THE FRAUDSCAPE

2018

Fraudulent conduct decreases overall – but worrying rises in some areas

Over 300 organisations contribute to Cifas' National Fraud Database. In 2017, these organisations identified and recorded 305,564 instances of fraudulent conduct, which was 6% fewer than in 2016.

This reduction was due to lower recorded cases of misuse of facility, where people fraudulently evaded payment for products or services. These products were primarily mobile phone contracts, where individuals obtained a handset on a contract but never made the monthly payments; or online retail credit accounts, where the individual had no intention of paying for the goods they ordered.

Continued on page 2

Identity fraud continues to grow – but also evolve

The number of identity frauds increased further in 2017, with almost 175,000 cases recorded. This was only a 1% increase compared with 2016, but a 125% increase compared with 10 years ago. In line with previous years, in 95% of cases the fraudster used the identity of an innocent victim, and in almost 4 out of 5 cases, the victim's genuine address had been used.

The difference this year is that increases have not been seen in fraudulent applications for plastic cards and bank accounts, which are usually the products most frequently targeted by identity fraudsters. The biggest increases have actually been seen in telecoms, online retail and insurance.

Continued on page 4

Lower filings of misuse of facility cases – but identity fraud rises

Continued from page 1

While lower levels of fraudulent conduct must be seen as positive, it should not distract from the concerning increases that were seen in some areas. Most notably, the unremitting rise of identity fraud continued, hitting a high of 174,523 cases in 2017. In 95% of these cases it involved the impersonation of an innocent victim.

Another worrying trend was that, despite the decreases in misuse of facility fraud overall, misuse of bank accounts increased (up 13%), with many of these cases involving young people using their bank accounts to launder criminal funds, essentially becoming 'money mules'.

CASE TYPES

Asset conversion

2017..........547

2016..........381

↑44%

Application fraud

2017..........30,995

2016..........31,559

↓2%

False insurance claims

2017..........541

2016..........496

↑9%

Facility takeover fraud

2017..........24,070

2016..........22,525

↑7%

Identity fraud

2017..........174,523

2016..........172,919

↑1%

Misuse of facility fraud

2017..........74,888

2016..........96,803

↓23%

Total

↓6%

2017	**305,564**
2016	**324,683**

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.

Application fraud

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

False insurance claims

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

Facility takeover fraud

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

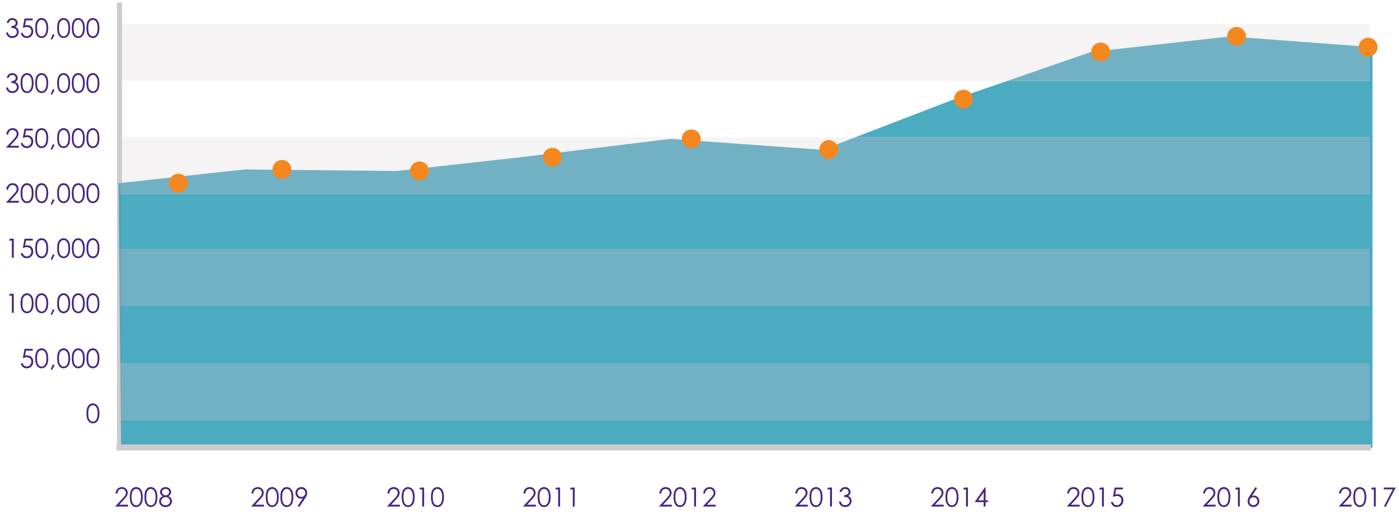
Identity fraud

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.

