YOUNG OR OLD – WHO IS MORE AT RISK?
Read more on page 6

HORIZON SCANNING:
Three things to look out for
Read more on page 18

INSIDE THE WORLD OF DEGREE FRAUD
Read more on page 29

FRAUDSCAPE

2019

cifas
Leaders in fraud prevention

IDENTITY FRAUD AND MONEY MULES RISE AGAIN

Fraud on the increase overall

Contents

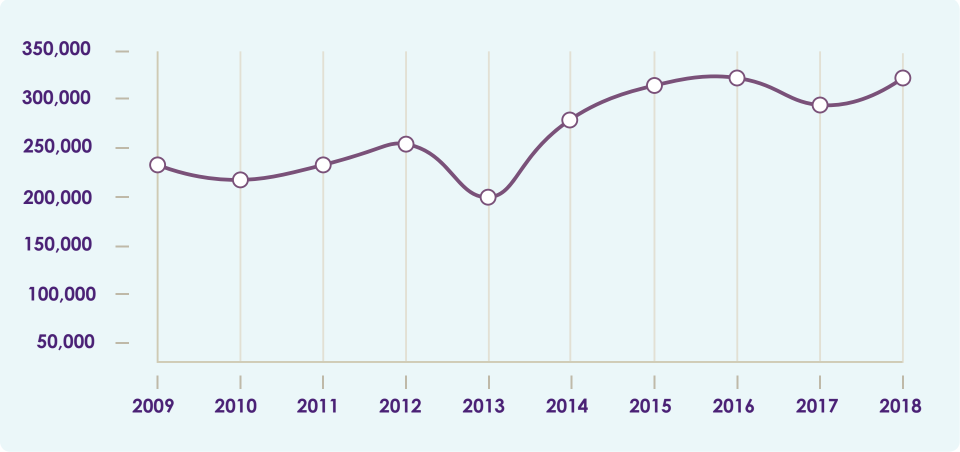
Introduction: Surge in identity fraudsters and money mules

By Sandra Peaston
Director of Research
and Development, Cifas

2018 sees rise in fraudulent conduct

Over 350 organisations contribute to the Cifas National Fraud Database (NFD). In 2018, these organisations reported almost 324,000 cases of fraudulent conduct – a 6% increase compared with 2017.

Number of fraud cases

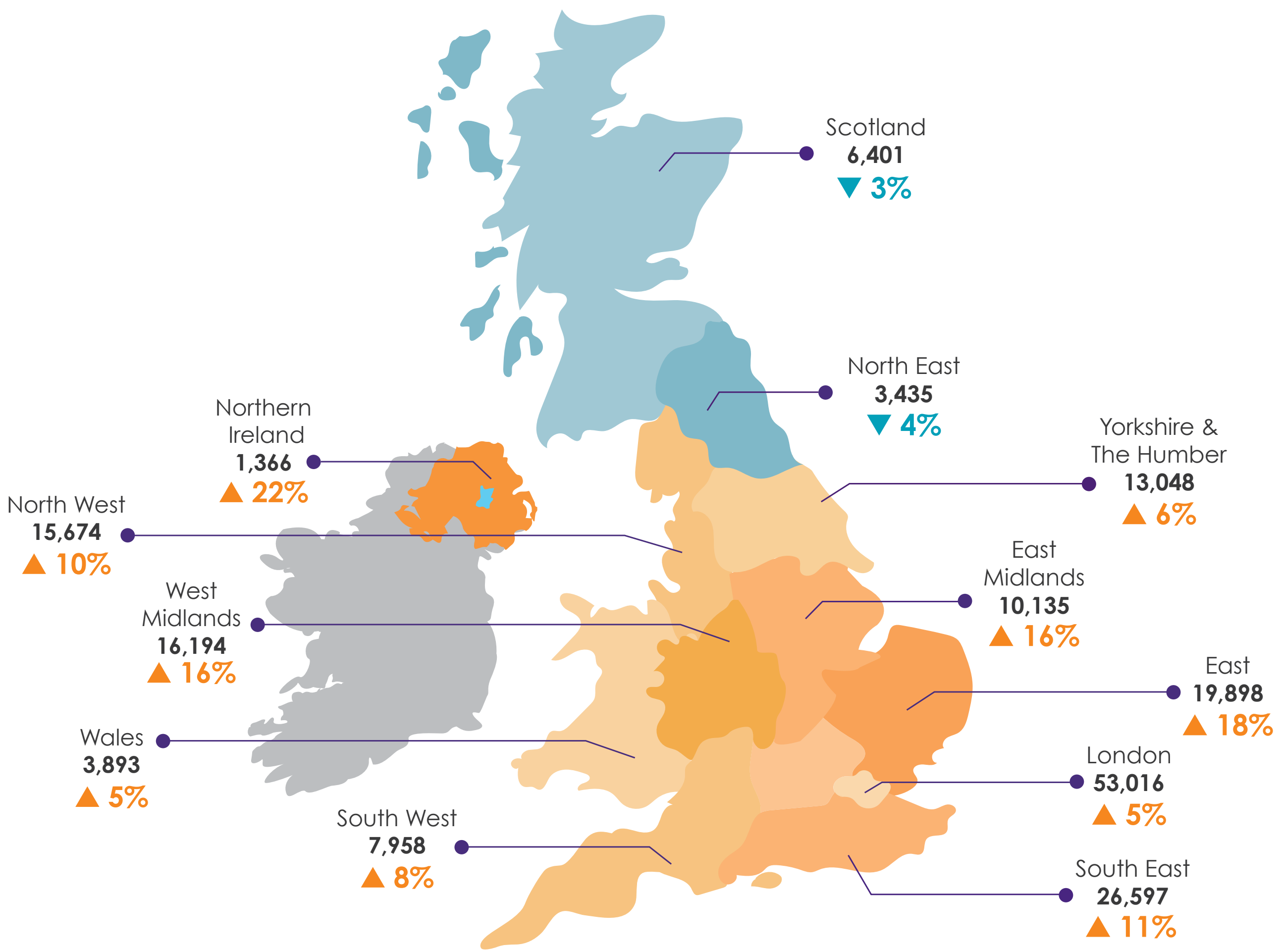


This represents a return to the high levels seen in 2015 and 2016, eclipsing a dip in 2017. The rise was driven by two main types of fraudulent conduct, namely identity fraud and the fraudulent misuse of a facility. Identity fraud increased by 8% and accounted for 58% of the frauds reported while misuse of facility increased by 10% and accounted for 25%. Both fraud types have long been causes for major concern, but for very different reasons:

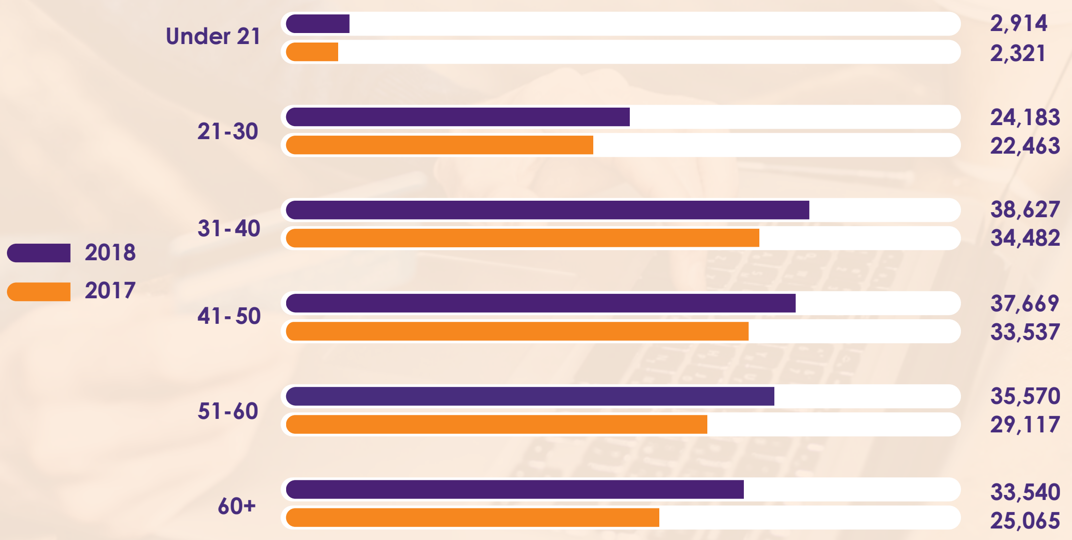
- 19 of every 20 identity frauds involve an innocent victim who is left to pick up the pieces after a fraudster has used his/her name to apply for products and services.
- The fraudulent misuse of a facility* predominantly relates to the misuse of a bank account, where the conduct bears the hallmarks of money mule activity. In short, this entails people laundering money through their bank accounts on behalf of criminals. The quantity of people, often young, engaged in this type of activity presents serious issues for financial services, regulators, law enforcement and society as a whole.

*Misuse of facility is where someone obtains an account/policy or other facility with the deliberate intent of using it for a fraudulent purpose.

