cifas

Leaders in fraud prevention

FRAUDSCAPE —2016

Contents

1. Introduction

– Sandra Peaston, Assistant Director, Insight, Cifas

Fraud is an age old problem.

Yet fraudsters have been quick to adopt new methods to exploit the latest technologies and attempt fraud on an industrial scale. In 2015, confirmed frauds recorded by Cifas member organisations were included for the first time in the Office for National Statistics Crime in England and Wales statistical bulletin as Police Recorded Crime. By including these offences in addition to those reported to Action Fraud, the crime figures increased substantially.

Prevention efforts are also increasing. Working with many different partners, and across public, private and the charity sectors, we see increasing amounts of time and resource invested in combatting fraud, and notable successes as a result. Using Cifas, our members alone prevented £1.1 billion in fraud losses in 2015 and worked hard to protect vulnerable customers and individuals. The significant savings in 2015 highlight the invaluable work of fraud prevention professionals within these organisations and the huge benefits derived from sharing cross sector fraud data.

Despite these successes, 2015's data underlines the need for all of us to do more and to do it quickly. Recorded fraud continues to increase as criminals turn to online channels and scams to commit fraud and launder money. To combat it, we need to work ever more closely across sectors. This is already picking up pace, with initiatives such as the Home Office's Joint Fraud Taskforce and the Joint Money Laundering Intelligence Taskforce. Both projects bring the private and public sectors, and law enforcement, together to share information and fight fraud and financial crime. We are proud to be part of them and to share our expertise to help prevent further financial crime.

The data in this report shows that identity fraud and mule activity (where individuals are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts) are two of the biggest concerns, emphasising the increasing importance of more closely aligning fraud prevention and anti-money laundering functions, not just within banks and other private institutions in the regulated sector, but also within law enforcement. Keeping these functions separate risks overlooking valuable intelligence and giving organised criminals an advantage that they could otherwise be denied.

Anyone can be a victim of fraud and we know that from a victim's perspective, fraud is not just about the money. The feeling of violation and a loss of trust from scams and identity fraud can be just as serious as the financial impact.

We want to work with partners to do more to educate people about how to protect themselves and empower them to feel confident enough to report scams when they happen and continue their daily lives without fear of falling victim again.

Awareness is not just important for current or potential victims. Young people, in particular, deserve better education about the dangers of becoming involved in committing fraud and the serious consequences of agreeing to act as a mule or take part in a scam. Financial and fraud education in schools and further education establishments is an obvious area for improvement.

The vast majority of fraud detailed in this report is internet-enabled – 62 per cent of all frauds, rising to 86 per cent for identity fraud. It is easy to get lost in the complex technology involved in some cyber frauds but we cannot forget that fraud is ultimately about people. Cyber enabled fraud is crime facilitated by the internet. There are people behind the keyboard – both victims and perpetrators. Focusing on deterrence and designing out opportunities to commit fraud are the building blocks of a strong response.

We hope you enjoy this year's edition of Fraudscape.

2. MAIN FINDINGS

The frauds recorded in the report are from the Cifas National Fraud Database. These frauds have been recorded by 261 organisations. The figures include all frauds recorded to the database, including those that were prevented before a financial loss, for example instances of identity fraud where the application was rejected as it was identified as fraudulent before the product or account was granted. We include all cases where a fraudulent application is submitted, regardless of whether the application is successful, as the fraud has already occurred.

FRAUDS COVERED IN THIS REPORT

In 2015, Cifas members identified and recorded more instances of fraud than ever before. More than 320,000 cases were recorded, an increase of almost 16% when compared with figures for 2014.

Recording and sharing the details of these frauds on the Cifas National Fraud Database enabled Cifas member organisations to prevent £1.1 billion in fraud losses in 2015 demonstrating the role that effective data sharing plays when it comes to fraud and financial crime prevention.

£1.1 billion

fraud losses prevented by Cifas members in 2015.

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), often 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 an account to be used to transfer criminal funds (acting as a 'money mule' to aid money laundering).

