Retail Consortium reported that the level of online fraud suffered by retailers has increased 12%, costing £223m*. This points to an adaptability on the part of the fraudsters – when one avenue is closed to them they seek to exploit the next available one. In this case, fraudsters have increased their focus on defrauding retailers at the point of payment, such as through online shopping using stolen card details.

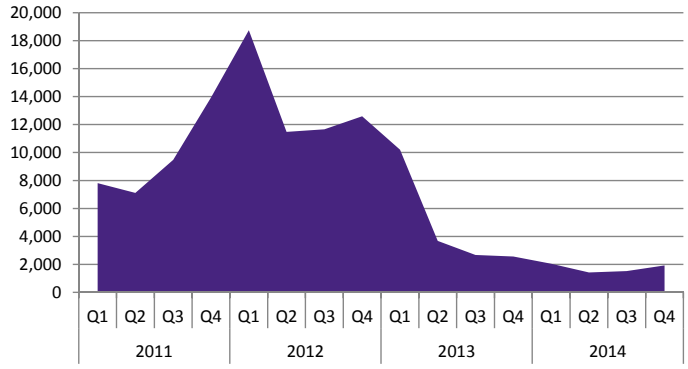


Figure 2: Identity Frauds on online retail accounts 2011-14

The other notable decrease in the number of Identity Frauds recorded in 2014 was against mobile phone providers (communications). These declined by 42% compared with 2013, a further drop from 2012 levels. Typically, Identity Fraud would be perpetrated against a mobile phone provider in order to obtain a handset to be sold on, without honouring any of the monthly payments associated with the contract. While the drop in Identity Fraud in this sector is welcome, 2014 saw a substantial increase in another form of fraud against mobile phone providers. This is explored in the next chapter.

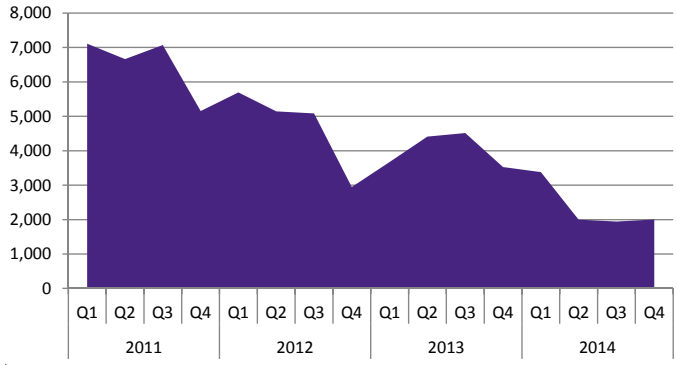


Figure 3: Identity crimes on communications products 2011-14

Bank accounts see sharpest rise

The greatest increase in Identity Frauds, in terms of both the number of cases (23,686 cases in 2014 compared with 12,544 in 2013) and as a percentage (+89%), was where a fictitious or stolen identity was used to obtain bank accounts. This finding is concerning when the potential uses of fraudulent bank accounts are considered. It is not unreasonable to assume that the intended purpose – for some of these accounts – will be to launder money (move criminally obtained funds). Criminals do not always open new accounts to launder money. Often, they will use "money mules": genuine account holders who are either complicit or scammed into moving criminal money around. It is not possible from Cifas data to understand exactly how the accounts are being used, or intended to be used, but it is clearly an area for further research in 2015/16. In 2014 Cifas published advice on how to avoid becoming a 'money mule', available at www.cifas.org.uk/research_and_reports

Other valuable uses for a bank account in someone else's name include diverting payments due to go to someone else (for example, a loan taken out in that same person's name or an insurance pay-out) or simply seeking to obtain chequebooks and overdraft facilities as a source of free money.

Almost 10 % of Identity Frauds against bank accounts involved an entirely fictitious identity (as opposed to one stolen from a genuine person), almost double the rate for other types of Identity Fraud.

* www.brc.org.uk/brc_policy_content.asp?iCat=48&iSubCat=646&sPolicy=Retail+Crime&sSubPolicy=BRC+Retail+Crime+Survey

Identity Fraud and the loans market

Fraud in the loans sector continues to evolve. In 2014 fraudsters focused on stealing and using genuine identities to apply for fraudulent loans rather than creating fictitious ones. 85% of Identity Frauds to obtain a loan were made using the victim's genuine address. This is likely to be due to a growing realisation that the loans sector does use fraud prevention techniques and is increasingly capable of detecting identities that are entirely false.

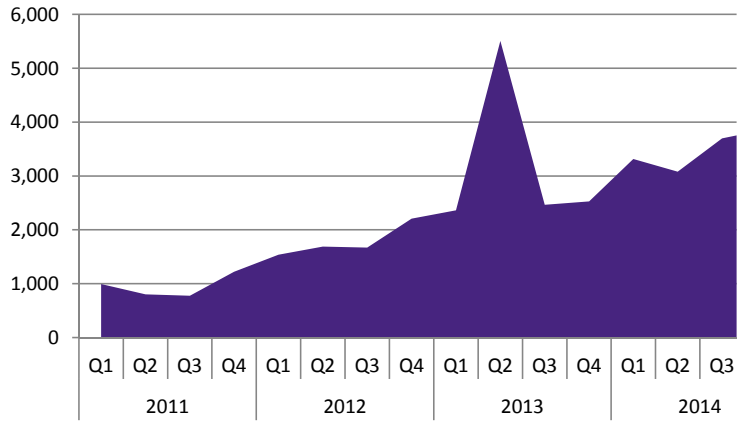


Figure 4: Identity Frauds on loans 2011-14

FCA regulation of the Consumer Credit industry

In April 2014, the Financial Conduct Authority (FCA) took over regulation of consumer credit firms – a market worth £200bn.