Number of fraud cases



Telecoms and online retail among sectors targeted by fraudsters

Continued from page 1

This 'retargeting' by identity fraudsters can be seen as a shift towards more accessible products, such as mobile phone contracts, online retail accounts, retail credit loans and short-term loans. These products are less likely to be subject to the stringent credit checking of bank accounts and credit cards. The fraudster is more likely to find that the victim of impersonation passes the credit check.

This also means criminals are able to utilise a wider range of people as potential victims. 2017 saw an increase in the number of victims of impersonation from a younger age bracket, and a decrease in those over the age of 50.

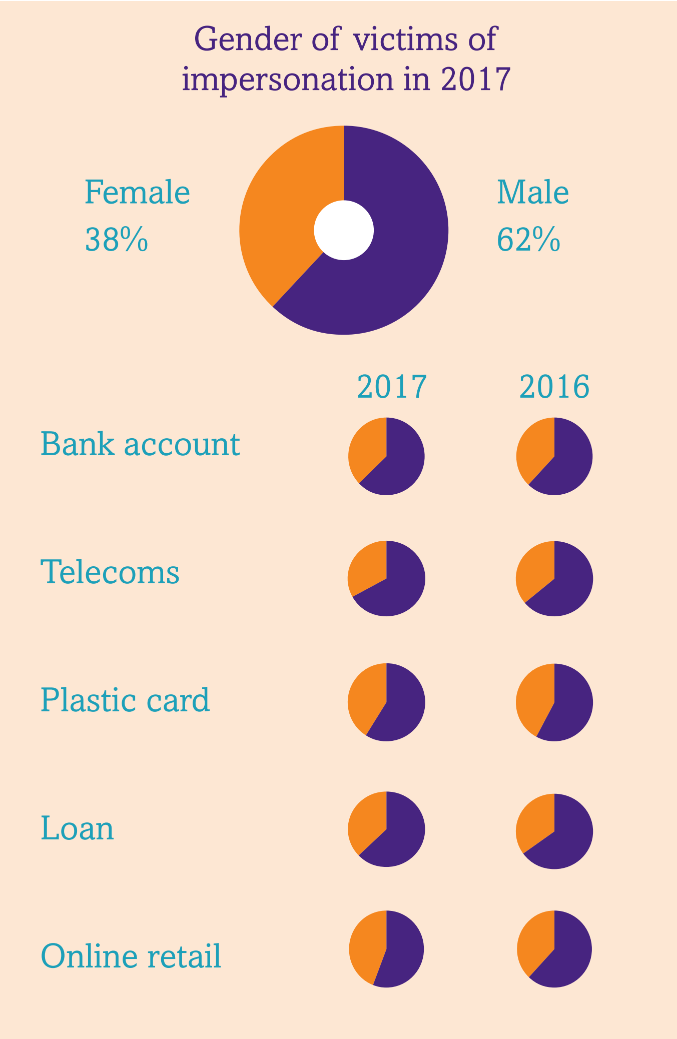
What comes first for the fraudster, the choice of product, or the choice of victim? On one hand, increased take-up of fraud prevention tools – like device recognition software within the banking industry – is likely to have hindered their ability to make as many rapid applications, resulting in the lower numbers recorded by that sector. This change is likely to have pushed identity fraudsters into targeting other sectors.

On the other hand, fraudsters are able to obtain large amounts of key information about individuals from online sources. While the number of identity frauds carried out in face-to-face environments (such as shops) increased in 2017, it remains a predominantly Internet-based offence, with 84% of identity frauds occurring through online application channels. The information obtained about a person online helps the identity fraudster pass knowledge-based authentication checks for product and services.