Victims of impersonation by region



Victims of impersonation by age



Going Up

Asset conversion

▲ 10%

2018 | 602
2017 | 547

False insurance claims

▲ 27%

2018 | 685
2017 | 541

Identity fraud

▲ 8%

2018 | 189,108
2017 | 174,523

Misuse of facility fraud

▲ 10%

2018 | 82,032
2017 | 74,888

Going Down

Application fraud

▼ 18%

2018 | 25,424
2017 | 30,995

Facility takeover fraud

▼ 1%

2018 | 23,791
2017 | 24,070

Total

2018 TOTAL:

▲ 6%

2018 | 323,660
2017 | 305,564

Cifas case types explained

Asset conversion

The unlawful sale of an asset subject to a credit agreement; for example, a car bought on finance and sold on before it has been paid off.

False insurance claims

These occur when an insurance claim, or supporting documentation, contains material falsehoods.

Identity fraud

When a fraudster abuses personal data to impersonate an innocent party, or creates a fictitious identity, to open a new account or product.

Misuse of facility fraud

The misuse of an account, policy or product; for example, allowing criminal funds to pass through your account or paying in an altered cheque.

Application fraud

When an application for a product or service is made with material falsehoods, often using false supporting documents.

Facility takeover fraud

When a fraudster abuses personal data to hijack an existing account or product; for example, a bank account or phone contract.

Identity fraudsters target the young and old

Identity fraud continued to increase in 2018, with 8% more cases recorded to the National Fraud Database than in 2017. In 97% of these cases, the fraud involved the misuse of the identity of an innocent victim. Worryingly, those aged 21 or under and those over 60 experienced the greatest rises in victimisation.

In 2018,the targeting of plastic cards by identity fraudsters returned with a vengeance. There was a 41% increase on 2017 and, generally, when the product targeted was a plastic card, the victims tended to be older. More than 33,000 individuals over 60 became victims of impersonation during the year, an increase of 34% over the previous year. Plastic cards, in particular credit cards, have long been the product most targeted by identity fraudsters and as older people are perceived to be more likely to be approved for credit they have found themselves increasingly targeted.

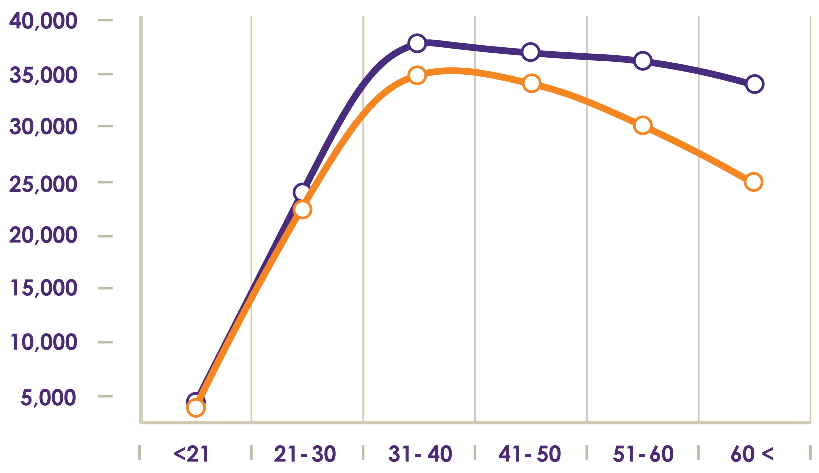
> **"THE INFORMATION A FRAUDSTER NEEDS TO COMMIT IDENTITY FRAUD CAN COME FROM A NUMBER OF DIFFERENT SOURCES."**

The substantial increase in the targeting of older people for identity fraud is a real cause for concern. However, more attention continues to be given to addressing fraud against the elderly and vulnerable where the individual is deceived by a fraudster into making a payment. While undoubtedly this type of fraud is the most harmful to the victim, the stark increase in identity fraud using the identities of older victims emphasises that this is not the only area where older age groups are at risk.

The information a fraudster needs to commit identity fraud can come from a number of different sources, but the two most likely are the Internet and the individual themselves. As more services have moved online, so there is a greater danger of data being involved in a breach. There is also a higher risk of people falling victim to phishing attacks or other forms of social engineering as there are more 'hooks' for the fraudsters to use to lure their prey. Whether someone over the age of 60 is new to the online world, or has 15 or more years experience, there are now more Internet users over the age of 60 than ever before. Accepting that Internet use increases the risk of identity fraud, it follows that there are now more potential victims in this age group.

Although an individual cannot do much about the possibility of their data being exposed by a breach at a service provider, there are however steps that they can take to mitigate the other areas of risk. There is clearly a requirement to provide educational messaging properly tailored to, and targeted at, older age groups to help them recognise and protect themselves from the risks fraudsters pose. This will be key to helping older age groups to safeguard their personal information online.

Age of victims of impersonation



At the other end of the spectrum, the number of under 21s becoming victims of identity fraud also increased in 2018 -by 26%. The continuing increase in the number of young victims of identity fraud is a clear signal that the need for education on the risks of fraud is pressing. Younger age groups, particularly under 21s, should present far less of a challenge when it comes to delivering appropriate prevention messages as many are still in education and can be more easily reached. The key here is to impress upon the authorities that this is an issue that deserves its place in the national curriculum.

In Fraudscape last year, we reported that fraudsters were willing to target different types of product. This year the trends show that fraudsters are willing to target different types of victim. Information from Cifas members and law enforcement highlights that fraudsters are also willing to use different methods. For example in the period where the biggest increases in identity fraud were reported, intelligence highlighted both the targeting of rural areas and blocks of flats in London by crime groups. This shows that the identity fraud threat continues to evolve and that, for identity fraudsters, one size certainly does not fit all. We must all be alert to this ever-changing crime.

Protecting your brand from identity fraud

Why do organisations need to invest in preventing identity fraud? Aside from a moral obligation to prevent the abuse of an innocent person's identity, there are two obvious reasons:

- to prevent financial loss to the organisation; and
- to comply with requirements to Know Your Customer, where that applies.

Less recognised, perhaps, is the value to the brand of effective prevention of identity fraud, and, where identity fraud does occur, swift and efficient resolution for the victim of impersonation. Every victim of impersonation is a potential or current customer, and for those organisations where their direct financial exposure is limited or non-existent, this could well be the area of the greatest impact. An individual who finds that they are receiving correspondence from an organisation that they have not entered into a relationship with is unlikely to regard that organisation well, and are therefore less likely to become a customer of that organisation in the future. An organisation does have the opportunity to reduce the negative impression, however, by providing excellent customer service when they are contacted by the victim. Investment in identity fraud prevention and resolution can therefore be seen as protecting future revenue.

*www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2018

Wolves of the Internet: where is data stolen online?

With identity fraud levels reaching an unprecedented 189,108 cases in 2018, the need to know how identities are compromised in the first place becomes more and more pressing. In today's world, much of what we do is online. Not only is it an easy and convenient way for us to do everyday tasks such as banking and shopping, but it also provides a way for us to network on both a professional and personal level. Ofcom research in 2018 revealed that 9 in 10 adults use the Internet, with more than three-quarters having a presence on social media or messaging sites and apps.

In 2018, Cifas released Wolves of the Internet: Where do Fraudsters hunt for data online, which looked at what personal information was available on the Internet and how it could all be pieced together. The report showed that 65% of victims of identity fraud had a visible social media presence or had been victims of a data breach. Of particular interest was that personal information had not just been stolen from profiles that were currently used, but also profiles that were no longer in use but had not been deactivated and deleted. Such profiles are often forgotten about, but remain in the public domain, revealing a wealth of personal information.

Younger victims of impersonation had a high social media presence and could easily have their identities pieced together through information available on various sites such as Facebook, LinkedIn and Google+. In such cases, their details were being used by fraudsters primarily for payday loans and mobile phone contracts. Although victims of impersonation aged 61 years and over had a low social media presence compared with their younger counterparts, they were more likely to have had their email address leaked (often repeatedly) as part of a data breach with the most likely sources of the breach being digital newsletters.

Gone is the myth that personal information is just sold on the dark web. This research shows that forums on the normal surface web play a pivotal role in the illicit trade of personal information. In one forum that had ostensibly been set up for sharing problems about telecommunications, 98% of the posts in one month were in relation to selling personal information.

The research revealed that often, it was forums like this, i.e. those no longer being used for their original purpose, that were instead being misused to sell information, mainly due to the lack of monitoring or administration. It is essential that owners of all forums monitor them, and/or close old forums down, as well as ensure that there are channels to report any misuse.

Recommendations

1 Review privacy settings on all your social media accounts. It may take time, but it is worth it to keep your personal information safe.

2 Be cautious of accepting an invitation to "connect" from individuals you do not know. LinkedIn provides advice in its help centre about reporting fake profiles, inaccurate profiles and scams.

3 Deactivate and delete old profiles. Using search engines like Pipl will help you identify your old social media accounts.

4 If it seems too good to be true, it probably is. Never reveal personal or financial information. See www.getsafeonline.org for more about how to safe on social media.

5 Use a password manager tool to help you to store your passwords securely and to help create new ones for every different site you use.

Steep rise in money mules

In 2018, organisations reported over 40,000 cases of fraudulent abuse of bank accounts that bore the hallmarks of money mule activity. This was an increase on 2017 of 26%.