The objective was to ensure that anyone taking out a credit card, loan, overdraft or using a debt management company will be better protected.

Most pertinently, this regulatory regime will cover payday loan firms operating in the UK. The big changes for the payday lenders will be:

- limiting the number of loan roll-overs to two.
- restricting (to two) the number of times a firm can seek repayment using a continuous payment authority (CPA).
- a requirement to provide information to customers on how to get free debt advice.

As of 2 January 2015, the FCA has capped interest and fees at 0.8% per day, while the total cost of the loan will be capped at 100% of the initial amount. Default fees will also be capped at £15.

So, what will this mean for fraud prevention?

Payday lenders are unlikely to be able to afford to lose money to fraudsters. This may result in more stringent vetting of applicants and more opportunities to identify fraud before the money is lent.

If the vetting procedure is more stringent, and payday lenders are seen as less of a soft target, then the frauds that they are currently suffering may migrate elsewhere.

The restrictions being imposed on lenders may drive some operators out of business. This will concentrate the fraudulent activity targeting the sector onto a smaller number of organisations – probably the larger lenders who are currently taking fraud prevention more seriously by engaging in data sharing schemes such as the Cifas National Fraud Database. This, in turn, will result in more of the fraud affecting the sector being recorded, prevented and quantified.

Where next for identity crime?

The battle between organisations and identity fraudsters can be considered an arms race: fraudsters start using software to make multiple applications automatically, so organisations bring in Device ID software to stop it; finance companies bring in card readers and one time passcodes, fraudsters start phoning the individuals and socially engineering those codes out of them there and then. So, what happens next? There are various debates taking place now within the fraud prevention community that organisations and citizens will increasingly need to engage with:

1 Biometrics

Authentication based on a fixed human characteristic (face, voice, finger, retina, etc). While they may be considered unique to an individual, can this information be lifted or copied? And does the use and storage of such information make many feel uneasy?

2 Consumer satisfaction vs. security

The constant tension between allowing customers to access accounts quickly, maintaining customer satisfaction, costs and robust security is one that becomes more and more pertinent. As consumers, we all want suspicious transactions to be challenged, but without the inconvenience of having our own transactions challenged.

In an ideal world it would be possible to offer services that are secure, convenient for users and low cost. Yet it is impossible to achieve all three aims together. Services that are secure and convenient come at a price, just as services that are cheaper and secure may not be convenient for the consumer.

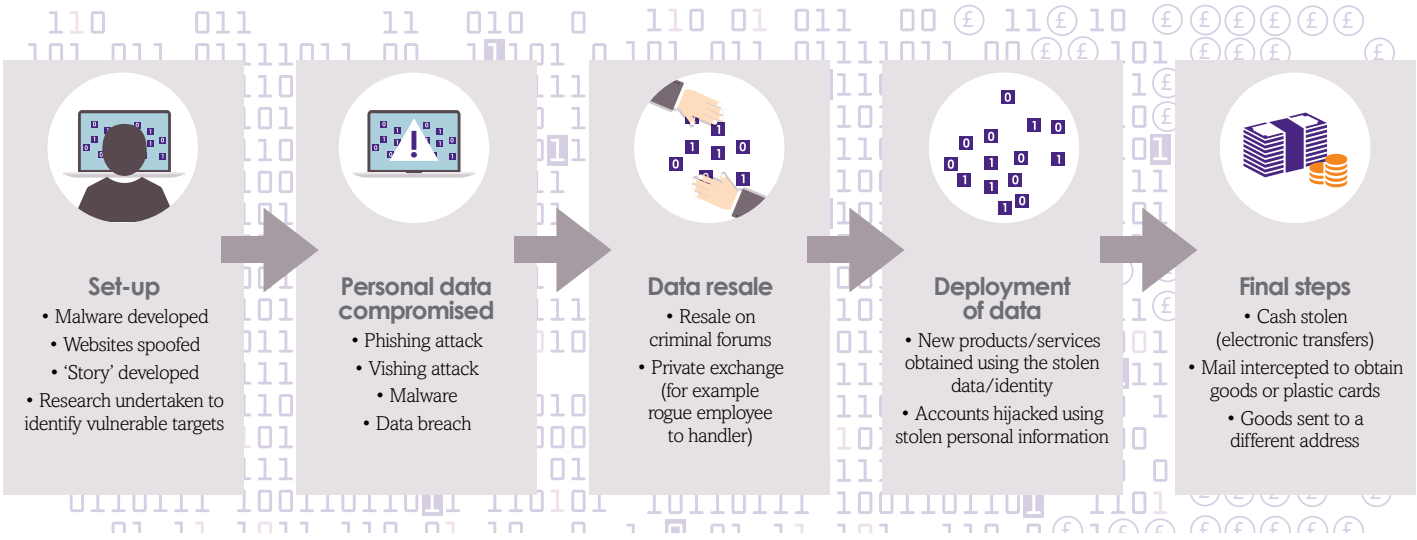
Stemming the tide of identity crime requires organisations, government and consumers to think about how they wish business to be conducted and agree on the aims that matter most to them.