Fraud by Type

FOR SALE

Asset Conversion

2014 | 323
2015 | 258

-20.1%

Application Fraud

2014 | 37,960
2015 | 41,186

+8.5%

False Insurance Claims

2014 | 321
2015 | 366

+14%

Total

2014 | 276,993
2015 | 320,900

+15.9%

Facility Takeover Fraud

2014 | 18,771
2015 | 15,497

-17.4%

Identity Fraud

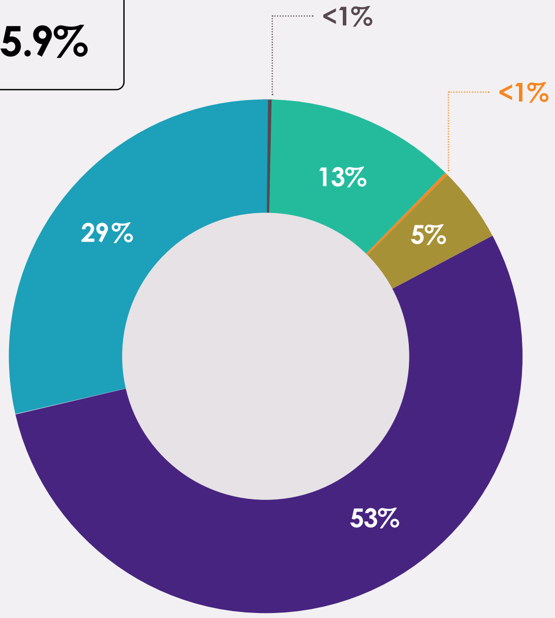
2014 | 113,839
2015 | 169,592

+49%

Misuse of Facility Fraud

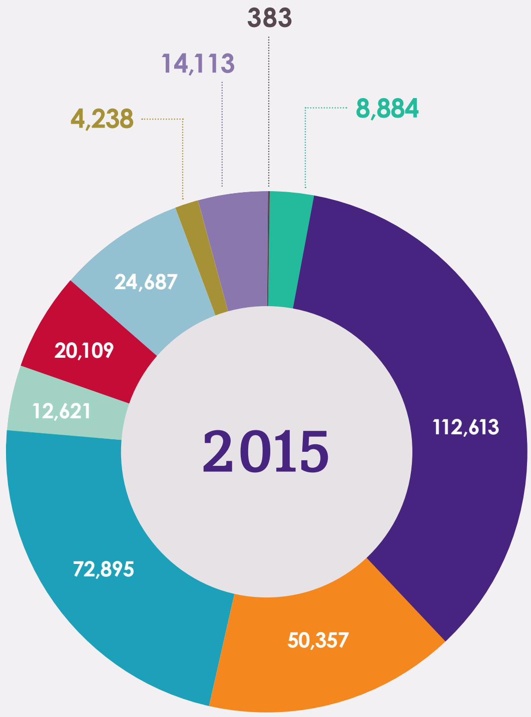
2014 | 105,779
2015 | 94,001

-11.1%



Fraud by Product

	2014	2015	%
All-in-one	488	383	-21.5%
Asset Finance	8,932	8,884	-0.5%
Bank Account	70,535	112,613	59.7%
Communications	68,361	50,357	-26.3%
Plastic card	64,519	72,895	13.0%
Insurance	8,908	12,621	41.7%
Loan	20,080	20,109	0.1%
Online retail	20,723	24,687	19.1%
Mortgage	4,223	4,238	0.4%
Other	10,224	14,113	38.0%
	276,993	320,900	15.9%



Key Statistics

169,592

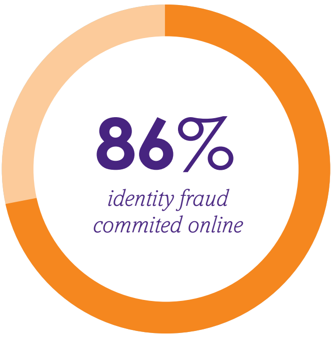
identity fraud

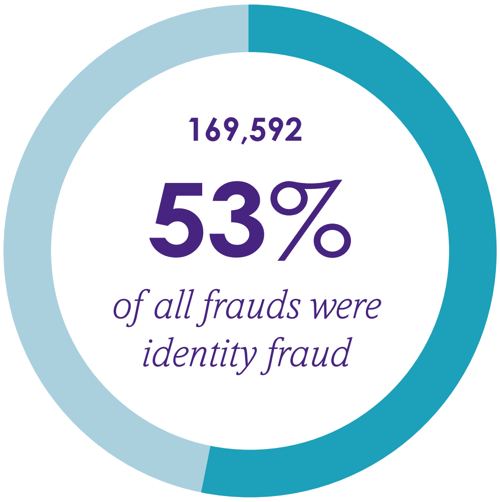
Increase in identity fraud
49%

Banks accounts were the most targeted product with a

60%

rise in attempts.





Mule activity continued in 2015, with

26,430

cases that are indicative of this activity.

49%

of first party frauds were carried out by people who are 30 years of age or younger, demonstrating the need for better education about fraud and its consequences.

Incidences of identity fraud in 2015

Product	2014	2015	% Change
All-in-one	146	141	-3.4%
Asset Finance	439	560	27.6%
Bank Account	23,686	64,174	170.9%
Communications	9,323	12,341	32.4%
Plastic card	49,318	59,423	20.5%
Insurance	33	50	51.5%
Loan	13,956	13,392	-4.0%
Online retail	6,898	5,734	-16.9%
Mortgage	45	41	-8.9%
Other	9,995	13,736	37.4%
Total	**113,839**	**169,592**	**49.0%**

3. VICTIM FINDINGS

Victims and demographics

Anyone can be a victim of fraud. In the past our victim data has shown that men are the most likely identity fraud victims and that they are usually in their mid-forties, due to their perceived likelihood of obtaining credit. While this profile is still common, the gender gap between male and female is narrowing. We are seeing more female fraud victims and more younger victims, than ever before. This suggests that fraudsters are increasingly targeting a wider range of demographics.