A money mule is an individual who allows his/her bank account to be used to move criminal funds – money laundering. In some cases the recipient account will have been opened through identity fraud, but the number of such accounts has been decreasing due to improved security – leaving the fraudsters needing to recruit mules to launder their illicit funds for them. Often these funds will have come from members of the public who have fallen prey to Authorised Push Payment (APP) fraud, that is where a fraudster has deceived an individual into transferring his/her own money to another account. In the first half of 2018 alone, £145.4m was lost through this type of fraud.*

We would be naive to think, though, that it is purely the proceeds of fraud and scams that are laundered through networks of mule accounts. Fraud, particularly APP fraud, is in itself a harmful crime with the power to ruin lives, but it also provides an identifiable entry point into a mule network as victims know the account number and sort code to which they paid their money. This gives an investigator somewhere to start. The same does not apply to other crime types, so the extent to which mule networks are used to launder the proceeds of other forms of serious, organised crime is less well understood.

Mule herders (those controlling networks of mule accounts) recruit prolifically online, using social media and instant messaging channels to recruit an army of money mules. Individuals are recruited through posts on sites such as Facebook and Instagram, with pages advertising easy money or asking for use of accounts in return for a 'fee' or a cut of the proceeds. On many of these pages there will be images or videos designed to lure in potential mules by showing individuals flashing lots of cash, high-end trainers or other luxury items. When a potential mule takes the bait, the conversation is often taken to an encrypted channel such as WhatsApp. Mule recruits are typically young and male. In 2018, where the gender was known, 70% were male and 27% of account holders were under the age 21, with 50% 26 or younger. The age distribution of the account holders was very similar to that reported in 2017, but of interest was an increase in those over 40, where the rate of increase was higher, albeit from a low base.

The fraud prevention community continues to raise awareness of the harmful consequences of money mules, with education a key strand to preventing more young people becoming involved in criminal activity. As more people become aware of the impact and repercussions of money muling, including the potential for custodial sentences, then it is hoped that the number of people willing to engage in it will reduce. Cifas, through the Home Office-led Joint Fraud Taskforce seeks to encourage educators to provide fraud prevention awareness and prevention lessons. Anti-fraud lesson plans, prepared in partnership with the PSHE Association to support that aim, can be found at **www.cifas.org.uk/insight/public-affairs-policy/anti-fraud-lesson-plans**

40,139
Mule accounts in 2018

▲ 26%

31,846
Mule accounts in 2017

Money mules by age

MULE AGES	2017	2018	% CHANGE
<21	8,475	10,686	▲ 26%
21 - 30	12,149	15,066	▲ 24%
31 - 40	6,571	8,209	▲ 25%
41 - 50	2,948	3,970	▲ 35%
51 - 60	1,242	1,671	▲ 35%
60<	412	516	▲ 25%
14-24	**13,905**	**17,708**	**▲ 27%**

*www.ukfinance.org.uk/system/files/2018-half-year-fraud-update-FINAL.pdf

Public inquiries into fraud raise awareness amongst MPs

Over 3.2 million frauds are committed in England and Wales each year, with the cost to the economy running into billions of pounds. The impact on victims is far-reaching. It is therefore clear that fraud is the volume crime of our time. Proposed by Cifas, The All Party Parliamentary Group on Financial Crime and Scamming (APPGFCS) was established in October 2017. Its purpose is to give MPs and Peers the information they need to represent and advise their constituents effectively, and to understand the challenges that all sectors face in trying to stem the tide of this growing crime.

Conor Burns MP, Chair of the group, announced the APPG's first public inquiry in spring 2018. Wide in scope, this inquiry examined two particular themes, seeking insights into:

- Young people exposed to fraud as victims.
- Those who were being groomed by unscrupulous fraudsters to launder the proceeds of crime by acting as money mules.

The inquiry received evidence from 12 organisations including financial institutions, law enforcement, consumer groups and the third sector. The report, *Young Victims of Financial Crime** was published on 17 December 2018. It highlighted that young people are both at risk of being victims of fraud, and of being drawn into financial crime as perpetrators.

Evidence submitted to the APPG inquiry showed that, between 2015 and 2017:

- 41% of money mule accounts were linked to young people aged 25 or under, and
- There was a 24% increase in young people under 21 being involved in fraud either as a victim or perpetrator.

Among the recommendations made in the report was a call for fraud education to become a mandatory part of the safeguarding curriculum in schools. This would educate young people about how to protect their identities and how not to be drawn unwittingly into criminal activity.

> **"A BETTER UNDERSTANDING OF THE UNDERLYING FACTORS BEHIND FRAUD AND SCAMS CAN ONLY HELP IN THE SEARCH FOR SUSTAINABLE SOLUTIONS FOR THE FUTURE."**

The report and the APPG attracted significant media interest, with Conor Burns MP being quoted in The Times: "*There is more that government, industry, social media platforms and law enforcement bodies can do to help protect and prevent young people becoming involved in fraud and scams.*"

Following the success of the first inquiry, the APPG decided that the second should be framed to look at vulnerability. This was seen as a significant factor in many frauds and scams, with vulnerable people often specifically targeted by fraudsters.While much research into this area already exists, there were specific areas that the APPG considered should be explored in more detail.

In particular, these included issues around the potentially detrimental effect of differing definitions of vulnerability, and the understanding of transitional vulnerability. In September 2018, the Impact of Fraud and Scams on Vulnerable People inquiry opened for written submissions. Cifas, which provides the APPG secretariat, has received over 20 submissions on this matter from organisations across the public, private and third sector. The evidence is currently being assessed in preparation for the launch of the report in spring 2019 alongside a parliamentary debate led by the group's Chair.

The issues tackled by the Inquiries to date underline the need for parliamentarians to explore contentious subject areas and to consider what can and should be done in amelioration. Reducing fraud is never going to be easy. But understanding its drivers, and holding to account those who have a role to play in reducing it, is undoubtedly important for parliamentarians. A better understanding of the underlying factors behind fraud and scams can only help in the search for sustainable solutions for the future.

*www.appgfinancialcrime.org/uploads/files/APPG_V3_email.pdf

Fraud focus: bank accounts

In 2018, for the first time in recent memory, the fraudulent misuse of accounts exceeded the number of reported cases of identity fraud.

Cases of the fraudulent abuse of accounts increased by 19% in 2018 compared with 2017. Nearly 80% of these bore the hallmarks of money mule activity. This represents not just an increase in real terms, but also as a proportion of the misuse cases reported.

This finding must be taken in conjunction with the lower number of identity frauds to obtain bank accounts. These reduced by 12% in 2018 compared with 2017 and, to a degree, this decrease offset the increase in misuse cases reported.

It appears that those who wished to launder the proceeds of crime through bank accounts made a choice. Clearly, they considered it easier to recruit people to move money for them or to give up access to their account than to open new accounts in the name of a victim of impersonation or an entirely fictitious identity. While on the surface this could be considered a success for the security measures on applications for bank accounts, it would be premature to see this as a problem solved. There were still over 43,000 attempts to obtain a bank account in someone else's name, and another 2,362 in a fictitious name. In addition, with over 40,000 instances where it looks like an individual was recruited to do their dirty work for them, why would criminals waste time obtaining data and submitting applications?

This is especially true given that many of the applications would most likely be declined for either credit risk or fraud reasons. When an easier option is no longer available for criminals to obtain access to accounts, then the account opening processes will again come under pressure.

Technology continued to be at the forefront of the fight against identity fraud, not least because 98% of the reported identity frauds occurred online. Device recognition and data analytics have long since proven their value in countering this threat. In 2018, however, the number of false documents identified in association with identity frauds increased, despite the overall decrease in cases. This suggests that the use of document imaging through a smartphone or tablet at the point of application is bearing fruit as a fraud prevention tactic. Handsets will become ever more crucial as the channel through which people interact with their financial service providers and, as a consequence, will need to become increasingly effective in the fight against fraud.

Within the cases of identity fraud reported, the number of entirely fictitious identities accounted for a smaller proportion of cases than in 2017. Historically there was a higher proportion of false identities used to obtain bank accounts than other types of product. One of the reasons for this is that anyone wishing to live under an assumed name is likely to want a bank account in that name in order to function in society – an account to pay a salary into, to obtain a debit card, and so on. It was therefore surprising that in 2018 the proportion of false identities dropped to 5% from 8% in 2017. By comparison, across all products, only 3% of identity fraud cases in 2018 involved a false identity as opposed to a victim of impersonation. So while a higher proportion of false identities were used to obtain bank accounts than other products, the gap is closing.

Although they were by far the largest in terms of volume, identity fraud and misuse of accounts were not the only fraud threats affecting bank accounts. In 2018, bank accounts were one of the few products that saw an increase (2%) in the number of cases of fraudulent conduct by the genuine applicant compared with 2017. This was driven by an increase in the number of applicants fraudulently hiding a previous address where they had adverse credit information recorded against them. This accounted for 78% of application frauds in 2018 compared with 63% in 2017. The provision of false documents remained the second most common type of fraudulent conduct with applications, although the number of cases actually decreased, despite reports from fraud investigators that they were seeing an increased number of false utility bills provided in support of applications. It is important to ensure that those who would perpetrate these 'opportunistic' first party frauds are aware of the consequences. Their efforts are likely not only to prove fruitless in terms of obtaining the products they seek, but will also actively hinder their future applications as the fraudulent conduct they have perpetrated is reported and shared.