3 Big data

With the proliferation of data sources (from organisations' databases to publicly available records, social media to data generated by handheld devices), the idea of 'big data' has become the new 'norm'. Intelligent use of big data allows for more sophisticated approaches to fraud prevention. Without it, organisations are forced to prioritise on the basis of cost or prevalence. As a result key patterns are missed and low level fraud continues unabated.

The potential from big data is considerable and it is already being used in the fight against fraud. Yet it is the preserve of larger companies with the ability to analyse and investigate the data. By definition, these are broad collections of data that are so large or complex that traditional data processing applications are inadequate. But where does that leave small-to-medium sized companies, a known risk group for fraud? Smaller organisations cannot be left behind and more focus must be given to finding models that work for the size and nature of their business.

The industry of organised identity crime



Why card fraudsters pick properties.

Before a card fraudster picks up a card, they pick up an unsuspecting address.

One that's shared, say, in a block of flats. Or one that simply doesn't exist.

That way they can sneak under the radar of a card issuer who's using postcode data alone to check an applicant's address.

AddressBase Premium provides over 39 million addresses including multiple occupancy addresses and flats. With this intelligence, mail 'non-receipt' fraud can be reduced.

Contact us now for our thought paper on how location data can spot fraudulent transactions.

Visit **os.uk/cifas** or call us on **02380 055991**

Ordnance Survey

Helping to cut up card fraud

SIRA

Syndicated Intelligence for Risk Avoidance

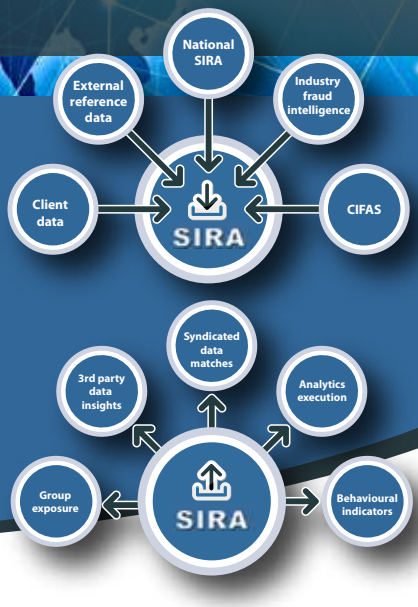
Banking & Finance Sector

SIRA Is The Leading Fraud Prevention And Detection Solution From Synectics Solutions

SIRA provides a single, integrated fraud detection and prevention system to deliver full lifecycle protection. A fully managed, hosted service solution, which eliminates multiple points of referral and streamlines working practices, SIRA places unrivalled flexibility and control in your hands at point of application and for ongoing account and transaction monitoring.

- **Full Application & Transaction Lifecycle Protection**
- **Client Control**
- **Consolidated Risk**
- **World Of Data At Your Fingertips**
- **Enhanced Access**
- **Enhanced Scoring & Risk Ranking**
- **Compliance**
- **Value Added Modules**
- **Help Is At Hand**

Providing A 'One World' Fraud View



Mitigate Your Fraud Risk Today:

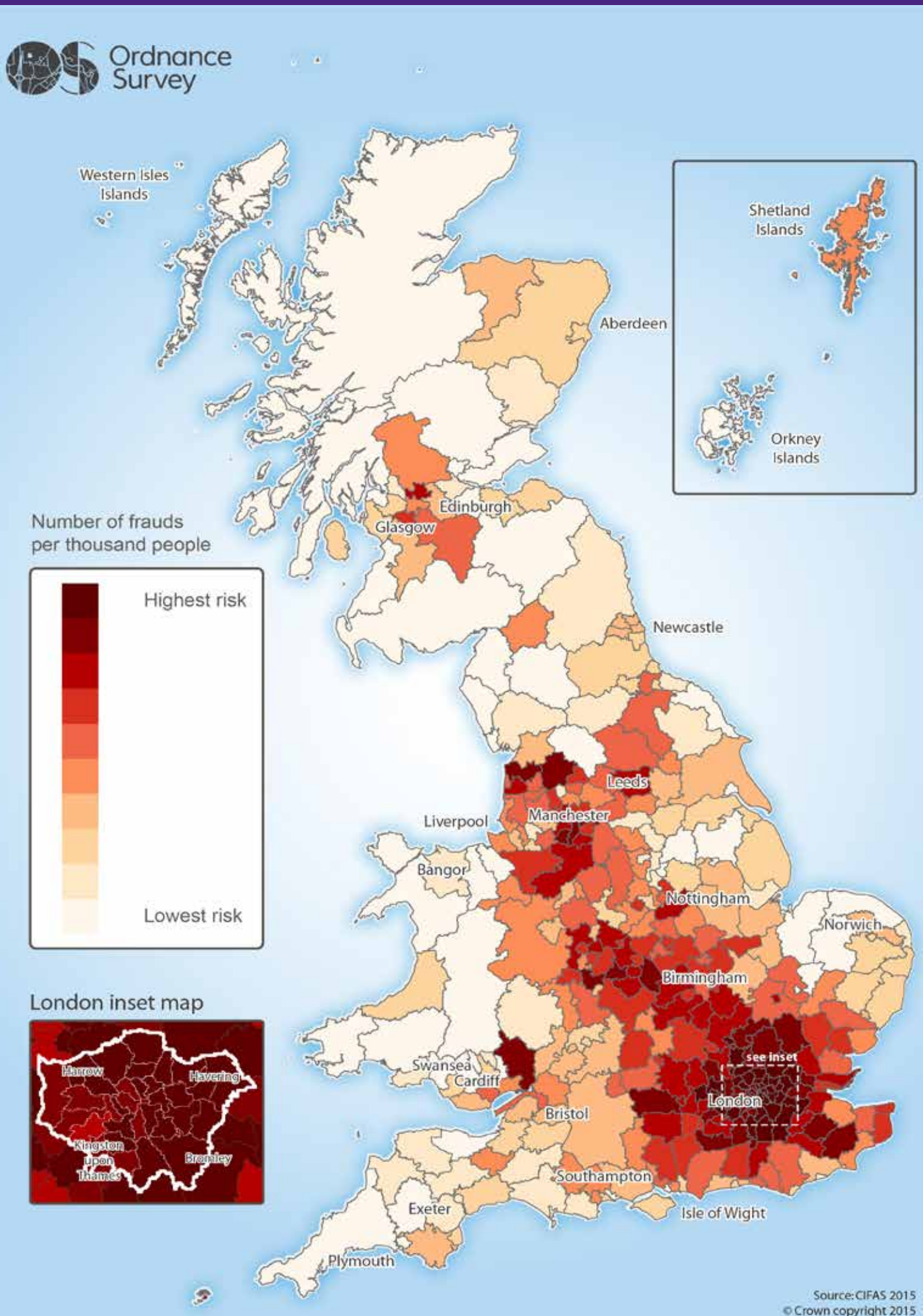
01782 664000

sirasales@synectics-solutions.com • www.synectics-solutions.com

Synectics Solutions Ltd • Synectics House • The Brampton • Newcastle-under-Lyme • Staffordshire • ST5 0QY

SYNECTICS SOLUTIONS

Victims of identity crime in 2014 per thousand people by local authority



First party frauds: 2014 trends

First party frauds occur where no evidence exists that any abuse of identity details occurred: meaning that the named account holder or applicant is genuine and is also the perpetrator of the fraud.

The largest increase in first party frauds in 2014 was a fraud type known as Misuse of Facility Fraud.

Advances in the communications and retail sectors lead to better recording and prevention

The largest percentage increases were in the communications and retail sectors, with both sectors seeing large rises (see Table 3). Part of this is due to increased reporting, aided by better technologies to record and report this kind of fraud to the National Fraud Database. This is a positive step.

The communications cases covered a specific type of fraud: where an individual took out a mobile phone contract which committed the account holder to paying the monthly fee for the life of the contract. As part of the contract they received a handset for considerably less than the retail price of the phone. No further monthly payments were made against the contract. The fraudster, therefore, has committed to a contract that they never intended to honour in order to obtain a high value phone.

These frauds tended to be carried out by young men. The phones will be blocked and cannot be used on any of the major UK networks. It may be that the person perpetrating the fraud believes that the phone can be 'unlocked' and that they would then be able to either use or sell the phone in the UK if they obtain a SIM for another network, or alternatively sell it abroad. It may also be that fraudster is aware the phone is unusable but sells it on to an unsuspecting individual for cash.

The other product that saw a noticeable increase in the number of Misuse of Facility frauds was online retail. The vast majority of these frauds involved the account holder fraudulently evading payment for retail goods. In 2014 there was a change in the demographic of those perpetrating these frauds. In 2013, the majority were men (54%), but in 2014 women perpetrated this type of fraud more frequently (55%).

The objective behind both the retail frauds and mobile frauds is the same – to obtain a tangible product without any genuine intention to pay for it. In one case it is a mobile phone and the other involves goods from online retailers.

The hand of organised crime is likely to play a part in these frauds, particularly where high quality goods such as new phones are involved. Criminals are practised at recruiting people to obtain items in exchange for cash. It is attractive to organised criminals as they are distanced from the fraud (in these cases the fraud is committed in the account holder's name) and their 'mules' are likely to be approved because the identity is genuine. The chances of success are also higher than the criminals trying to commit Identity Fraud against these sectors. Both communications and retail saw significant reductions in Identity Fraud last year due to better prevention techniques. This year's report calls for more research into the role organised fraud and Cifas will explore this further in 2015/16.