VICTIMS OF IMPERSONATION

2015

60.5% *Male*

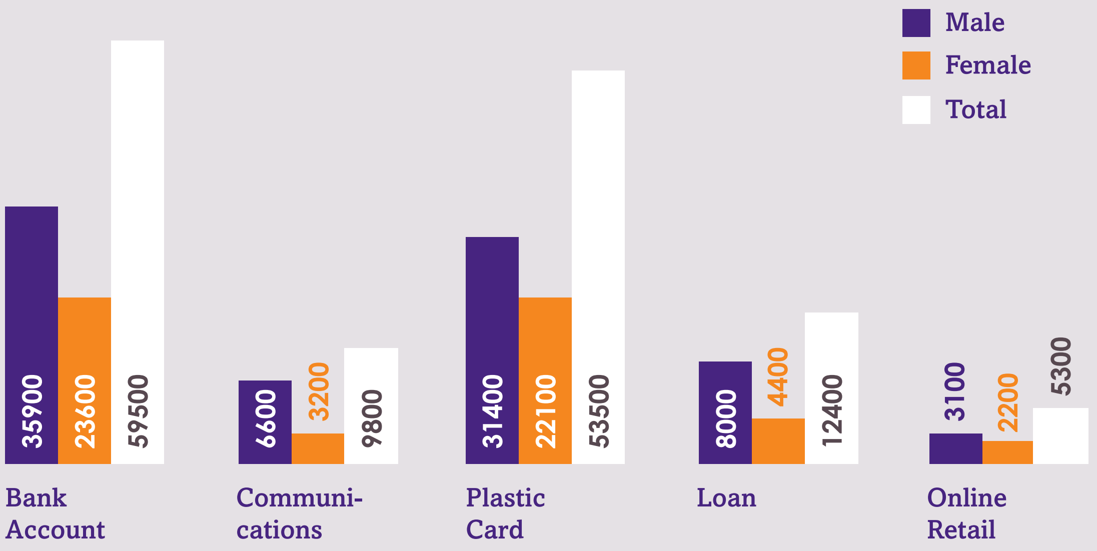
↗ 39.5% *Female*

2014

63.0% *Male*

37.0% *Female*

Gender of victims of impersonation, by product



VICTIMS OF ACCOUNT/ POLICY TAKEOVER

2015

58.9% *Male*

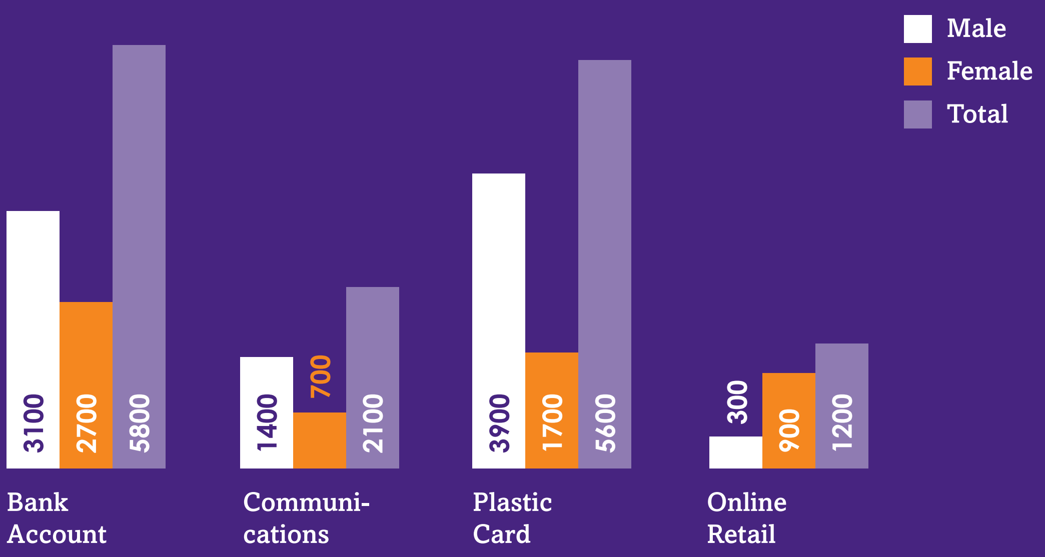
41.1% *Female*

2014

62.2% *Male*

37.8% *Female*

Gender of victims of account/ policy takeover, by product



Victims of impersonation

UNDER 21

2014 | 916
2015 | 1,343

46.6%
increase

21-30

2014 | 14,850
2015 | 22,616

52.3%
increase

31-40

2014 | 22,248
2015 | 36,502

64.1%
increase

41-50

2014 | 21,717
2015 | 33,702

55.2%
increase

51-60

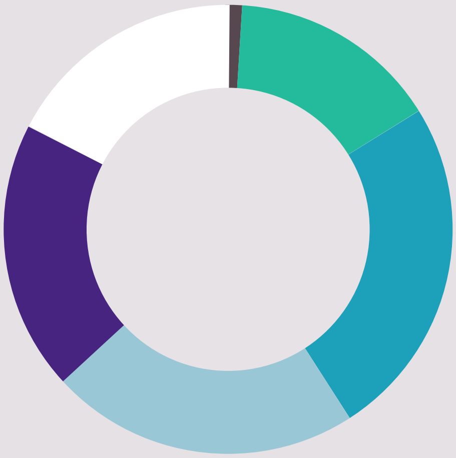
2014 | 17,698
2015 | 28,366

60.3%
increase

OVER 60

2014 | 17,063
2015 | 25,934

52.0%
increase



Victims of takeover

UNDER 21

2014 | 225
2015 | 204

-9.3%
change

21-30

2014 | 2,173
2015 | 2,459

+13.2%
change

31-40

2014 | 3,087
2015 | 3,117

+1.0%
change

41-50

2014 | 4,301
2015 | 3,364

-21.8%
change

51-60

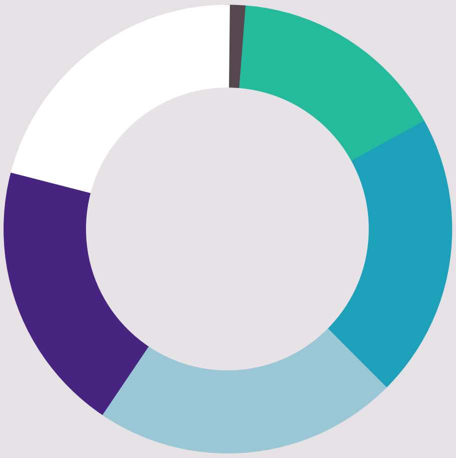
2014 | 4,076
2015 | 3,016

-26.0%
change

OVER 60

2014 | 4,685
2015 | 3,278

-30.0%
change



Victim Support: help during difficult times

Neil Masters / CJS Business Development Manager / Victim Support

Fraud poses a threat to every area of our lives, and with every case there is a victim. The common view that some fraud is a victimless crime is far from the truth.

Every day, the independent charity Victim Support sees the devastation and misery that is the inevitable outcome of fraud, whether it be a victim who has been conned into spending their life savings on a worthless financial product; paid an extortionate sum for shoddy workmanship or a lonely person who trusted someone they met online and have been scammed in search of happiness.

> *Some victims just want their money back, but others have had their trust destroyed.*

While the financial loss will be important, the impact on someone's daily life can be far reaching and long lasting.

We are now seeing a new type of victim – one who in the past would have felt safe behind the locked doors of their home. The internet, and having an online presence, can provide access to those with fraudulent intent into the very heart of the home.

A significant number of stories told by the media imply that the internet is the only fraud threat. But every day people also fall victim to often less sophisticated doorstep frauds such as bogus tradesmen or door to door salesmen. These individuals use high pressure techniques, often targeting those who are more susceptible to fraud such as older people to scam them out of sometimes large sums of money for poor work or worthless goods.

Age can be a factor in susceptibility to fraud, whether it's online or on a person's door step. Victim Support's analysis of its own service data in 2015 showed that over-65s made up 35% of the 39,272 fraud referrals to us in 2014-15 despite making up just 18% of the population. Further to this, 22% of victims were aged 75 or over despite making up just 8% of the population.

Coming to terms with fraud, whether you are young or old, as with any other crime can be a very long process for a victim. Our charity works with other agencies to help take away the stigma that is often attached to fraud and give the victim the confidence to report it, knowing that they are not alone and will be taken seriously.

It is helping to rebuild lives where our charity excels and where our 1,100 staff and 3,000 volunteers have over 40 years of experience. We will support a victim for as long as it takes, whenever the crime took place, and whether or not it has been reported.

Whilst we can't compensate the victim for their financial loss, we can work with them to piece their lives back together. Through working closely with Cifas, the City of London Police who run Action Fraud, and Get Safe Online, Victim Support believes that it is well placed to provide victims with the support they need and the respect that they deserve.

To contact Victim Support you can visit the charity's website at victimsupport.org.uk or call the Supportline team for free and confidential information and support on 0808 1689 111.

4. Fraud in an age of digital and data — exploring the trends

Data – the fraudster's gold

Advances in technology are making life easier, quicker and more convenient for UK citizens, but they are also creating more ways in which fraud can be committed. Fraudsters have always tried to find new methods of obtaining money, goods and services, using whatever means is available to assist them. The speed of some new technologies, coupled with the proliferation of data available, have combined to play a part in the significant rise of identity fraud.