A continuing trend from 2017 was the reduction in the number of cases of facility takeover. This fell by another 45%, on the back of an 18% decrease in 2017. This means that the number of cases of this type of fraud have halved in the space of 2 years. Robust security measures in place make this type of fraud difficult for fraudsters. That in itself is likely to be one of the drivers for the increased problem of 2017, the key reason for the drop was a reduction in the number of instances of the genuine account holder fraudulently setting up regular payments from an innocent party's account – known as regular payments fraud. More robust scrutiny of third party authentication of payment instructions by card issuers has clearly driven down this type of fraud.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	7,203	7,369	▲ 2%
Facility Takeover Fraud	5,490	3,017	▼ 45%
Identity Fraud	51,544	45,528	▼ 12%
Misuse of Facility	42,803	51,106	▲ 19%
TOTAL CASES	107,040	107,020	0%

* appcrmsteeringgroup.uk/wp-content/uploads/2019/02/APP-scams-Steering-Group-Final-CRM-Code.pdf

** www.ukfinance.org.uk/system/files/2018-half-year-fraud-update-FINAL.pdf

Fraud focus: plastic cards

There was a 29% increase in fraud targeting plastic cards in 2018 compared with 2017. Last year's Fraudscape reported a surprising overall reduction, including the number of identity frauds to obtain plastic cards. At the same time, the takeover of card accounts increased substantially. In 2018, however, that situation dramatically reversed, with a huge surge in identity fraud and a decrease in takeovers.

Identity fraud to obtain a plastic card account, more than 9 in 10 of which were personal credit cards, increased by 41% in 2018 to more than 82,000 reported cases. The rise was predominantly seen in the final two quarters of the year. Only 2% of cases involved a fictitious identity as opposed to a genuine person's identity, and 83% involved impersonating the individual using their current address. This was up from 78% of cases in 2017. This means that fraudsters continued to acquire large volumes of current personal information, and to use it to make high volumes of online applications. Work to determine where personal data is compromised online has debunked the myth that data is only traded in marketplaces on the dark web, The research (*see Wolves of the Internet on page 5*) showed that trading is also prevalent on the surface web. For would-be fraudsters, therefore, this reduces the requirement for specialist skills and increases the opportunities.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	1,385	1,038	▼ 25%
Facility Takeover	7,365	5,797	▼ 21%
Identity Fraud	58,788	82,608	▲ 41%
Misuse of Facility	4,209	3,425	▼ 19%
TOTAL CASES	71,747	92,868	▲ 29%

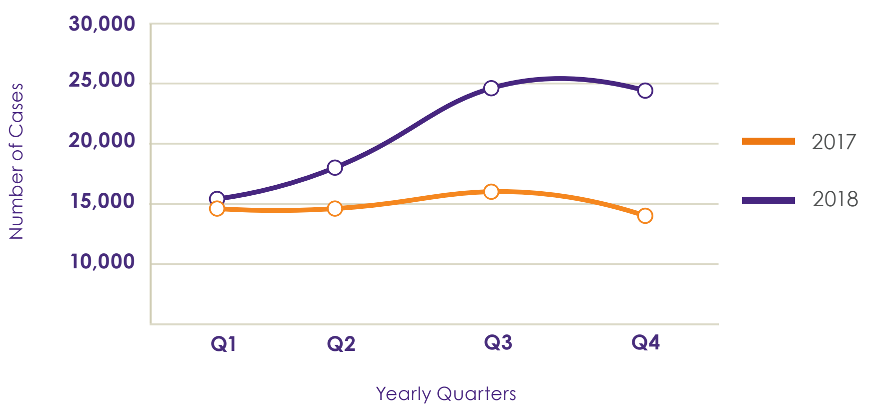
The number of victims of impersonation rose across all age groups. An increase in the quality of reporting in 2018 accounted for some of this (93% of impersonation cases involved a date of birth compared with 83% in 2017). Despite this, the surge in the over 60s becoming victims of identity fraud was significant, increasing from 9,700 in 2017 to 17,200 in 2018. This hike in older people becoming victims aligns with reports of increased targeting of rural areas, where an older demographic generally prevails. In addition, the Wolves of the Internet report also suggests that victims of impersonation in this age group are more likely to have had their personal details compromised in a data breach.

The cases of takeover of plastic card accounts fell, following a substantial increase the year before. It is worth noting, however, that 2018 levels remained higher than those seen in 2016. It is also interesting that the way fraudsters take over an account has shifted.

In 2017 most takeovers resulted from the perpetrator changing the address on the account. This was generally a precursor to requesting that replacement cards be issued to the new address. This type of fraud decreased by almost 25% in 2018. Instead, 2018 saw an increase in the instances of the perpetrator changing security or personal details on the account – effectively locking out the genuine account holder. This type of account takeover rose from 37% of cases in 2017 to 49% in 2018. The implication is that there was less of a requirement for the fraudster to obtain the cards themselves, but more for the fraudster to have access to the account itself, potentially to use it as another avenue for money laundering.

Misuse of plastic card accounts decreased again in 2018. As in 2017, the key reason for the drop was a reduction in the number of instances of the genuine account holder fraudulently setting up regular payments from an innocent party's account – known as regular payments fraud. More robust scrutiny of third party authentication of payment instructions by card issuers has clearly driven down this type of fraud.

Plastic card identity fraud cases



Fraud focus: telecoms

Frauds against telecoms are often organised attempts to obtain expensive handsets with the intention of selling them, most likely overseas as the handsets would be blocked by UK networks. Fraudsters will attempt this in various ways, with identity fraud and facility takeover being prime examples.

Fraud against telecoms, in particular mobile phone contracts, decreased by 9% in 2018 compared with 2017. Most notable, and counter to the overall trend, was a 25% reduction in the number of identity frauds reported. This followed a 47% increase the previous year. This reduction is likely to be a reflection of the tightening of processes. In 2017, the increase in identity fraud was attributed to abuse of 'click and collect' services where the application was submitted online, but the handset was obtained by an individual walking into a store and presenting a high quality fake bank card. Improved detection of such cards will have made this fraud more difficult and driven the number of identity frauds back down – although the number recorded in 2018 was still 10% higher than in 2016.

Linked to this, members have shared intelligence about increased levels of recruitment of third parties to pretend to be 'victims' of identity fraud. The third parties are recruited to provide their personal details and genuine bank card, allowing the application to be made in their name with someone else presenting their card in the branch. They are then instructed to report the card stolen, dispute the payment and claim to be a victim of identity fraud .

Victims of telecoms-related identity fraud continue to be a younger demographic than victims of identity fraud more generally. In 2018, 57% of identity fraud victims for telecoms accounts were 40 years of age or under, compared with 38% for all victims of Identity fraud. The accessibility of the product means that younger people are perceived to be just as viable a target for identity fraudsters as older age groups.

While overall reported fraud against telecoms decreased, the number of facility takeover frauds increased. Most commonly, the takeover was in order to obtain someone else's upgrade. This accounted for 45% of cases and increased by 22% compared with 2017. The biggest increase, though, was seen in instances of the facility hijacker attempting to change the security details on the account, effectively locking out the genuine customer. This increased by 57% to become the second most prominent reason for takeover.

2018 saw fewer instances reported of misuse of facility fraud where the customer had no intention of honouring the contract. The number of these cases, where the customer obtained the handset on contract without ever intending to make the monthly payments, decreased by 27% in 2018 compared with 2017.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	586	535	▼ 9%
Facility Takeover	9,342	11,924	▲ 28%
Identity Fraud	16,973	12,706	▼ 25%
Misuse of Facility	4,608	3,555	▼ 27%
TOTAL CASES	31,509	28,520	▼ 9%

Fraud focus: online retail

In 2018 there was a 12% rise in fraud reported by online retail members. This was largely due to an increase in members operating within the online retail sector, and so should not be interpreted as a trend. It does, however, highlight some of the main areas of concern for online retailers outside fraudulent card transactions at point of purchase.

Cifas members in this sector are mainly those that offer credit, where the primary fraud concern is to ensure that credit is not granted to anyone with the intention of spending and not repaying it.

This risk is clearly seen in the high proportion of cases recorded by the sector that relate to:

- misuse of facility, where the individual has fraudulently evaded payment; and
- identity fraud, where the fraudster attempted to obtain credit in the name of an innocent victim.

These account for 57% and 38% of reported cases respectively.

The cases where an individual has opened an account, purchased goods on credit, then fraudulently evaded payment, are more likely to be perpetrated by opportunists. The appeal of being able to purchase goods for either personal use or resale is obvious, but there is no attempt (or at best limited attempts) by the individual(s) to distance themselves from their actions. Potentially, they may not have considered what the consequences of their actions might be, or are hoping that the organisation will not consider it worthwhile to pursue the matter. This does not mean that all of these acts are as naïve as they might seem – for example where an individual is leaving the country and doesn't expect the repercussions to follow them across borders.

It is unsurprising that credit granting online retailers are targets for identity fraudsters, as a successful identity fraud essentially means free goods for the fraudster.

> **“A SUCCESSFUL IDENTITY FRAUD [AGAINST RETAILERS] ESSENTIALLY MEANS FREE GOODS FOR THE FRAUDSTER”**

The increase identified in the takeover of online retail accounts is similarly unsurprising, but in these circumstances the fraudster risks the genuine customer becoming aware of (and cancelling) the purchase before it is delivered. A competitive marketplace with ever more emphasis on customer service and speed of delivery increasingly plays into the hands of the fraudster, however. Next day or even same day deliveries reduce the chances of the genuine account holder being made aware of the fraud and forestalling it. These risks are extending beyond the credit granting online retailers as other retailers strive to make the checkout process smoother by allowing customers to pre-load payment card information to accounts. The security around access to these accounts must be robust enough to prevent them becoming easy prey for fraudsters.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	119	159	▲ 34%
Facility Takeover	1,002	1,903	▲ 90%
Identity Fraud	11,729	13,867	▲ 18%
Misuse of Facility	20,108	21,004	▲ 4%
TOTAL CASES	32,958	36,933	▲ 12%

Fraud focus: insurance

Cifas does not have comprehensive coverage of the this sector of the market so the full scale of insurance fraud is not reported to the National Fraud Database. To gain a complete understanding of the fraud threats in this sector, therefore, these figures need to be taken together with insights and trends reported by other fraud intelligence agencies, such as the Insurance Fraud Bureau.