Product	2013	2014	% Change
All-in-one	45	26	-42.2%
Asset Finance	1,239	650	-47.5%
Bank Account	26,210	33,301	+27.1%
Communications	8,543	54,495	+537.9%
Plastic card	4,322	4,152	-3.9%
Insurance	42	101	+140.5%
Loan	306	529	+72.9%
Online Retail	2,020	12,173	+502.6%
Mortgage	173	265	+53.2%
Other	56	87	+55.4%
Total	42,956	105,779	+146.2%

Table 3: Misuse of Facility Frauds by product 2013-14

Abuse of bank accounts and the rise of the money mule

While 2014 saw the mobile phone contract become the most frequently recorded product subject to Misuse of Facility Fraud, the bank account also experienced a higher level of this fraud in 2014 than 2013, increasing by 27%.

This kind of fraud is also linked to organised criminals, known as mule herders, who recruit numerous individuals to create networks of bank accounts through which the proceeds of crime can be laundered.

The advent of faster payments makes it more difficult for banks and law enforcement to follow, and indeed recover, these funds. The added challenge is that, when a bank identifies that an account has been used to move criminal funds, it is not necessarily easy to know whether the account holder was complicit in the fraud.

Mule herders are known to use a number of tactics to enlist their mules. This will range from offering payment to the money mule for the use of the bank account, through to conning an unsuspecting individual into moving funds - such as using the now well-publicised employment scam where fake jobs are offered as a 'money transfer agent', coercion or another technique.

The increase in this type of fraud in 2014 suggests that more people are willing to engage with organised criminals and allow their bank accounts to be used illegally. This, coupled with the increase in Identity Fraud to obtain bank accounts, paints a worrying picture of the extent that organised criminals are abusing the UK financial system.

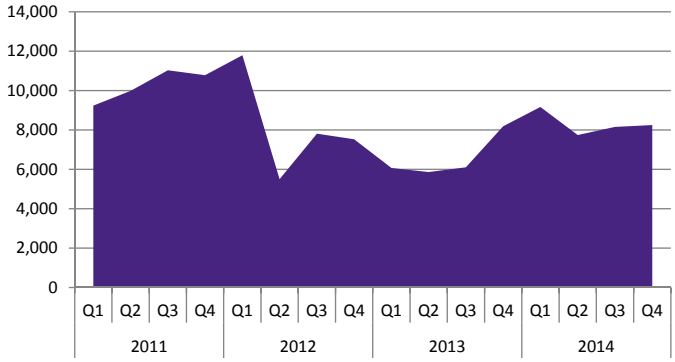


Figure 5: Misuse of Facility Fraud on bank accounts 2011-14

Figure 6 below clearly shows that those who are engaging with criminals as money mules are predominantly young men. With the consequences of such fraud including the freezing and withdrawal of bank accounts, and up to 10 years in prison, questions have to be asked about why this group is so much more willing to engage with organised criminals than other demographic groups? This is a clear area for further Cifas analysis during 2015.

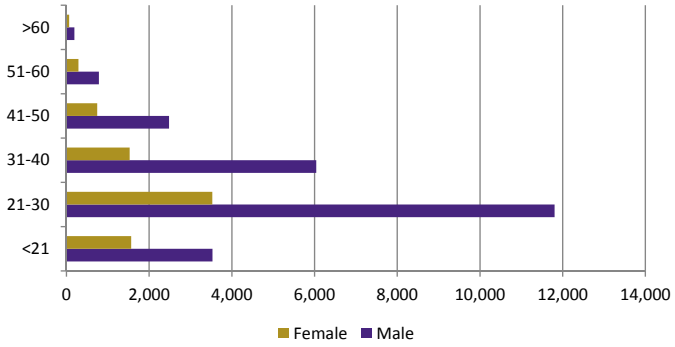


Figure 6: Age and gender of those fraudulently misusing bank accounts in 2014

Countering the money laundering threat

Cifas is taking part in the Joint Money Laundering Intelligence Taskforce (JMLIT), a new 12 month pilot project developed by the Home Office, National Crime Agency, British Banking Association and other financial institutions. Its aim is to improve intelligence sharing arrangements to aid the fight against money laundering and other criminal activity.

Cifas is sharing confirmed fraud cases from Cifas' National Fraud Database, where member organisations file confirmed fraud cases (for example, where a false identity has been used to try and open a bank account), with partner organisations in the JMLIT – in order to support this activity. Cifas already streams confirmed fraud cases to the National Fraud Intelligence Bureau at the City of London Police on a daily basis.

Cifas has a member of staff seconded to the Taskforce on a part-time basis to provide analytical support. We are supporting this initiative, launched by the Home Secretary in February 2015, in order to ensure that our Members' data is better used to prevent and detect financial crime.

Changes in circumstance: economics and education

The increase in the fraudulent misuse of mortgage accounts is smaller than bank accounts and mobile phones, but remains notable. The increase in 2014 related to people letting out properties that were subject to residential mortgages. Owing to the very different level of risk associated with a property being rented out, as opposed to being inhabited by the property owner, mortgage terms and conditions stipulate that the mortgage lender must be informed if the owner intends to let out the property. This will likely result in a change in the terms of the mortgage, including a higher interest rate being applied. These frauds of 'a failure to declare a change in circumstance' allow the owner to avoid paying this higher rate, and make a greater profit from the rental income. It is not clear whether the owners are aware of the seriousness of this kind of fraud and the potential consequences.