Organisations have implemented increasingly sophisticated technology to authenticate their customers and potential new customers. The difficulty with stopping modern identity fraud is that fraudsters are sometimes able to obtain enough data about victims to make fraudulent applications almost identical to an application from the genuine party.

There are a number of reasons for this, not least the sheer volume of data that is available to fraudsters on the dark web – whether obtained through data leaks, hacks, social media or other methods. Numerous organisations experienced data breaches in 2015 and no organisation is completely immune to these risks. These breaches can then provide the information fraudsters can use to carry out an array of scams and crimes using the obtained data.

It is no longer unusual for an individual to place a significant amount of their, and their acquaintances, data online. Seemingly innocuous pieces of information such as posting details of a birthday or address can be used by identity fraudsters to build up a picture of an individual's life, whether it is on social media or other publicly available websites.

Once obtained, personal information is used by fraudsters in a number of ways: pretending to be the victim and applying for accounts and services in their name (such as a bank account or mobile phone contract), taking over ownership of facilities that individual already owns or contacting the individual and using the data they have to trick them into falling for a scam or revealing even more information over the phone or email.

Fraudsters' need for data to carry out scams is also affecting the way insider frauds are changing. Whereas insider fraudsters still use their position within a company to steal money or access customer accounts, the less common but equally if not more damaging insider frauds now occur where it is not money that is stolen, but customer and staff data.

Online identity fraud

Identity fraud, where fraudsters use data to impersonate an individual or create a fictitious identity to get products or services, is one of the most significant fraud types facing the UK. These frauds are, in almost four fifths of cases (78%), perpetrated by the fraudster using their victim's genuine address as the current address on the application, adding to the difficulty in distinguishing between the genuine individual and the fraudster.

Data from the past five years shows that the number of identity frauds involving an entirely fictitious identity has dropped substantially.

2011

10.6%

of all identity frauds involved fictitious identities.

2015

3.4%

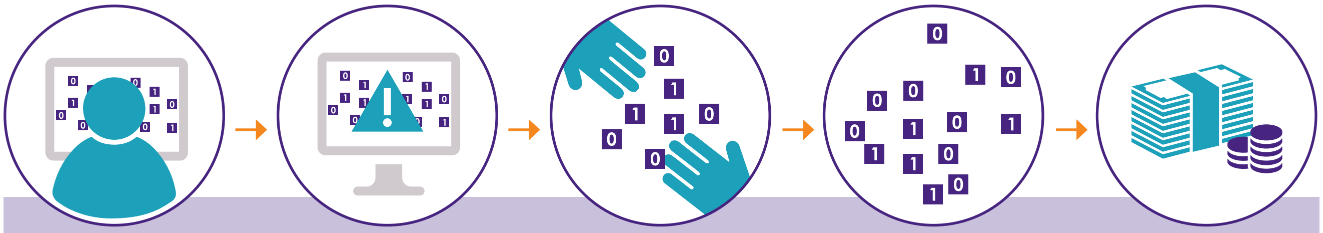
of all identity frauds involved fictitious identities.

Fraudsters are more likely to use stolen genuine identities as fictitious identities are unlikely to pass verification checks. This widespread use of genuine identity details makes identity fraud increasingly difficult to spot from genuine applications.

Increase in Online ID attempts

from 82% in 2014 to 86% in 2015

Organised identity fraud



SET-UP

- *Malware developed*
- *Websites spoofed*
- *'Story' developed*
- *Research undertaken to identify vulnerable targets*

PERSONAL DATA COMPROMISED

- *Phishing attack*
- *Vishing attack*
- *Malware*
- *Data breach*

DATA RESALE

- *Resale on criminal forums*
- *Private exchange (for example rogue employee to handler)*

DEPLOYMENT OF DATA

- *New products/services obtained using the stolen data/identity*
- *Accounts hijacked using stolen personal information*

FINAL STEPS

- *Cash stolen (electronic transfers)*
- *Mail intercepted to obtain goods or plastic cards*
- *Goods sent to a different address*

Bank accounts were the products targeted most frequently by fraudsters. They are likely to be targeting bank accounts for a number of reasons. The fraudster may merely want access to the bank account in order to make money through transferring out the available funds and overdraft or making purchases through cheques or contactless payments. They may also be using the account as a means to open other facilities and to access other services and products. Accounts could be used to move and obscure the source of illicitly obtained funds, through a network of accounts.

800 member cases per day to the police

All of these recorded cases have been fed directly to the City of London Police National Fraud Intelligence Bureau for investigation.

The level of impersonation to obtain bank accounts is significant, and the number of times someone was induced into fraudulently misusing their bank account on behalf of criminals has also increased. The co-ordinated efforts of the Joint Money Laundering Intelligence Taskforce, led by the National Crime Agency, and the Joint Fraud Taskforce, led by the Home Office, are working to tackle these trends.

Security vs convenience – a question for us all

Inevitably the increase in identity fraud cases through online channels will raise questions about how accounts are opened and how applicants are identified. Organisational procedures, including the sharing of confirmed fraud information, are sufficiently robust to detect high volumes of fraud before accounts or policies are opened. As security systems grow ever more complex some fraudsters clearly feel it is easier to trick someone into handing over their own money than to attempt to hack into accounts directly. This is clear from the examples of scams where individuals are conned into giving their own details away or clicking on malware that allows a takeover.

However systems are not fool-proof and it is clear that fraudsters are attempting to take advantage of society's desire for ever faster, more convenient ways of applying for and accessing products.

The availability of mobile and online channels to apply for products and services is welcomed by many who wish to enjoy the convenience of fast applications for the products and services that they want, whenever and wherever they want but that same convenience and speed of access is also being exploited by fraudsters to make multiple applications while hiding their true identity.

Identification is at the heart of this issue and it is not an issue for banking alone. Government, banks and other organisations are exploring new ways of verifying identities and the identification of the device on which an application is made or an account accessed. Many organisations are looking to deploy biometrics, behavioural analytics, or social media analysis to validate identities and it is crucial that such technology is linked to existing data sets and a layered approach to security is adopted. Improving the way identities are verified through better use of new types of data and information will be the basis of a solution. Cifas could play a role in sharing information on 'bad' devices and on biometrics, however, a significant challenge remains in agreeing standards and deploying cost effective solutions across industries. In addition to biometrics there is also a growing interest in utilising the power of big data analytics, and Cifas is exploring how search data can be utilised to predict fraud.