The number of insurance fraud cases reported to the National Fraud Database decreased by 14%, with a reduction in application fraud cases the main reason. Counterbalancing this, however, was the continued rise in identity fraud. Identity fraud against the insurance sector has increased substantially over the last three years and in 2018 was the type of insurance fraud most frequently reported to the National Fraud Database, growing by another 15%. These cases continue to be perpetrated by:

- ghost brokers', who use the identities of innocent victims of impersonation to obtain insurance policies for their 'clients'; and
- by those who wish to ensure that a vehicle is insured for the lowest possible cost by using the details of someone who is considered low risk.

Wider public understanding of the work being done by the DVLA, the Motor Insurance Bureau and the police to identify uninsured vehicles will have fuelled this increase. This in turn has led to a development where insurers have noticed that fraudsters are adding named drivers to these policies. These named individuals are unconnected to the victim of impersonation, but are in fact the actual intended driver(s) of the vehicle. Adding named drivers in this way will be an attempt to increase the perceived legitimacy of the policy without substantially increasing the cost.

- The number of false insurance claims grew in 2018, with the biggest increase being people inflating what would otherwise have been genuine claims. The number of these cases increased by 56% to account for 27% of the false claims identified. People attempting to claim for events that did not take place also rose, albeit by less. These cases climbed by 18% and accounted for 24% of false claims.

It was reassuring, however, to see that the number of staged events actually decreased in 2018 (by 12%). This type of fraud often relates to 'crash for cash' claims, where criminal groups orchestrate traffic accidents, often involving innocent road users, in order to profit from fraudulent insurance claims. These events place road users in physical danger, so any reduction represents a major step in the right direction.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	5,462	3,220	▼ 41%
False Insurance Claim	541	685	▲ 27%
Identity Fraud	4,215	4,864	▲ 15%
Misuse of Facility	151	105	▼ 30%
TOTAL CASES	10,357	8,874	▼ 14%

THREE THINGS TO LOOK OUT FOR

There have been various developments recently that are likely to have an impact on fraud and fraud prevention over the next 12 months. Here we take a look at three of them.

OPEN BANKING

What is it?

Open Banking is an initiative designed to give consumers greater control of their money by obliging major banks to allow third parties to access customer account information, or make payments, with the consent of the customer. The idea is to encourage innovative services, such as apps that allow customers who choose to do so to see all their accounts in one place, irrespective of who the account is with, so that they have a greater understanding of their finances.

What's the (likely) impact?

Open Banking has actually now been around for over a year, but take-up remains relatively low with limited awareness of it among the public. We are also not yet seeing people making payments through Open Banking channels. This means that what would probably be the biggest fraud risk, the fraudulent initiation of payments, has not yet materialised. There are still risks though. The dearth of consumer knowledge about what Open Banking is may mean that fraudsters can exploit this when socially engineering information from potential victims by convincing them to do things that aren't in their best interests.

THE CONTINGENT REIMBURSEMENT MODEL

What is it?

This is a voluntary code that a number of banks have signed up to that sets standards and criteria for how and whether a customer is repaid in the event of an Authorised Push Payment (APP) fraud . Where the paying bank, the customer, and the receiving bank are not deemed to be at fault, then the customer is reimbursed from a central pot, funded by the banks.

What's the (likely) impact?

The standards within the code should encourage the signatories to improve the identification of payments that are likely to be fraudulent and to warn their customer accordingly. It follows that this should reduce the number of APP frauds that occur. It also means that where someone has been defrauded, he or she is more likely to be reimbursed, and so the direct harm to the individual is reduced. There is, however, speculation that this 'safety net' for customers may mean that there is less of a deterrent to risky behaviour. Where someone may have doubts about the legitimacy of an offer or investment opportunity (for example) they may be more inclined to go for it if they believe that, even if it is a fraud, they won't ultimately lose their money.

SECURE CUSTOMER AUTHENTICATION

What is it?

From September 2019 there will be a requirement for additional levels of security authentication for online payments, with customers not being able to 'check out' with just their card details (where the payment is over €30). That extra level of authentication requires that the customer's identity must be verified by two out of three of the following:

A. Something you know (e.g. a PIN)

B. Something you have (e.g. a card or a mobile phone)

C. Something you are (e.g. biometric identification like a fingerprint or voice).

What's the (likely) impact?

In principle, this should make Card Not Present fraud far more difficult, and that is one of the greatest areas of fraud loss in the UK. We need to be mindful, however, that fraudsters will be attempting to circumvent these measures if they can and, where they can't, they will migrate to other forms of fraud. It's also worth considering the extent to which Open Banking could displace payments from channels using Secure Customer Authentication – if an online retailer chooses to become a regulated provider of Open Banking, where payments can be initiated (for instance to purchase goods), then this will put more pressure on that retailer's account security to access pre-authenticated payment details.

These are just three of the measures that will affect fraud prevention in 2019 and beyond. As with any major change to the financial landscape, these carefully considered developments will bring with them new challenges and repercussions. Vigilance and co-operative working will continue to be paramount.

Editorial: Equipping ourselves for the challenges ahead

We live in interesting times. And that's without even mentioning Brexit, which I am consciously ignoring for the purposes of this article on the basis that anything I write now will probably turn out to be wrong before this is even published.

There are various interesting developments which have either landed or are about to do so which may have an impact on fraud and fraud prevention, or at least raise questions. What will Open Banking mean for fraud? What will Strong Customer Authentication mean? What will be the impact on payment service providers and scam victims of the Contingent Reimbursement Model? This is before we get too far into the ramifications of evolving fraudster methodologies and the use of emerging and developing technologies to prevent fraud.

Beyond such complexities, though, there remain some truths that are more stable. As this year's Fraudscape clearly illustrates, fraudsters continue to apply for products and services in other people's names, crime gangs continue to use the young and naïve as money mules to launder money, and scammers continue to exploit any available opportunity to part members of the public from their money.

At the heart of the response to fraud, communication and collaboration remain key. No one can expect to deliver an effective defence against these ever-present threats on their own as no one sees the whole picture. Data sharing between organisations through Cifas continues to provide evidence to substantiate this point, with £1.4bn in fraud loss prevented through the use of the National Fraud Database in 2018. An effective prevention strategy in one area, however, may well lead to a knock-on effect in another. We've seen this recently with the emergence of identity fraud to obtain insurance policies as a response to increasing scrutiny of uninsured vehicles on the roads. Similarly, as security around accounts increased, so fraudsters increasingly turned to targeting the account holders themselves. Clearly, in taking actions to prevent fraud, we need to be looking further ahead in order to limit such unintended consequences before they occur.

Careful horizon scanning will help us to be more proactive and to 'design out' opportunities for fraud in the future. There are, however, already some active steps that we can take to reduce the harm caused by fraud now, as well as further down the line. Much has already been said about the necessity of educating people to help prevent them from becoming victims of fraud. The increasing levels of identity fraud highlighted in this report, and the findings of the Wolves of the Internet research, are testament to this continuing requirement. Ultimately though, fraud is committed by people. There are many types of first party fraud, and while we've seen a general reduction in many variations of this type of fraud, this may have more to do with the escalation in vigilance and prevention practices of organisations than any reduced appetite of individuals to commit fraud. Partly, this may be down to people thinking that fraud is a victimless crime where it's only big business that pays (and they should probably pay more tax anyway).

It may also be that some don't realise what they're doing is actually fraud. For example, if you falsely claim to be the primary driver of a vehicle in order to name your teenage son or daughter on the policy, when you know full well that you are never going get behind the wheel of that car, you may just think that you've found a clever loophole. You haven't. It's a lie that has a direct impact on an insurer's decision, so it's fraud. Ensuring that people understand this, and that such behaviour is unacceptable, is vital. This is so not only to reduce the harm that individuals inadvertently cause themselves, but also to limit the amount of fraud that occurs in areas where the investment in prevention technologies is less developed or where the threat is less well understood.

During 2019, Cifas is working to raise awareness of first party fraud. We are drawing attention to those types of fraud which people either may not recognise as fraud – or perceive as acceptable – in order to challenge those perceptions. By doing so, it is hoped that a more aware public will be less likely to fall for some of the attempts by organised crime groups to dupe people into carrying out frauds on their behalf, such as becoming a money mule or being complicit in fraudulent attempts to obtain mobile phones. There will always be those who choose to commit crime, but if we can raise more people's awareness of what constitutes fraud, and thereby deter them from being drawn into it unwittingly, detection and prosecution efforts can be focussed on the real criminals.

INSIDER **THREAT**

Could your brand survive an internal fraud attack?

Who commits internal fraud?