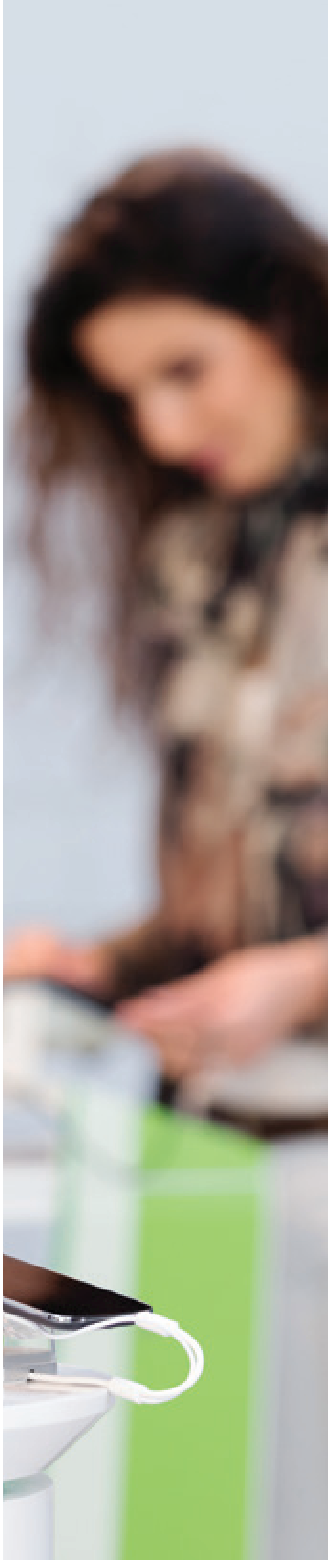
A common view is that the younger generation are more forthcoming with the information they share online, for example, on social media sites. However, our data shows that there were 48% more victims of impersonation over the age of 40 in 2017 than under 40.

But social media is not the only problem; data is compromised in a number of different ways. There have been yet more high profile data breaches in 2017, with organisations losing the details of millions of people. It is understandable that some people may feel a degree of frustration when they are given advice around taking care of their personal data – not over-sharing, keeping anti-virus and software patched and up to date – when so much personal information is lost by organisations through no fault of the individual.

But the reality is that the information lost in one breach is unlikely to be sufficient to lead to a successful impersonation. The identity fraudster will need more information to make online applications, and that may well come from the individual directly – through phishing, malware attacks,



social media, or through other forms of social engineering. Reducing the level of identity fraud must be considered a collaborative endeavour in which everyone needs to play their part.



Product type	2017	2016	
All-in-one	45	23	↑ 96%
Asset finance	970	1,053	↓ 8%
Bank account	51,544	56,084	↓ 8%
Telecoms	16,973	11,529	↑ 47%
Plastic card	58,788	65,425	↓ 10%
Insurance	4,215	248	↑ 1600%
Loan	20,082	18,736	↑ 7%
Online retail	11,729	7,883	↑ 49%
Mortgage	45	48	↓ 6%
Other	10,132	11,890	↓ 15%