What is clear is that until new ways of identifying applicants have been developed, the security of personal data will remain the central issue for fraud prevention.

5. Tackling fraud in the UK

At Cifas, we are working with a wide range of organisations to collaborate in the fight against fraud. Here are seven key areas we are focused on for the year ahead.

01

Better measurement

The inclusion of fraud data from Cifas' members in the Office for National Statistics Police Recorded Crime Statistics is a positive and welcome step. However it is still the case that the UK does not have a single, agreed and coordinated measure for fraud and the associated victims and losses. There is a lot of good progress recently – the "Understanding the Threat" strand of the Joint Fraud Taskforce, for instance, will build a deep picture of some of the key threats.

A single measure for fraud, agreed by and covering industry, the public and third sectors, is needed. The more we develop the understanding of the threat in the UK, the better equipped we will be to beat it. To do this as effectively as possible, it will be crucial to bring a wide range of partners together.

Better information

As part of the coordinated industry and Government led education and awareness campaign on fraud and cyber fraud we propose that the Government work with industry and law enforcement to create a universal advice pack that can be sent to victims of scams and fraud. We believe that a multi-format pack, including digital, could help Government, charities, fraud prevention agencies and businesses to provide consistent messaging and practical advice.

02

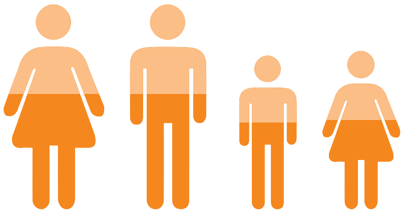
03

Widening prevention efforts

As our statistics show this year, we can all be victims of fraud. This is not an issue that simply affects older or vulnerable people. Fraudsters are increasingly sophisticated and organised, and they can target anyone.

We look forward to working with fraud prevention partners on larger scale awareness campaigns to reach greater numbers of people. We are also working on bespoke campaigns for newer audiences, such as younger people. The internet plays a big part in young people's lives, they share lots of information about themselves through social media, making them prime targets for fraudsters when they are old enough to apply for financial products and services.

Fraudsters can target anyone



04

Protecting the Vulnerable

Fraudsters actively target all of society. However, there are people that may be more susceptible to becoming victims of fraud, especially when they rely on others for their care or lack capacity to make sound decisions about their finances.

Launched in 2014, our Protecting the Vulnerable service is a form of Protective Registration aimed at individuals that are subject to a court order of protection under the Mental Capacity Act 2005. As such they are deemed to lack capacity in managing their financial affairs and local authorities take on this responsibility under a Deputyship or Appointeeship order.

Cifas is pleased to offer this service free of charge to all local authorities and healthcare trusts in England and Wales as part of our Corporate Social Responsibility policy and in line with our not-for-profit status.

The service works by placing a protective marker on the person's details in our National Fraud Database. Should any of our members receive an application for a product or service using those details then they will be aware of the client's vulnerable status and will take appropriate action.

This helps to protect the vulnerable people from financial abuse perpetrated by family, friends, carers or fraudsters.

We welcome applications to join this free service from any local authorities or healthcare trusts that would like to register their clients with us for protection.

We are currently working with 11 local authorities and 1 NHS healthcare trust to provide protection to

2,393
VULNERABLE ADULTS

To find out more then please get in touch. ptv@cifas.org.uk

05

Perpetrators – working with the next generation

We know that more young people than ever before are also being recorded as committing first party fraud. Focus groups with young people suggest that these age groups are not aware of what constitutes fraud and the very real consequences of becoming involved in fraudulent activity.

Stronger fraud education, as part of schools' safeguarding policies, and taught in Computing, PSHE and Financial Education classes at both primary and secondary levels would help to protect future generations – both from becoming victims of fraud and from becoming involved in fraudulent activity.

Universities and Colleges should also be encouraged to work with fraud prevention agencies and other partners to provide students with prevention and online identity protection advice, as well as information on what constitutes fraud and the consequences of acting as a money mule.

06

Policing and Intelligence – less silo working, improved data sharing and better training

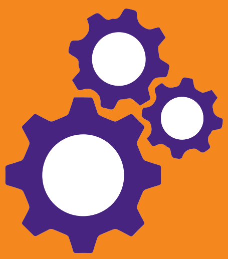
We will continue to work closely with law enforcement partners to improve intelligence and increase data sharing. This will help to ensure that law enforcement has the right information to hand, from across sectors, to build an accurate and timely picture of criminality. This data can also be used to better tackle organised fraud rings, particularly those using the proceeds to fund other crime, and also prolific fraud rings that are targeting vulnerable people.

We have also called on the Government to ensure that all new officers, cadets and Special Constables, receive detailed education as part of their initial police training on fraud and scam prevention advice to enable them to provide advice in their communities, to spot local trends, and to help pick up unreported fraud and cyber crime.

07

Smart adoption of new technologies

The fraud prevention fight is an arms race. As one method to prevent fraud emerges, fraudsters work to find a way around it. The need to collaborate to develop new and innovative ways to keep pace with fraudsters, and even to get a step ahead, has never been greater. We are therefore stepping up our efforts to collaborate with technology providers to ensure that our data can be deployed to prevent fraud and to develop and deploy new techniques and data matching rules. We are open to working with members, and new and existing partners, to innovate to reduce even more fraud. Technological developments such as machine learning, audio and behavioural analytics, device recognition, and big data analytics, provide ever more exciting opportunities to prevent fraud and Cifas is increasingly looking to facilitate cross sector solutions to today's and tomorrow's fraud problem. It is crucial that smaller businesses do not miss out on the benefits of new preventative technologies due to cost or lack of knowledge and so we are also developing our ideas on how we can reach out to help protect this crucial segment of the UK economy.



24,000

Identity fraud victims under the age of 30 recorded in 2015

In Focus

Education: teaching the next generation to be savvy about fraud

In 2015, there was a 52% increase in the number of identity fraud victims under 30 years old compared with 2014.

The figures have more than doubled since 2010, where there were just over 11,000 recorded victims, increasing to almost 24,000 in 2015.

We are also seeing proportionally more young people committing fraud. 49% of first party frauds recorded were committed by people who were 30 and under.

The recent trend of more young people both falling victim to and committing fraud is concerning.

42%
21-30
year olds

Cifas believes that the UK education system can play a role in reversing these trends. We welcome the fact that under the last Government financial education was expanded to England, meaning it is now compulsory in all regions of the UK; however we feel more could be done and hope to work with partners to improve the information offered to young people. Currently, there is no mention of teaching online identity protection or fraud awareness in the financial education curriculum guidelines.