See section 3

Global trade in false qualifications reflected in the latest figures

Internal fraud continues to present a serious danger to all industries, from the claiming of false qualifications and concealment of adverse employment history to wholesale data theft. Organisations simply cannot afford to be complacent when it comes to protecting their business, employees and customers from the insider threat. Read up on the latest trends and learn how to build your defences inside.

Definitions: Frauds covered in this section

Account Fraud

Unauthorised activity on a customer account by member of staff knowingly, and with intent, to obtain a benefit for themselves or others.

Being Bribed

Request, agree or receive or accept, for own or anoither benefit, a financial or another advantage with the intention to improperly performing a function or activity.

Dishonest action by staff to obtain a benefit by theft or deception:

Where a person knowingly, and with intent, obtains or attempts to obtain a benefit for themselves or others through dishonest action, and where such conduct constitutes an offence.

Employment Application Fraud (Successful)

A successful application for employment (or to provide services) with serious material falsehoods in the information provided, including the presentation of false or forged documents.

Employment Application Fraud (Unsuccessful)

An unsuccessful application for employment (or to provide services) with serious material falsehoods in the information provided, including the presentation of false or forged documents.

Unlawful Obtaining or Disclosure of Commercial Data

Where commercial data is obtained, disclosed or procured without the consent of the data owner, includes using the data for unauthorised purposes placing an organisation at a financial or operational risk.

Unlawful Obtaining or Disclosure of Personal Data

Where personal data is obtained, disclosed or procured without the consent of the data owner, includes using the data for unauthorised purposes placing an organisation at a financial or operational risk.

Focus on Internal Fraud

1. Introduction

According to *BDO Fraudtrack 2018*, employee fraud cost UK businesses about £500 million in 2017. Employee fraud not only has a major financial detriment, but it also affects the business reputationally and has an impact on staff morale.

The Cifas Internal Fraud Database helps over 200 organisations to share details of members of staff or applicants for employment whose conduct has been fraudulent. This article will look at the internal fraud cases reported to the Internal Fraud Database in 2018, providing insights into the trends that Cifas members experienced during this period.

2. Findings

There were 381 cases recorded to the Internal Fraud Database in 2018, a slight 9% reduction on the number recorded in 2017. 21% of the cases reported in 2018 were reported to law enforcement. Despite a 13% reduction in 2018, Dishonest action by staff to obtain a benefit by theft or deception remains the most common type of internal fraud. Employment application fraud (Unsuccessful) saw a 7% increase:

CASE TYPE	2018	2017	% CHANGE
Account Fraud	23	26	▼ 12%
Dishonest action by staff to obtain a benefit by theft or deception	166	191	▼ 13%
Employment application fraud (successful)	16	29	▼ 45%
Employment application fraud (unsuccessful)	164	153	▲ 7%
Unlawful obtaining or disclosure of commercial data	3	7	▼ 57%
Unlawful obtaining or disclosure of personal data	29	40	▼28%
TOTAL CASES	381	419	▼9%

2.1. Dishonest actions still remain the most common type of internal fraud.

Dishonest action by staff to obtain a benefit by theft or deception was the most common type of internal fraud in 2018, accounting for 46%. The most prevalent form of dishonest action during the year was theft of cash from the employer. This accounted for 22% of cases compared with 24% in 2017. The second most common fraud type in 2018 was theft of cash from a customer, which rose to 22% of cases in 2018 compared with 17% in 2017.

The growing pressures of modern life can conspire to drive up internal fraud. The Trades Union Congress noted in its spring statement in 2019* that in the third quarter of 2018, unsecured borrowing per household was at an all-time high of £15,400. In addition, unsecured debt as a share of household income had reached its highest in over ten years. Such financial pressure might conceivably drive an employee to steal from his/her employer or customers to supplement income.

> "THE MOST COMMON FORM OF DISHONEST ACTION IN 2018 WAS THEFT OF CASH FROM THE EMPLOYER"

*www.tuc.org.uk/sites/default/files/springstatement2019.pdf

2.2. Employment application fraud still high, with employment application fraud (unsuccessful) seeing a 7% increase.

Employment application fraud remained the second most common internal fraud. Although employment application fraud in general saw a slight reduction between 2018 and 2017, employment application fraud (unsuccessful) saw a 7% increase in 2018 compared with 2017: (this is where an applicant's fraudulent application was detected before an offer of employment).

Hiding adverse credit information on an application form was the reason for a large number of cases (53% in 2018, down from 60% in 2017). Also, the number of people using false qualifications was the highest on record, with 12 individuals reported in 2018 compared with just one in 2017. There are a number of websites offering degrees for sale, encouraging individuals to buy a degree to help them get that promotion they need, thereby enabling candidates to take roles that they are not qualified to do. Not only could the use of false qualifications lead to a criminal conviction, it might also put others at risk, particularly if the job requires a specific skill set such as within healthcare.

Hiding unspent criminal convictions remained the most common form of fraudulent conduct where the employment application fraud was successful, as the individual may have started in employment before the pre-employment checks had been completed. False references saw an increase of 150% in 2018 compared to 2017, with members reporting the highest number in five years. In these cases, the individual had provided a fictitious reference confirming certain work experience, to put themselves ahead of others applying for the same job.

3. Who commits internal fraud?

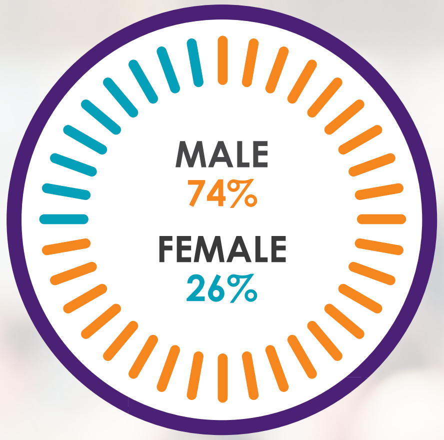
Overall, 61% of individuals recorded on the Internal Fraud Database in 2018 were male, which was slightly up from 60% in 2017. Notably, the proportion of males filed for account fraud increased to 74% in 2018 compared with 58% in 2017. The majority of males worked not only in branches but also in customer call centres, in positions where they could more easily access customer information. Office for National Statistics (ONS) data showed that in September 2018 there was a 23% increase in the number of men in customer service occupations, meaning more men had the opportunity to access such records.

Traditionally, men have been associated more with the unlawful obtaining or disclosure of personal data, but, more recently, women have become increasingly involved in this kind of conduct.

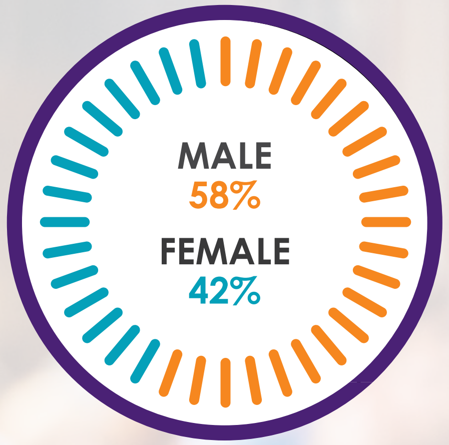
The proportion of females committing this type of fraudulent activity in 2018 increased to 48% compared with 30% in 2017.

WHO COMMITS INTERNAL FRAUD?

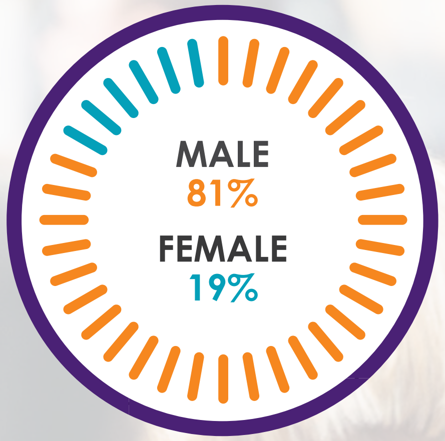
Account Fraud



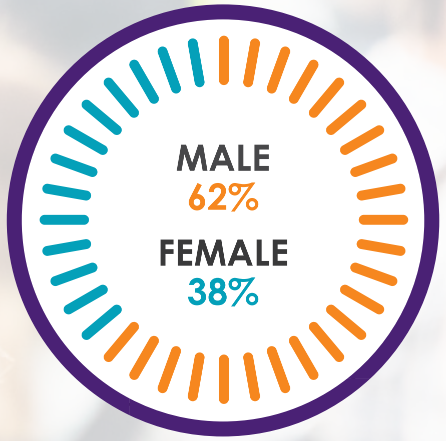
Dishonest Actions



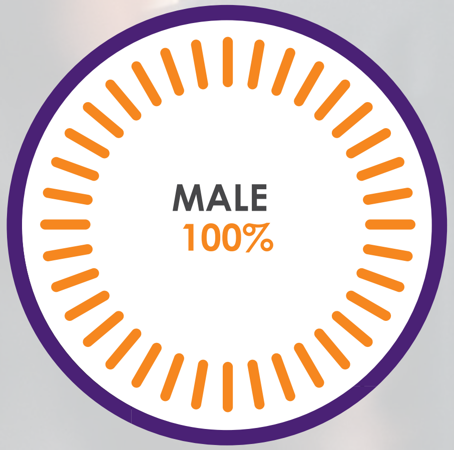
Employment Application (successful)



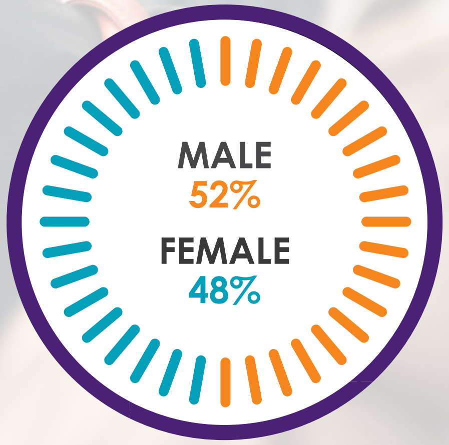
Employment Application (unsuccessful)



Unlawful Obtaining or Disclosing Commercial Data



Unlawful Obtaining or Disclosing Personal Data



3.1. Focus on males committing Employment Application (Unsuccessful) Fraud:

There was a 19% increase in the number of males recorded for employment application fraud (unsuccessful). Of the reasons provided, a large proportion of cases were for concealing employment history (47%). There was, however, a 500% increase in false qualifications being used. 50% of males recorded for this type of conduct were aged between 21-30 and a third were aged over 35. All applicants were for roles within the banking industry.