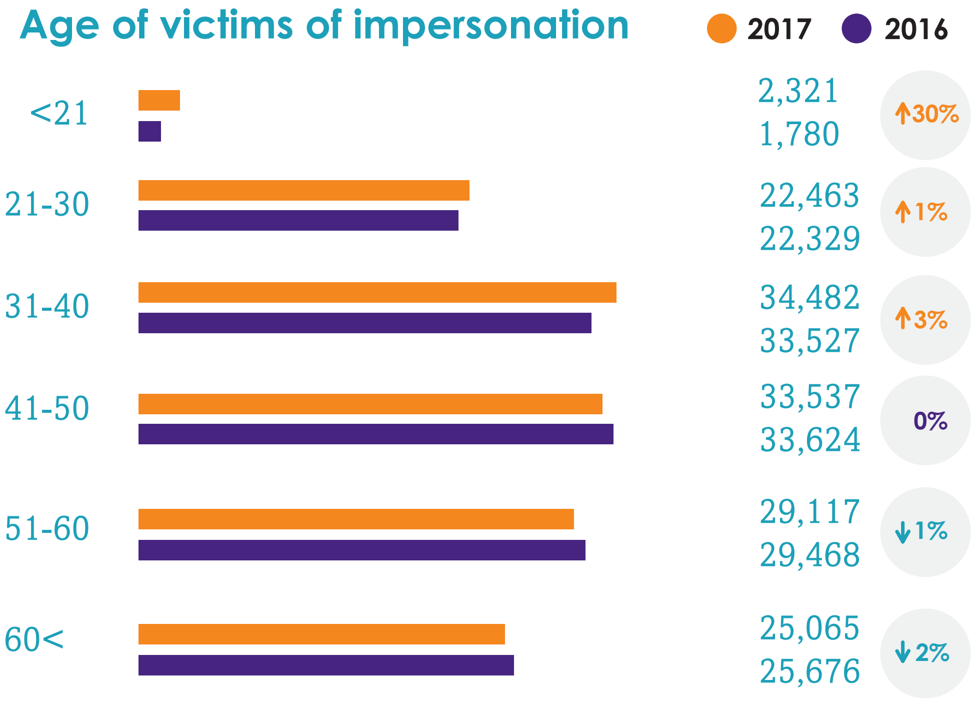
TOTAL

2017
174,523

↑1%

2016
172,919

Age of victims of impersonation



	2017	2016	
<21	2,321	1,780	↑30%
21-30	22,463	22,329	↑1%
31-40	34,482	33,527	↑3%
41-50	33,537	33,624	0%
51-60	29,117	29,468	↓1%
60<	25,065	25,676	↓2%