Attempts by mortgage customers to pay their mortgage with false instruments, such as a cheque that will bounce, halved in 2014. This kind of fraud is usually attributed to people taking fraudulent measures to pay the important bills, like the mortgage. The decrease is a positive finding as it could be a sign of a recovering financial situation.

The lower levels of Misuse of Facility Fraud against asset finance companies (such as for cars on finance) and credit card issuers are a similar positive sign.

It is not unusual to see clear links between fraud patterns and changing economic circumstances. Asset Conversion Fraud increased in 2014 for the first time since 2010. This fraud refers to when an individual buys a car, lorry or other asset on finance (where the lender retains the title) and sells it illegally without repaying the debt. It is typically seen as a fraud committed by those who have over-stretched themselves and are subsequently unable to repay the debt. During the economic downturn finance was harder to get, which would have resulted in fewer people being in a position to obtain finance that would 'push them over the edge' and the numbers of Asset Conversation Fraud decreased in line with this.

The continuing decline of Application Fraud

Over the last five years, there has been a fairly consistent, year on year, decline in the number of Application Frauds – equating to a 15% decrease over that five year period. Application Frauds occur when an application for a product or service has been made either containing material falsehoods (lies) or using false supporting documentation (where the name provided has not been identified as false).

These kinds of frauds tend to be more opportunist in nature, with less involvement from organised criminals. The most common reason for an organisation to identify an Application Fraud is that the applicant has been asked to supply an address history covering a specified period of time, but within that time period there is an address where the applicant has accrued adverse credit information, like defaults or County Court Judgements. Knowing that this information is likely to harm their chances of being approved, applicants do not disclose their full address history; unaware that most lenders or product providers will have access to fraud prevention and risk scoring systems that will reveal the fraud. It is these frauds, specifically, that have consistently decreased over the last five years.

The fall is also partly due to a number of customers continuing to fail an organisation's initial credit scoring checks, meaning that the application is simply rejected outright and does not progress to the stage where the fraud contained within it is recorded.

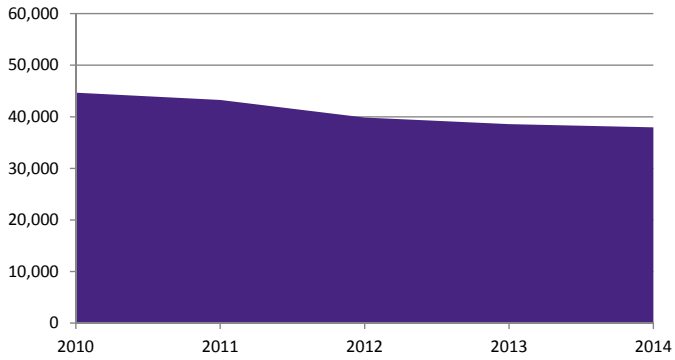


Figure 7: Application Frauds 2010-14

The challenge for insurers

In line with overall trends, 2014 saw a reduction in the number of Application Frauds perpetrated against insurance companies. In particular, motor insurers have seen a reduction in 'ghost broker' cases. These are people applying for insurance on behalf of their 'client', taking the money for the policy from the client but using false payment details to pay the insurer for the policy.

The top three insurance application lies were:

- Applicants claiming to live somewhere they don't, in order to lower the premium. This accounted for over 26% of cases.
- Fronting an insurance policy: typically a parent doing this so that a young, and therefore expensive, driver can be put down as an additional driver (when it is actually the younger driver's car). This accounted for 18% of cases.
- Falsely claiming to have a no-claims discount – another 18% of cases. This has also lead to an increase in the number of faked no-claims notification letters that insurers have been presented with.

There will be many who feel that these practices, particularly for young people, are acceptable and in some cases necessary. A recent survey of 2,000 parents with children between 16 and 25, by Gocompare.com*, revealed that 49% thought young driver premiums were too high and 38% thought that high premiums were pushing young drivers to drive uninsured. These findings clearly suggest that there is work to do to improve public perceptions and ensure that insurance fraud ceases to be seen as a comparatively acceptable form of fraud.

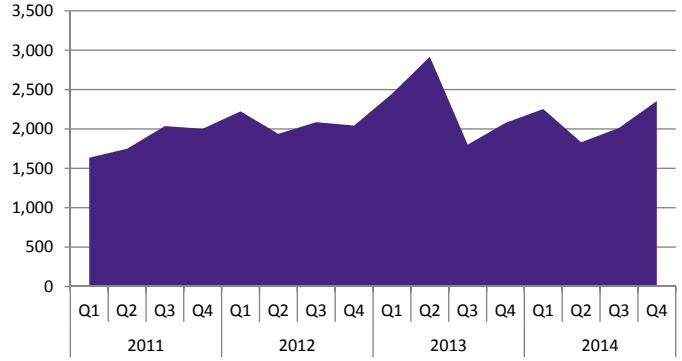


Figure 8: Insurance Application Frauds 2011-14

* www.easier.com/128808-1-in-4-parents-of-young-drivers-are-fronting-their-car-insurance-policies.html