We also believe that both primary and secondary school students should be receiving fraud prevention and online identity protection advice. A recent Opinium survey found that over half of children have used social media sites by the age of 10. We believe that primary school students through financial education, Personal, Social and Health Education (PSHE) and computing classes should be taught how they can keep their online identity safe. We believe many victims of identity fraud are becoming victims through social engineering and some of this is happening through social media sites.

Evidence has shown that criminals have exploited young people in a number of ways, primarily coercing them to act as 'money mules', getting them to sell their bank accounts, credit cards and taking out mobile phone contracts where the phones are then sold abroad and the contract is never honoured. Criminals are adept at presenting these as quick opportunities to make money, with few consequences. In reality, becoming involved in this kind of activity can have lasting consequences, including finding it difficult to access financial products. Our initial work in this area suggests that young people do not always recognise that this is fraudulent activity or that what they are getting involved in is illegal and has serious consequences. Better education will help the next generation to make more informed decisions and think twice before becoming involved in fraud.

Parents can be part of the education solution too. In the United States, the Federal Trade Commission has issued advice to parents on how they can protect their children from online identity theft. Replicating this in the UK would be valuable.

52%

Increase in the number of identity fraud victims under 30 years old compared with 2014

6. NATIONAL FRAUD DATABASE FRAUDS BY TYPE

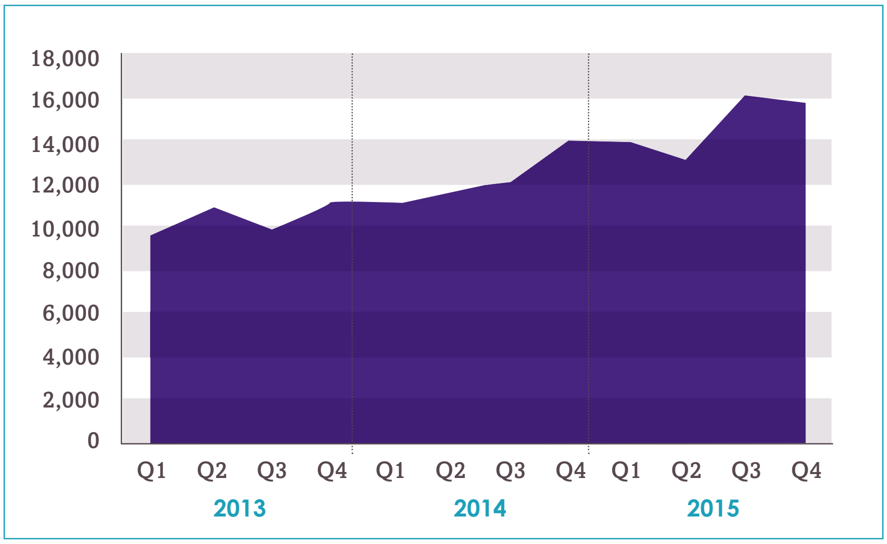
Identity-related crimes

Identity-related crimes occur when a fraudster has abused identity details in order to commit fraud. This can be through impersonation of an innocent party or the creation of a fictitious (synthetic) identity (identity fraud) or making use of personal data to hijack the running of an account (facility takeover fraud).

Incidences of identity fraud in 2015

Product	2015	2014	% Change
All-in-one	141	146	-3.4%
Asset Finance	560	439	27.6%
Bank Account	64,174	23,686	170.9%
Communications	12,341	9,323	32.4%
Plastic card	59,423	49,318	20.5%
Insurance	50	33	51.5%
Loan	13,392	13,956	-4.0%
Online retail	5,734	6,898	-16.9%
Mortgage	41	45	-8.9%
Other	13,736	9,995	37.4%
Total	**169,592**	**113,839**	**49.0%**

Incidences of identity frauds to obtain plastic cards



The number of identity frauds involving plastic cards continued to increase. Most of these cases used the victim's genuine address and were perpetrated online. As with the identity frauds to obtain bank accounts, it is clear that cyber is playing a big role in this kind of fraud.

Identity fraud and mobile phones

Last year the number of instances of identity fraud to obtain a mobile phone rose by almost a third, the first rise since 2011. The 12,300 cases recorded in 2015 are still far below the peak level of almost 26,000 cases seen in 2011, but it is a trend that Cifas will be monitoring.

Compared to other products, identity fraud to obtain a mobile phone is less reliant on the internet. Fewer than 20% of cases involve applications being made purely online. Fraudsters focussed their attention more on other delivery methods, including through retailers and a combination of different channels.

Identity fraud and loans

The number of identity frauds committed in 2015 to obtain a loan fell by 4% when compared with the number recorded in 2014. This is particularly interesting as our data revealed there had been year-on-year increases since 2011. The decrease last year is somewhat counter-intuitive given the substantial rise in identity fraud concerning other products, but it can be attributed to the effect of the changes in the regulation of the consumer credit market.

In the 2015 edition of Fraudscape, we highlighted the potential effect of new Financial Conduct Authority (FCA) regulation around short-term, high cost credit. The change is likely to have played a role in the reduction in the number of cases recorded. It has been reported that there has been a 75% decrease in the number of payday loan approvals from the peak levels seen in 2013 and a number of providers have left the market altogether. With fewer approvals, it will also be more difficult for a fraudster to successfully submit an application in someone else's name. A higher number of fraudulent applications will fail credit scoring criteria and be declined before an investigation can take place and the identity fraud proven and the case recorded.