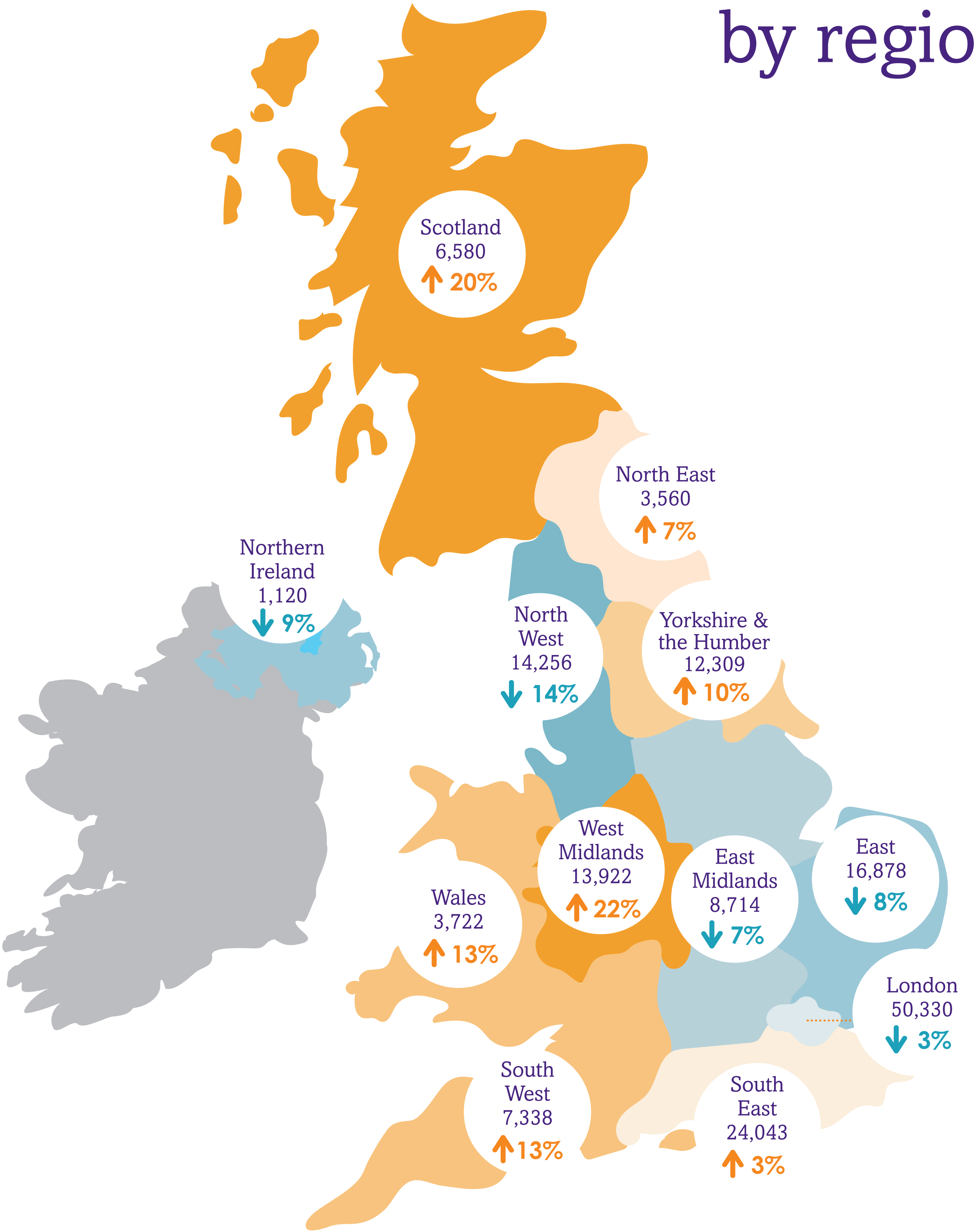
Age
14-24

2016
7,477

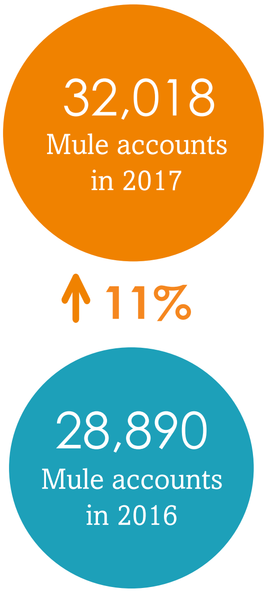
2017
8,613

↑15%

Victims of impersonation by region



The 'money mule' threat continues to grow



Cifas members identified almost 11% more bank accounts that bear the hallmarks of money mule activity in 2017 than they did in 2016 – over 32,000 cases. A 'money mule' is an individual who allows their bank account to be used to move the proceeds of crime. This shows that attempts to launder money through UK bank accounts continue to increase year-on-year.

The pertinent question is whether this increase in identified mule accounts is happening because more people are abusing their accounts in exchange for financial reward, or is it due to improvements in the ability of banks to spot them?

Most likely, it is both. As banks become more proficient at identifying mule activity and accounts are closed faster, the 'herders' (those that recruit and co-ordinate networks of mule accounts) need fast solutions to replace them.

Increased use of technology – such as device identification software – means that those operating mule networks are less able to open accounts impersonating victims in the volumes that they need. So they increasingly turn to the recruitment of others to move their illicit funds.

The unfortunate side effect of increased security around opening an account, and improved account monitoring, is that those involved in operating mule networks are driven to prey on others to provide the accounts they need. Those they recruit may now be considered as 'disposable' to organised criminals as the identities of victims of impersonation have been for the last four years.

What is particularly worrying is that criminals are increasingly preying on younger people. There was a 36% increase in the number of people aged 21-and-under that have been identified as carrying out this type of fraudulent conduct. This disturbing trend draws attention to the tactics that are being deployed by criminals and criminal gangs to recruit young people to act as mules. This recruitment could take a number of forms – in person during social engagements, or via mules recruiting other mules. But it is the role that social media plays which causes particular concern.

> A 'money mule' is an individual who allows their bank account to be used to move the proceeds of crime

Images and videos featuring young people with luxurious goods and cash are being used to draw in those who either don't recognise the illegality of what they are being asked to do, or think that the benefits outweigh the risks. In 71% of cases identified in 2017, the mule account holder was male, which shows that these messages clearly resonate well with young men.

The laundering of money by moving criminal funds through a bank account is a crime. It is down to the combined efforts of law enforcement, government, and industry and fraud prevention partners to ensure that those being approached, or those targeted by adverts on social media, recognise that what they are being asked to do is a crime.

To this end Cifas and the PSHE Association, the national body for Personal, Social, Health and Economic education in schools, have recently released fraud education