False Insurance Claims

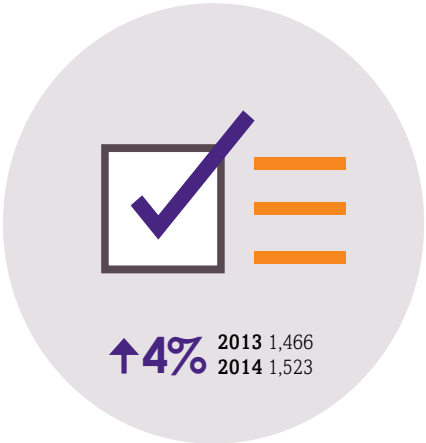
False Insurance Claims occur when an insurance claim, or supporting documentation, contains material falsehoods (lies). The Association of British Insurers puts the number of false claims detected in 2013 at 118,500 with an associated value of £1.3bn*. The 321 False Insurance Claims recorded to the National Fraud Database in 2014, therefore, are only a snapshot of the size of the problem faced by insurers.

Of those recorded, the most common type was a false claim against a motor insurance involving staged events (such as deliberately damaging or writing off a vehicle). More worrying, however, is the number of these that are 'crash for cash' events; where criminals enlist people to take part in staged accidents or induce innocent road users to crash into other vehicles. Such staged accidents continue to put UK road users in danger. Staged events represented 38% of reported False Insurance Claims against motor insurance companies. The other common False Insurance Claims were for events that never took place (24% of claims) and fraudulent claims that an insured vehicle was stolen (17%).

Where the claim is against home insurance policies, the most common fraud involved the manipulation of dates; to make the items being claimed for appear to be covered by a policy when they were not actually covered at that time. These accounted for 46 % of the False Insurance Claims against home insurance providers. The next most common fraud, accounting for 20% of claims, involved fraudulently inflating the value of a claim.

Customer education

Do customers know that the following are fraud and the consequences are serious?



Fronting an insurance policy

Misuse of bank accounts: this will include where customers have allowed their bank account to be used by others to receive and transfer funds

Letting out a property that you have a residential mortgage on without letting the mortgage lender know

* www.abi.org.uk/News/News-releases/2014/05/Insurance-cheats-feel-the-heat-value-of-fraudulent-claims-uncovered-by-insurers-hits-record-level

Conclusions

Cifas recorded fraud increases in 2014.

This report covers recorded fraud levels only. It is likely to be the tip of the iceberg. This year's data confirms that Identity Fraud remains the biggest threat and highlights the increasingly organised nature of fraud. Cifas will carry out further work in 2015 to analyse these trends and raise awareness of new or growing threats.

There are a number of trends emerging that suggest fraud is becoming more organised and sector specific trends are playing an increasingly smaller part in understanding the overall fraud landscape. Over the coming year, Cifas will focus on identifying the themes that are emerging across sectors, common trends in fraudulent behaviours and understanding public views on fraud policy. More focus must also be given to vulnerable groups – both businesses and individuals that are more susceptible due to their business model or personal circumstance.

The strongest message is the continued need for education, awareness and reporting. In 2015, Cifas will seek to build partnerships that will join up fraud prevention and help to simplify advice for the public, whatever product or company they may be dealing with.

But there have been significant successes over the past year. Device recognition software continues to prevent frauds and a number of sectors have seen reductions in certain types of fraud. There are increasing signs of industry, government and consumer bodies working together and establishing new methods to counter threats. Cifas Members alone are estimated to have prevented £1 billion in fraud in 2014.

Estimates show that is enough to pay for:

£1 billion =

The salaries of 26,000 nurses

The average deposit on a house for 14,000 people

The average annual electricity bill for almost 800,000 households

About us

Cifas is the UK's Fraud Prevention Service. We are a not-for-profit Membership organisation with Members spread across banking, credit cards, insurance, investment management, telecommunications, the public sector and a range of other sectors.

245 organisations share confirmed fraud through Cifas' National Fraud Database to prevent further fraud and protect consumers by ensuring the same fraudster cannot continue to operate across sectors. Cifas data is streamed daily to the City of London Police's National Fraud Intelligence Bureau so it can be investigated by law enforcement agencies.

We offer Protective Registration for individuals whose identities are at risk of being used fraudulently, for instance after a burglary. Individuals can contact the Cifas team and register their details for a 12 month period. During this time, a warning flag is placed against their name and other personal details. The flag tells organisations that additional investigation is required to make sure any applications, such as applications for bank accounts, loans or credit cards, are genuine. This means that if a fraudster tries to make a fake application using the stolen identity it will be flagged up and can be prevented. Genuine applications from the individual are processed as normal once their authenticity has been confirmed.

It costs an individual £20 to register for a year. Providing protection over 12 months increases security — victims may have replaced the lost items detailing their identity, or set up new accounts, but criminals may attempt to use the data months later. Further information on Protective Registration can be found online at www.cifas.org.uk/pr.

In 2014, we launched a new scheme called Protecting the Vulnerable. This service is offered free of charge to local authorities. Many local authorities have an Appointee and/or Court Deputy team that is responsible for the financial affairs of individuals who have been assessed and do not have the mental capacity to manage their own financial affairs. They are placed under a court order of protection under the Mental Capacity Act 2005 and are not able to request financial or other services (such as credit, loans, passports and bank accounts). The Cifas Protecting the Vulnerable programme was created to offer greater protection to these groups. The service works in the same way as Protective Registration except it is applied for by the Appointee or Court Deputy, and it is provided to Local Authorities free of charge. For more details contact ptv@cifas.org.uk

We also operate an Internal Fraud Database to combat the risks from insider fraud. An annual report detailing the findings and trends from this database is published every Spring.