In 2018, the BBC exposed the global trade in fake qualifications across various industries. Using fake qualifications in order to meet the criteria of the job role is fraudulent and can lead both to a conviction, and to being recorded to the Internal Fraud Database. It is essential that employers not only check references but also verify qualifications through agencies such as HEDD, the Higher Education Degree Datacheck.

3.2. Focus on females Unlawfully Obtaining and Disclosing Personal Data.

2018 saw a 17% increase in the number of females involved in the Unlawful obtaining or disclosure of personal data, with a 300% increase in the number of females aged over 41 years old conducting this type of activity. Females were mainly filed because for contravention of systems access policy, disclosing customer data to a third party or for fraudulent personal use of customer data. 67% of females had been well established within the company, being employed for at least five years and 17% had been in employment for at least 25 years.

A large proportion of females recorded for this type of conduct worked within a branch or outlet (64%), with discovery means mainly being internal audit controls (57%) or by the customer (29%), resulting in the majority of females being dismissed from the company.

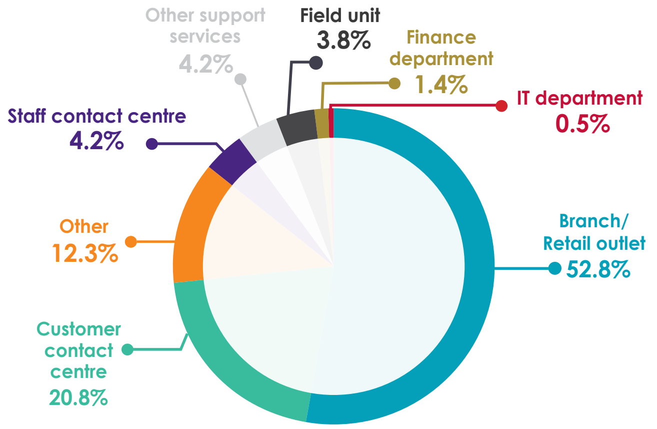
The increase in females over 41 becoming involved in this type of fraudulent conduct may be due to social pressures, but also a lack of investing in their financial future, therefore looking for other means to supplement their income. A UBS study* found that most women in the UK defer to their spouse for long time financial decisions and a prospects study** found UK women face retirement with 40% less in their pension pots than men.

* www.ubs.com/global/en/wealth-management/our-approach/investor-watch/2019/own-your-worth.html?intCampID=INTERNAL-HPPROMOTEASER-global_own_your_worth-en

**www.prospect.org.uk/help-at-work/pensions-retirement/pension-gender-pay-gap

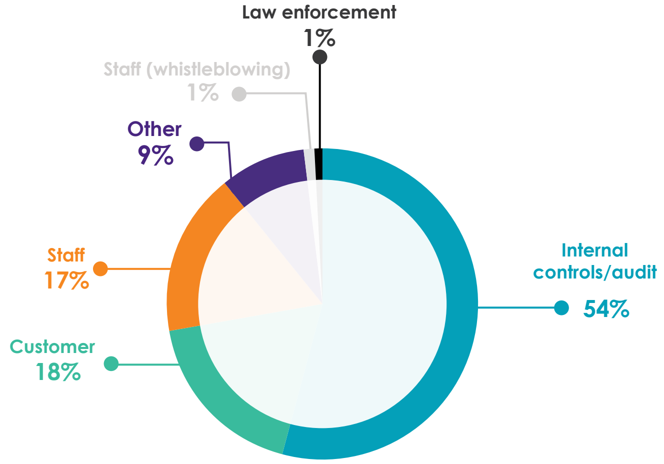
Overall business areas experiencing internal fraud

Overall, 53% of individuals reported to the Internal Fraud Database worked in a branch or retail outlet, with 21% within customer contact centres. The majority of individuals working in these departments were recorded for dishonest actions. The ease of access to assets in these departments is very high. Although businesses have taken steps to reduce opportunities for fraud, PwC's Global Economic Crime and Fraud survey 2018* showed that only 34% of companies actively invested in measures to counteract motivations and rationalisation, showing that more needs to be done to implement an anti-fraud culture:



Means of discovery

The majority of fraudulent conduct in 2018 was highlighted by internal controls and audit (54%), a slight decrease from 59% in 2017. Encouragingly, fraud reported by staff increased to 17% compared to 11% in 2017, suggesting that companies are providing staff with the channels to report fraudulent conduct. There is still more to be done, however, as demonstrated by a recent Tax Incentivised Saving Association survey published in 2018, which stated that over a third of businesses do not measure whether they have an anti-fraud culture:



*PwC, Global Economic Crime and Fraud Survey 2018: www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

The value of being 'trusted'

How do you place a value on trust? Increasingly, suppliers are being asked to demonstrate their trustworthiness by completing Third Party Supplier Questionnaires. There is a whole industry springing up to support organisations as they navigate their way through completing these (often complex) documents because the consequences of failure could well include the loss of the client.

There are several factors that go into establishing trust and, unsurprisingly, ensuring data security is high on the list.

If someone else holds your customers' data on your behalf, then it is your reputation on the line if goes missing – so working with suppliers who can be trusted to keep it secure is imperative. This isn't just about systems, though; it also encompasses physical security and the integrity of staff. Many organisations document the systems and processes that go towards data security, but far fewer are able to provide real assurance about the people using them and the systems are only as secure as those individuals.

For organisations that hold or process data of behalf of others, the use of data sharing schemes such as the Cifas Internal Fraud Database is a strong step towards providing such assurance to their clients. Not only does it mean that those with a history of fraudulent behaviour can be identified at the point where they apply for a role in the organisation, but it sends a clear message both internally and externally that internal fraud is not tolerated.

So, while the value of trust in today's environment is financial in terms of avoiding the loss of clients as a result of being unable to establish trust adequately, it goes further than that. Clear indications of trustworthiness can also be used as a selling point for acquiring new clients. Ultimately, a robust anti-fraud stance can be revenue generating.

FOCUS ON: DEGREE FRAUD

By Chris Rea
Head of HE Services, Prospects

Verifying candidates' credentials before making an offer of employment is, on the surface, nothing new. Traditionally, as a minimum, references are confirmed, and rigorous identity checks are carried out. Those long-established processes are still useful but, given the rise in 'degree fraud', no longer sufficient in themselves.

'Degree fraud' encompasses multiple types of deceit. These include:

- the manufacture of fake degree certificates (fake versions of real certificates or certificates from non-existent universities)
- the creation of bogus university entities
- the operation of degree and diploma mills (which provide fake degree or diploma certificates for a fee), and
- exaggeration or outright lies on CVs.

With the advent of desktop publishing, colour printers and other sophisticated technology, fraudsters now have access to the tools they need to turn out passable versions of real certificates. Crests and fonts are easy to imitate but watermarks and holograms can now be reproduced without difficulty. Sometimes even professionals in university registry offices find it difficult to tell a fake from the real thing.

Prospects Hedd, the UK's official degree verification service, was developed to streamline the process by which third parties – usually employers and screening agencies – may verify candidates' degree credentials. This role was formalised four years ago as Hedd began a degree fraud reporting service operated on behalf of the Department for Education.

The service has investigated more than 100 bogus providers and has helped to shut down more than 50 of them. The database of degree-awarding bodies on www.hedd.ac.uk includes more than 250 non-legitimate bodies, most of which are entirely bogus institutions. The number of cases creeps up every year: 25 in 2017, 29 in 2018, and 12 already in 2019, indicating that this year may be a bumper year for bogus institutions.

> "Fraudsters now have access to the tools they need to turn out passable versions of real certificates."

Employers and universities are the main providers of reports of suspected degree fraud, but Hedd is also contacted by employees with concerns about colleagues' credentials. Sometimes it can be very close to home – with one instance where a father informed on his son who had made up his degree credentials.

Much of Hedd's work is concerned with raising awareness of the problem and the risks posed by degree fraud, and with encouraging employers to make the necessary checks. It provides toolkits for employers and for universities to help with this.

It also runs an annual campaign warning graduates not to post photographs of their degree certificates on social media. Cifas' initiative 'Don't finish your career before it starts' has played an important role in the work with students, helping to increase awareness of the issues. Risk Advisory Group research in 2017 revealed that just 25% of students were aware that lying about qualifications is illegal.