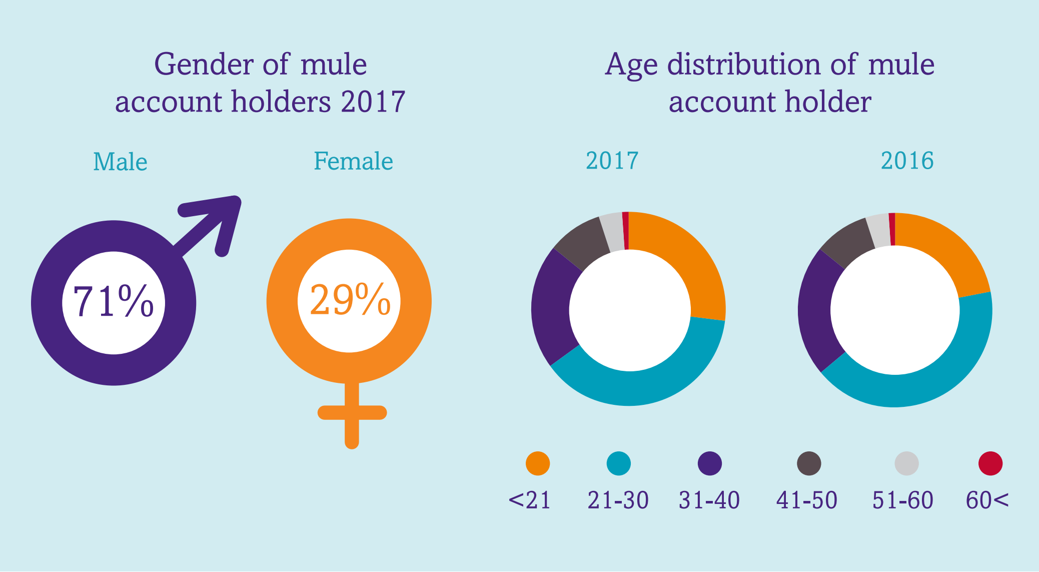
Continued on page 8

Continued from page 7

lesson plans for schools so that those attracted to this activity are made aware of the repercussions.

The number of these cases being identified and reported by banks must serve as a stark warning to those who are tempted by the easy money being offered by these criminal gangs. Nothing is free and the chances of getting caught are increasing all the time.

> Images and videos of luxury goods and cash draw in those who don't know it's illegal, or don't care



MAKE £250 PER WEEK
No experience necessary*
Easy job. Big cash payouts.
*Disclaimer: your details may be shared with fraud prevention agencies, limiting your ability to open bank accounts, get a phone contract or even a job. You may also be prosecuted and imprisoned for up to 14 years.

Older age groups are being targeted through social engineering for takeovers

Product type	2017	2016	
All-in-one	522	392	↑ 33%
Asset finance	6	6	0%
Bank account	5,490	6,730	↓ 18%
Telecoms	9,342	9,094	↑ 3%
Plastic card	7,365	5,262	↑ 40%
Loan	309	44	↑ 602%
Online retail	1,002	949	↑ 6%
Mortgage	9	22	↓ 59%
Other	25	25	0%

2017 24,070

↑ 7% TOTAL

2016 22,524

There was a 7% increase in the number of fraudsters hijacking the accounts or services of an innocent victim in 2017. Takeover of plastic card accounts increased the most in real terms, however telecoms accounts (mostly mobile phones) remained the most frequent.

Facility takeover frauds and identity frauds both involve the fraudster trying to assert an identity that is not their own, and therefore have the same root cause – the availability of personal information.

As with identity fraud, this information can be compromised in a number of different ways – from data breaches to other online methods, as well as information that is socially engineered from the individual themselves.

While there are similarities between facility takeover frauds and identity frauds, there are also some key differences. In contrast to identity fraud, there has been an increase in the targeting of older age groups for facility takeover fraud, while the number of younger victims has decreased.

What is particularly concerning is that over-60s are now the most commonly targeted age group. Clearly not everyone who is over 60 can be described as vulnerable, but age is a factor regularly associated with increased susceptibility to falling victim to scams and social engineering.

It's thought that older age groups are more likely to trust any contact they receive, such as those who ring them claiming to be from their bank, card issuer or another known service provider. Most commonly these contacts will ask the individual to confirm their details under the guise of a 'security check', i.e. a bogus caller stating "I just need to confirm that I'm talking to the right person…"