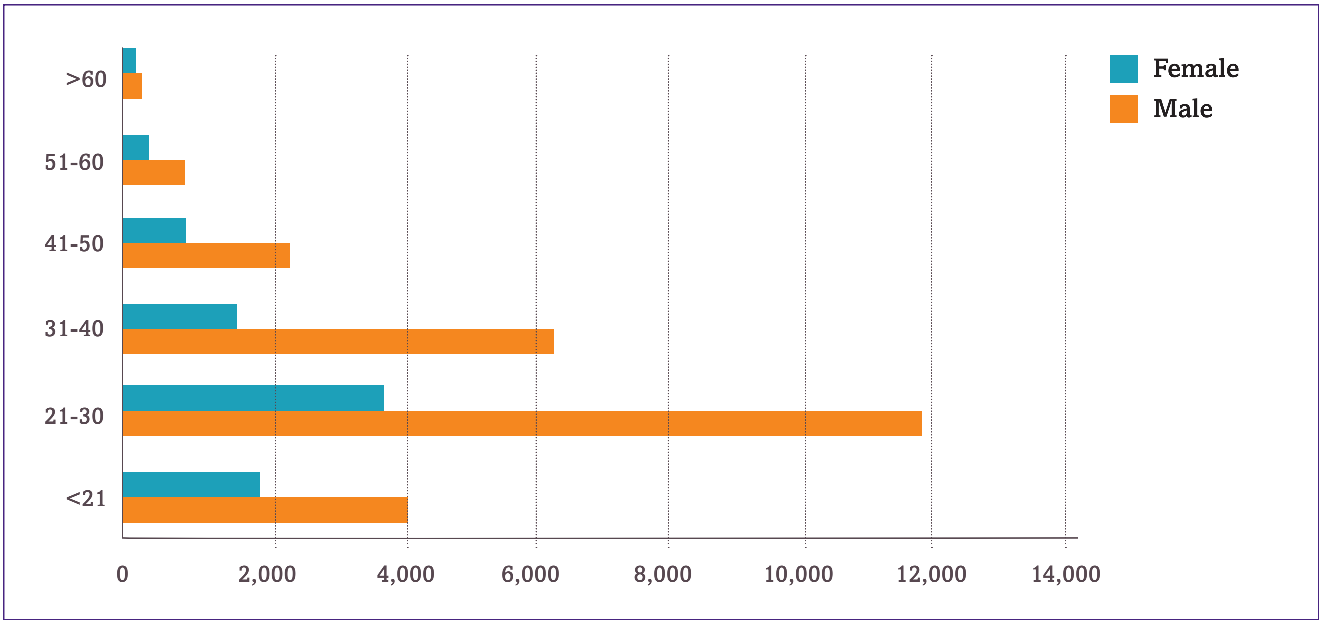
Facility takeover fraud

Facility takeover fraud is when a fraudster has enough details (like passwords) to bypass security on their victim's existing accounts and take them over.

2015 saw a further 17% decrease in facility takeover fraud – following a decrease of 38% in 2014 from 2013.

Taking over an account is not easy – security measures continue to evolve and improve. The effects of this can be seen in the falling number of takeovers. Vulnerabilities remain, particularly where no token is required to access an account, and there will always be a danger from skilful social engineering of the customer or malware attacks that intercept log-on details.

Age and gender of those fraudulently misusing banks accounts



Misuse of facility

The second most common type of fraud is the fraudulent misuse of a facility by the account holder. With this type of first party fraud the bank account was the most frequent target of fraudulent activity. There was an increase of 6% in 2015 compared with 2014 and the vast majority of these frauds were indicative of people acting as money mules. Money mules are those who, wittingly or unwittingly, allow money to be moved through their account on behalf of criminals – laundering their illicit finds.

As can be seen in the figure above, almost three quarters of those misusing bank accounts are men, and nearly two thirds of individuals involved are aged 30 or under.

Banks and fraud prevention partners are committed to ensuring that people are aware that by becoming a money mule, they are committing a crime and risk a criminal conviction. Clearly, though, the incentives offered by criminals can still be sufficient to offset the risks and there is an ongoing need for education. The challenge for law enforcement and fraud prevention partners is to identify and cut off the avenues that criminals use to recruit their mules.

Phone contracts

The level of misuse of mobile phone contracts decreased by 36% from 54,495 to 34, 738. Typically, in these cases an individual signs up to a mobile phone contract with an expensive handset, but they have no intention of honouring the agreement. The phone is sold on, often overseas as the devices cannot be used on a UK network, and no payments are made against the contract. As with the problem of money mules, further efforts are required to prevent members of the public from getting involved in this kind of criminality.

Never intended to pay

The biggest increase in misuse of facility frauds came from online retail accounts. This increased by almost 44% in 2015, compared with the previous year. These frauds are almost exclusively related to people spending on online shopping accounts and fraudulently evading payment. Uniquely for First Party Fraud cases, women are the perpetrators more frequently than men and account for almost 58% of these frauds, up from 55% in 2014. Half of those that misuse online retail accounts fall into the age 21-30 group.

Incidences of facility takeover fraud

Product	2015	2014	% Change
All-in-one	201	303	-33.7%
Bank Account	5,983	5,386	11.1%
Communications	2,154	3,198	-32.6%
Plastic card	5,810	8,353	-30.4%
Loan	6	30	-80.0%
Online retail	1,292	1,458	-11.4%
Other	51	43	18.6%
Total	**15,497**	**18,771**	**-17.4%**

Fraudulent use of plastic card accounts increased by 23% in 2015, showing that more people are using credit cards fraudulently. In contrast to the misuse of online retail accounts, Cifas' latest figures show that more than 85% of individuals fraudulently misusing plastic cards are men. In this case, there is a much more even split between 21-30 year olds (42%) and 31-40 year olds (39%).

More than 85% of individuals fraudulently misusing plastic cards are men.

Application fraud

This kind of fraud takes place where an applicant has used their own name but has made an application for an account, policy, service or insurance claim which contains a 'material falsehood', such as false employment details, concealed addresses or provided false supporting documents.

Incidences of application fraud

Product	2015	2014	% Change
All-in-one	24	13	84.6%
Asset Finance	7,318	7,527	-2.8%
Bank Account	7,191	8,162	-11.9%
Communications	1,124	1,345	-16.4%
Plastic card	2,558	2,696	-5.1%
Insurance	12,135	8,452	43.6%
Loan	6,360	5,556	14.5%
Online retail	173	194	-10.8%
Mortgage	4,037	3,913	3.2%
Other	266	102	160.8%
Total	**41,186**	**37,960**	**8.5%**

Motor insurance

Application fraud increased in 2015. This rise was primarily driven by an increase in the number or fraudulent applications for motor insurance. These frauds mainly involve the applicant trying to deceive the insurer so they pay a lower premium than they should. In 40% of cases the applicant gave a false address believing it would lower the premium because the address is in a safer area than where the car will actually be kept. Typically, the individuals that commit this type of fraud are students or other young people who have left home but continue to provide their parents' address as the place where the vehicle is kept.