For the future, the current drive by interested parties to tackle the problem in a co-ordinated way bodes well. Universities, employers and government are sitting down together to share ideas on best practice and enforcement. There are moves to include degree verification in the university Quality Code which, at a stroke, would deal with the use of fake certificates to gain admission to postgraduate courses. The health sector, reeling from a succession of high-profile degree fraud cases (most recently the unmasking of the Cumbria 'psychiatrist' who didn't have a medical qualification), is seeking to extend verification into non-clinical roles. Questions have been raised in Parliament about making degree verification mandatory in key sectors, including the Civil Service. Only when all employers check the authenticity of all their hires all the time will degree fraud be eradicated.

MARYLEBONE UNIVERSITY CASE STUDY

One afternoon in October 2018, Hedd received a call from an animal welfare charity in Canada. The HR Manager expressed concerns about the degree credentials of their recently-appointed Director of Animal Health. The employee in question claimed to have an MSc in Zoology from Marylebone University. The HR Manager said that, although they didn't have expert knowledge of the UK higher education system, they hadn't heard of Marylebone University.

She was right. It doesn't exist (even if, like Ridgeshire, it sounds as though it might). She sent over the certificate and transcript for inspection, and we confirmed that Marylebone University was not a legitimate degree-awarding body (code for 'It's a bogus university').

The following day, we received a call from the employee. Summoning all his powers of indignation, he told us that he had studied a 6-week online MSc programme in Zoology at Marylebone University in good faith. He was horrified to learn that it might not in fact be a real institution. He said he was taking the first flight back to the UK to sort things out. As the conversation proceeded, however, his vehemence subsided and his parting remark was 'How screwed am I?' Very screwed, as it turned out – he was sacked later that day. Interestingly, it transpired that great swathes of the previous work experience he had claimed were also fictional.

Product appendix

All-in-one

In relation to frauds against all-in-one products:

- After increases from 2015 to 2017, 2018 saw a decrease overall of 39%. As in previous years, the facility takeover frauds predominantly related to unauthorised electronic payment instructions.
- The number of identity frauds decreased slightly in 2018.
- The volumes are low in comparison to other products, which means that small changes in numbers lead to more substantial percentage changes.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	3	2	▼ 33%
Facility Takeover	522	286	▼ 45%
Identity Fraud	45	36	▼ 20%
Misuse of Facility	11	33	▲ 200%
TOTAL CASES	581	357	▼ 39%

Asset finance

In relation to frauds against asset finance products:

- The total number fell by 16% in 2018 compared with the previous year.
- The largest increase was in the number of facility takeover frauds. This was due to one member filing a high number of cases involving unauthorised address changes.
- Application frauds decreased by 21% from 2017 to 2018. The majority of these (80% and 73% of cases respectively) were reported as a result of undisclosed addresses with adverse information.

CASE TYPE	2017	2018	% CHANGE
Asset Conversion	520	574	▲ 10%
Application Fraud	10,791	8,506	▼ 21%
Facility Takeover	6	26	▲ 333%
Identity Fraud	970	876	▼ 10%
Misuse of Facility	1,487	1657	▲ 11%
TOTAL CASES	13,774	11,639	▼ 16%

Bank Account

Bank accounts were the most targeted product in 2018, constituting one third of all the cases filed during the year.

- Identity frauds to obtain bank accounts fell by 12% in 2018. Misuse of facility cases were therefore accounted for the majority of frauds. This reverses the situation seen in 2017 when identity frauds accounted for 48%, falling to, 43% in 2018, whereas misuse of facility frauds constituted 40% in 2017 rising to 48% last year.
- Misuse of facility cases saw a 19% increase in 2018. This figure has been increasing annually since 2014. Almost 80% of the 2018 misuse of facility cases indicate a link to money mule activity.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	7,203	7,369	▲ 2%
Facility Takeover	5,490	3,017	▼ 45%
Identity Fraud	51,544	45,528	▼ 12%
Misuse of Facility	42,803	51,106	▲ 19%
TOTAL CASES	107,040	107,020	0%

Product appendix

Telecoms

In relation to frauds against communications products:

- The total number fell by 9% in comparison to 2017. This was due to dramatic decreases in (i) misuse of facility cases involving evasion of payment, and (ii) current address frauds on identity fraud cases.
- The only increase for communications products was in facility takeover frauds, where there was a steep rise of 28%. These were mostly in relation to unauthorised changes to security or personal details on the account.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	586	535	▼ 9%
Facility Takeover	9,342	11,924	▲ 28%
Identity Fraud	16,973	12,706	▼ 25%
Misuse of Facility	4,608	3,555	▼ 27%
TOTAL CASES	31,509	28,520	▼ 9%

Plastic Cards

In relation to frauds against plastic card products:

- These increased by 29% from 2017 to 2018.
- Identity fraud saw a 41% increase in 2018 due to a 49% increase in the number of current address fraud cases.
- Facility takeover fraud cases fell by 21% from 2017 to 2018. Most of these over both years related to unauthorised address changes.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	1,385	1,038	▼ 25%
Facility Takeover	7,365	5,797	▼ 21%
Identity Fraud	58,788	82,608	▲ 41%
Misuse of Facility	4,209	3,425	▼ 19%
TOTAL CASES	71,747	92,868	▲ 29%

Insurance

In relation to frauds against insurance products:

- These fell by 14% in 2018 in comparison with 2017.
- Application fraud saw a large decrease this period of 41%. This was in part due to substantially fewer cases involving a false address on the application.
- Identity fraud saw a 15% increase in 2018. Most notably within this case type, there was a significant increase in current address fraud cases.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	5,462	3,220	▼ 41%
False Insurance Claim	541	685	▲ 27%
Identity Fraud	4,215	4,864	▲ 15%
Misuse of Facility	151	105	▼ 30%
TOTAL CASES	10,369	8,874	▼ 14%

Loans

In relation to frauds against loan products:

- These increased by 3% in 2018.
- Facility takeover frauds saw a 161% increase in 2018: notably, one member reported a 158% increase in the number of frauds on personal unsecured loans.
- The number of application frauds to obtain a loan decreased by 14% in 2018, accounted for by a decrease in applications containing undisclosed addresses with adverse information.

CASE TYPE	2017	2018	% CHANGE
Asset Conversion	27	28	▲ 4%
Application Fraud	2,416	2,082	▼ 14%
Facility Takeover	309	806	▲ 161%
Identity Fraud	20,082	20,665	▲ 3%
Misuse of Facility	1,399	1,263	▼ 10%
TOTAL CASES	24,233	24,844	▲ 3%

Online retail

In relation to frauds against online retail products:

- These rose by 12% in 2018.
- Identity fraud saw an 18% increase, mainly due to a rise in current address impersonations.
- Facility takeover fraud rose by 90%, seeing almost double the number of cases reported for an unauthorised instruction to despatch goods.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	119	159	▲ 34%
Facility Takeover	1,002	1,903	▲ 90%
Identity Fraud	11,729	13,867	▲ 18%
Misuse of Facility	20,108	21,004	▲ 4%
TOTAL CASES	32,958	36,933	▲ 12%

Product appendix

Mortgages

In relation to frauds against mortgage products:

- These fell by 18% in 2018.
- The number of misuse of facility cases decreased by 17%. There had been an unusually high number of instances of misuse of a mortgaged property in 2017, so this has decreased to more expected numbers.
- In 2018, the use of false or stolen documents replaced frauds around declared levelsof income as the most common reason for reporting application frauds.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	2,915	2,386	▼ 18%
Facility Takeover	9	6	▼ 33%
Identity Fraud	45	45	0%
Misuse of Facility	70	58	▼ 17%
TOTAL CASES	3,039	2,495	▼ 18%

Other

In relation to frauds against 'other' products:

- These decreased by 21% in 2018.
- Other' primarily relates to cases of identity fraud to obtain credit files, which can be a precursor to further identity fraud. These cases fell by 22% in 2018 compared with 2017.

CASE TYPE	2017	2018	% CHANGE
Application Fraud	74	126	▲ 70%
Facility Takeover	25	24	▼ 4%
Identity Fraud	10,131	7,898	▼ 22%
Misuse of Facility	42	24	▼ 43%
TOTAL CASES	10,272	8,072	▼ 21%

Why join Cifas?

Fraud and financial crime is a growing threat

Official UK government statistics show that fraud is now the most prevalent crime in the UK. The cases filed by our members also show the increasing threat from both external and internal fraud.

Fraud and financial crime is a shared threat and all businesses and organisations are a target. Criminals want the same thing from your business as they do from millions of other UK organisations, regardless of sector or size.

They strike at an organisation through any vulnerability they can find - be it systems, people or process - using any method they can: hacking, cybercrime, bribery and corruption, or the 'social engineering' of insiders.

Cifas is the shared solution

Through Cifas – an independent, not-for-profit organisation – hundreds of organisations from across all sectors share data and information to protect their business, employees and customers from the effects of fraud and financial crime. Become a Cifas member and we can help you help your organisation, customers and clients from falling victim to fraud and other financial crime. Our method of collaboration and cooperation, bringing together sectors and organisations to share intelligence and data, is the effective way to tackle financial crime. Visit www.cifas.org.uk for more information. You can also follow us on Twitter, LinkedIn and Facebook (search for CifasUK), or join the Cifas group on LinkedIn.

cifas

Leaders in fraud prevention

www.cifas.org.uk