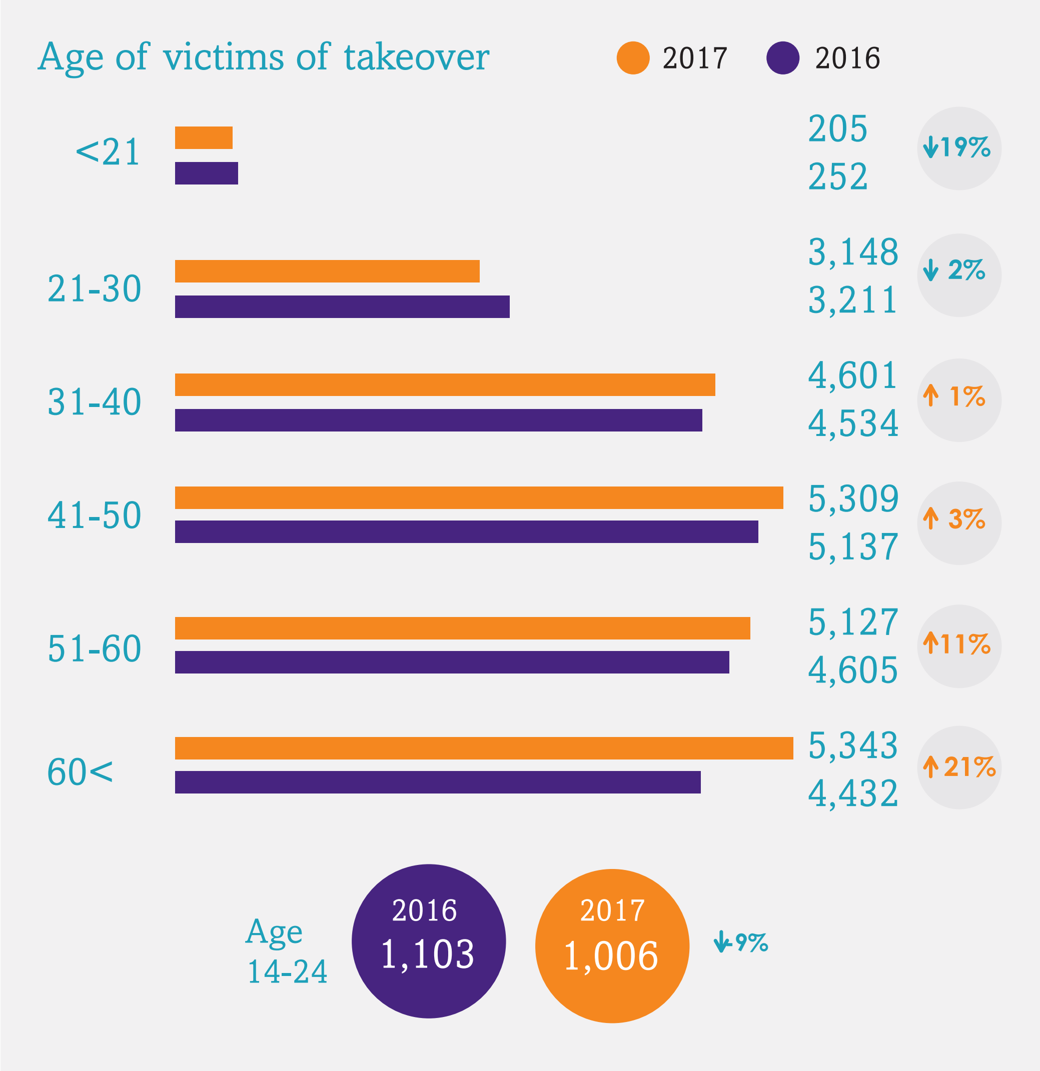
Continued on page 10

Continued from page 9

Another area where facility takeover differs from identity fraud is the channel through which the takeover occurs – overall, there has been a shift towards more ‘in person’ facility takeovers.

As well as an increase in face-to-face takeovers, there’s also been a rise in those initiated on the phone before the fraudster goes into a branch or store to complete the operation (so called ‘combination’ takeovers).

Overall, there were fewer takeovers carried out entirely over the phone, while the proportion carried out online remained on a par with 2016.



Interestingly, there was a lack of consistency across the most commonly targeted products. A higher number of bank accounts were taken over online, but takeovers relating to plastic cards through online methods decreased. Mobile phone contract takeovers occurred mostly in store, with fewer carried out over the phone.

This clearly indicates that those seeking to take over accounts and other facilities will target the route that will give them the highest chances of success using the information they have available, while taking into account the strength of the security in place.

An organisation’s defences are only as strong as the weakest link.

Fraud by product

Bank accounts: fraud down, mule accounts up

Fraud type	2017	2016	
Application fraud	7,203	7,641	↓ 6%
Facility takeover fraud	5,490	6,730	↓ 18%
Identity fraud	51,544	56,084	↓ 8%
Misuse of facility	42,803	37,732	↑ 13%

2017 107,040

↓1% TOTAL

2016 108,107

The number of frauds affecting bank accounts decreased slightly in 2017, with decreases in all fraud types apart from misuse of facility frauds.