Build more secure online customer relationships

Our device intelligence helps you to recognise the device and the individual to support the best service for your customers and protect them from fraudsters.

Deliver a seamless online experience with 41st Parameter, a part of Experian

Learn more:
Experian Identity and Fraud
www.experian.co.uk/41st
0844 481 5893

Experian™
Identity and Fraud

Stop fraud in its tracks.

Prevent, detect and investigate fraud with LexisNexis® Risk Solutions.

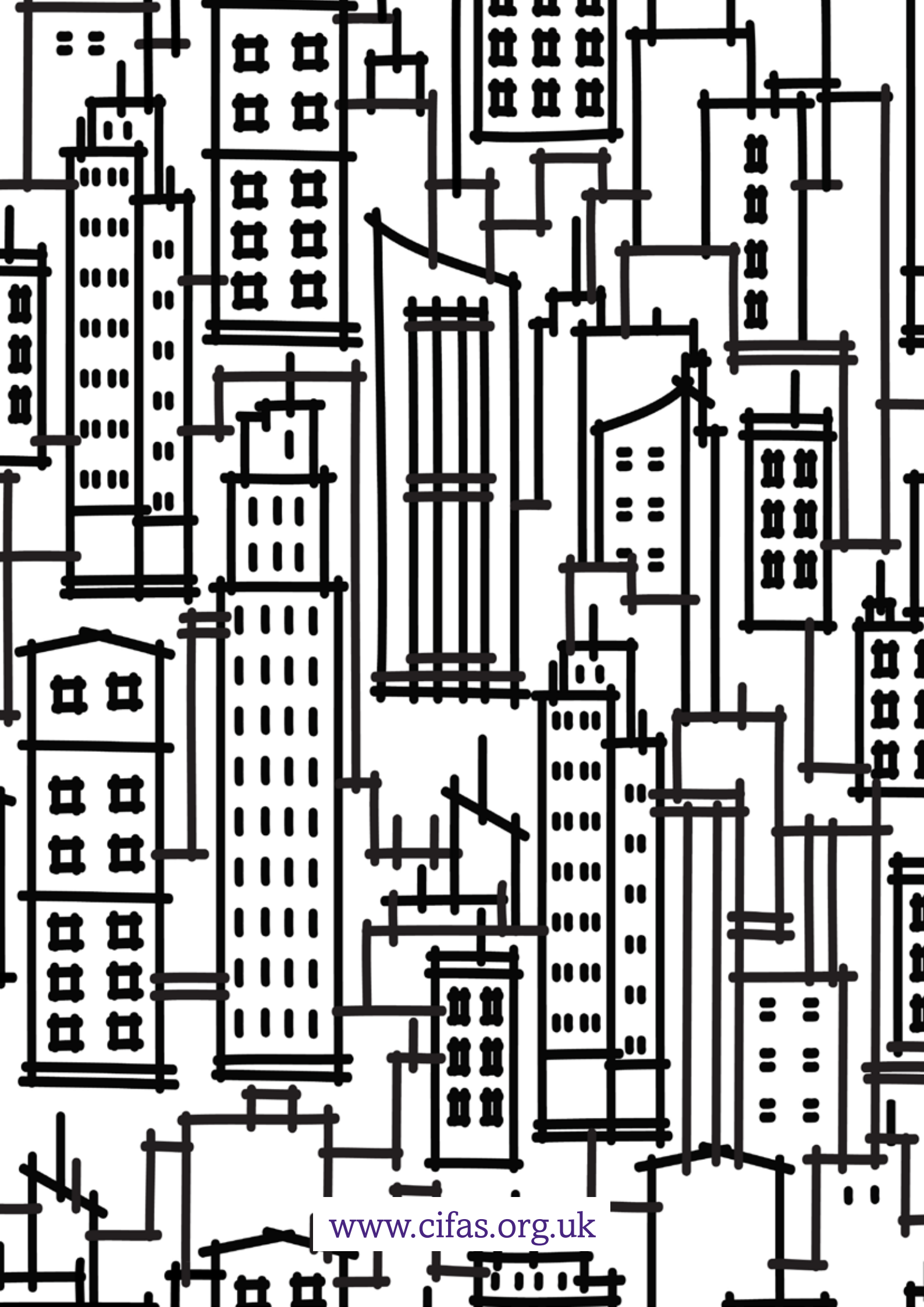
Offering a global defence in the battle against fraud and financial crime, LexisNexis® Risk Solutions allow you to manage the risk of fraud in a business friendly manner. Our software and data services enable you to confidently verify and authenticate customer identity, screen individuals against international watchlists, conduct systematic fraud investigations and comply with global regulations.

For more information, call 029 2067 8555 or email ukenquiry@lexisnexis.com

lexisnexis.com/risk/tracesmart

LexisNexis®

Risk Solutions



www.cifas.org.uk