Our data also revealed that in just over a quarter of cases the insurance policy has been 'fronted' by someone who will not be the primary driver of the vehicle. Often this kind of fraud is committed by a parent or guardian who claims that they are the main user of their child's car, while their son or daughter is listed on the policy as an occasional driver. In around 30% of cases the policy holder provided false payment information, be that false bank details or compromised card details. It may be that these instances of fraud are perpetrated by individuals who simply want to be emailed an insurance certificate and do not care that the policy will be voided when the payment fails to go through. It is likely, though, that there are still a number of unscrupulous 'ghost brokers' who are scamming people into giving them money to arrange insurance, only to find themselves out of pocket, uninsured and unaware.

Loans & mortgages

Application fraud to obtain loans increased by over 14% in 2015 compared with 2014. More than half of these cases involved the applicant attempting to hide an adverse credit history. The requirements of the Mortgage Market Review, leading to tightening up of lending practices on the mortgage market, may well be contributing to this increase.

The 3% rise in application fraud to obtain mortgages is perhaps not as marked as might have been expected, given the increased emphasis on affordability. While these frauds are some of the most common, the numbers are largely in line with those seen previously and it continues to be the hiding of undisclosed adverse credit information that is the most common falsehood, accounting for a third of cases.

False insurance claims

The National Fraud Database figures on insurance fraud are smaller than those for other sectors and should be considered in conjunction with other insurance fraud recording sources, such as the Insurance Fraud Bureau. False claims against home insurance policies accounted for 55% of the cases reported to the National Fraud Database, motor insurance accounted for 43% with the outstanding 2% representing false claims against other forms of insurance, such as travel and pet insurance.

Inflated claims were most common against home insurance policies, with the number of these cases more than doubling in 2015 compared with the previous year (albeit from a low base). These represented 35% of false claims. Other false claims involved the policyholder claiming for events that took place outside the period for which they were insured, staging events and claiming for events that never actually happened.

Where motor insurance is concerned, the most common fraud is to stage an event. These frauds accounted for more than 40% of false motor insurance claims and increased by 14% compared with 2014. Most worrying is the extent to which these frauds put UK road users in danger – a number of these cases will be 'crash for cash' events, where criminals enlist others to take part in staged accidents or induce innocent road users to crash into their vehicles. Such staged accidents continue to present a risk of death or serious injury.

Asset finance

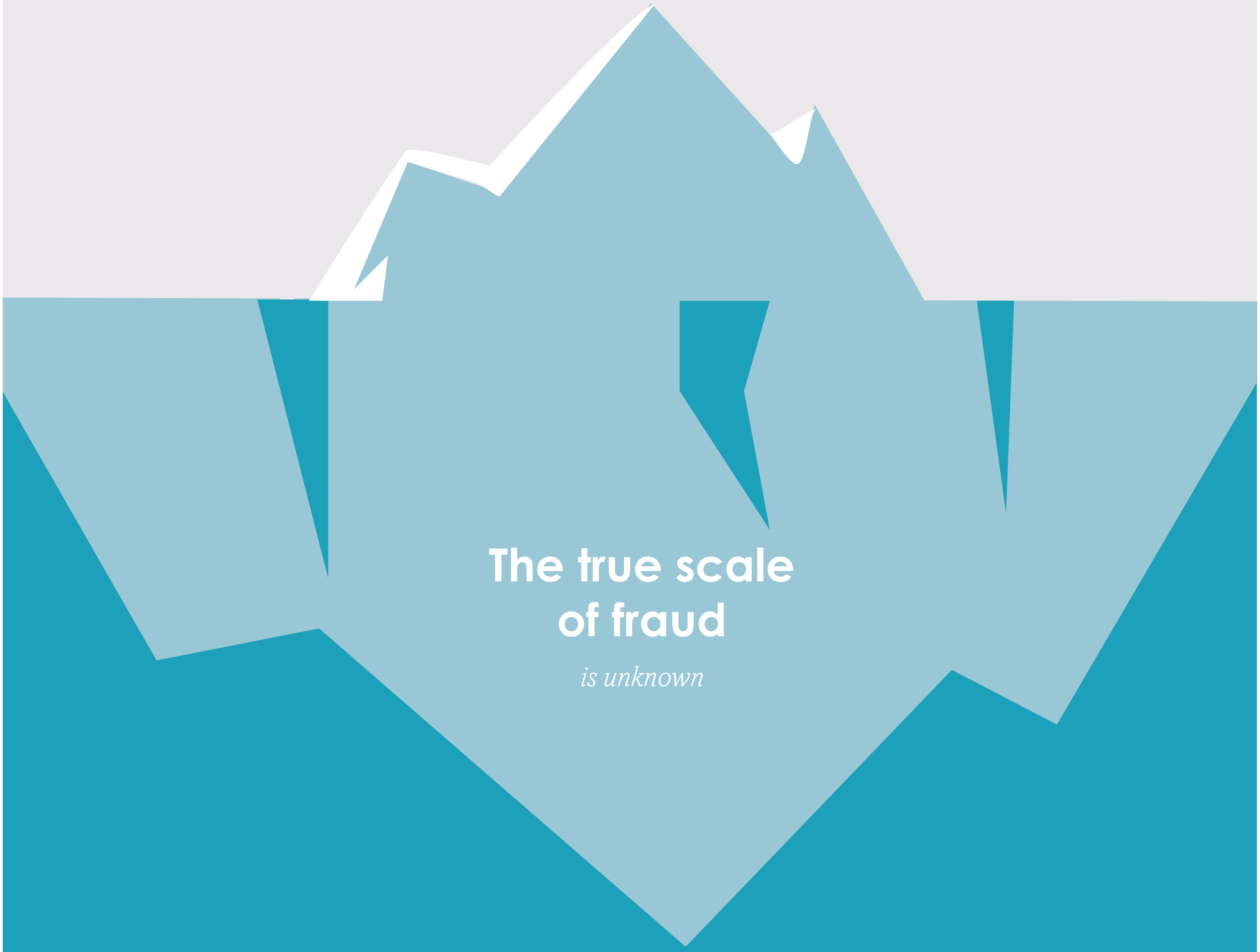
There were 258 cases of asset conversion in 2015, a 20% decrease on the 323 identified in 2014. These are cases where the individual has sold the asset (most often a car) when it was still subject to a credit agreement and therefore still the property of the finance company.

879

frauds every day

37

per hour
from Cifas members alone



The true scale of fraud

is unknown

This report has explored the frauds recorded by Cifas members in 2015 and outlined some of the key areas for action. The true scale of fraud in the UK will be higher than these figures.

Our mission is to detect, deter and prevent fraud and fraud-related crime in society by harnessing data and technology and working in partnership.

cifas.org.uk