These findings strongly suggest that preventative measures being employed by banks are helping to reduce fraud. The fraud types which decreased are those where the bank will be looking for anomalies that indicate the individual is misrepresenting who they are or their circumstances. The use of technology such as device recognition software, voice recognition and predictive analytics can reduce fraudsters' opportunities to commit identity fraud, and help prevent the takeover of accounts.

Of concern, however, is that fraud conducted by the genuine account holder has increased. Most commonly, this is where the account holder has acted as a 'money mule', laundering the proceeds of crime. This accounts for almost 85% of account misuse fraud and continues to present a substantial problem.

The next most common form of account abuse was multiple encashment fraud, where the customer knowingly withdraws in excess of the funds deposited or their overdraft limit, in the full knowledge that the bank will not honour the withdrawal. This accounted for 8% of cases in 2017, down slightly from 10% in 2016.

An interesting increase, although still comparatively low in number, was the number of cases of abuse of contactless cards. This has increased from 528 cases in 2016 to 1,395 in 2017. As contactless cards become more frequently used, and contactless payments are possible in more locations, the potential for this type of fraud to increase further is increasingly likely.

While the reductions seen in the number of identity frauds and facility takeover frauds is cause for optimism, it should not detract from the fact that the absolute number of these identity-related frauds is still too high – over 57,000 cases recorded. While it appears that in 2017 some identity fraudsters began to target other products, some were still able to overcome the obstacles to opening bank accounts in someone else's name. The use of compromised personal data is considered the principle enabler in these frauds.

Although the total number of bank account takeovers decreased in 2017, the number that took place through the online channel actually increased by 5% and now make up almost half of all account takeovers. Alongside this, the age of victims of account takeover continued to rise. Over 33% of male victims of takeover and 28% of female victims were over 60 years of age (compared with 27% and 25% in 2016).

One of the tactics used by fraudsters in order to bypass online account security is to ring the

Continued on page 12

Continued from page 11

victims posing as a member of bank staff and ask for the relevant security information in order to 'verify' who they are talking to. The fraudster can then use this to log in to their victim's account.

As the number of older people who bank online increases, so the number of potential victims of this scam increases – particularly when the victims may not think to question the legitimacy of the caller. Ensuring that those adopting online services are aware of the potential risks and, most importantly, what they will never be asked to disclose by bank staff, is therefore vital to reduce these frauds.

Plastic cards: takeovers up by 40%

The number of frauds targeting plastic cards, predominantly credit cards, decreased by nearly 9% in 2017 compared with 2016. All types of fraud reduced, apart from facility takeover fraud which increased by 40%.

Takeovers of plastic card accounts occurred through online and telephone channels in similar numbers, accounting for 36% and 35% of cases respectively.
45% of cases involved an unauthorised change of address on the account, which is up from 36% of cases in 2016.

The need to intercept cards in the post may partially explain the shift away from identity fraud and towards facility takeover fraud. For an application for a new card account to be successful, the fraudster will need to use the correct current address of the victim of impersonation – which is then where the cards are mailed to.

There are a number of methods that a fraudster might use to intercept the mail, such as accessing communal mailboxes in blocks of flats, but there is always a chance that the genuine account holder will take delivery of the card. Changing the address on an existing account means that the facility hijacker can have new cards dispatched to an address which they control, increasing their chance of a successful take over.

As with bank accounts, it is also likely that investment in enhanced fraud prevention tools is contributing to the lower number of identity frauds recorded in 2017. This reduction is partially counterbalanced by the increase in facility takeover frauds, suggesting that, not only are fraudsters prepared to target other types of product to achieve their objectives, they are also prepared to modify their approach against the same product.

In common with victims of bank account takeover, those that had their card account taken over were also in the older age groups, with the over-60s the most commonly targeted group when the victim is male (29% of male victims), and 51-60

Fraud type	2017	2016	
Application fraud	1,385	1,726	↓ 20%
Facility takeover fraud	7,365	5,262	↑ 40%
Identity fraud	58,788	65,425	↓ 10%
Misuse of facility	4,209	6.058	↓ 31%

2017 71,747

↓ 9% TOTAL

2016 78,471

year olds most commonly targeted when the victim was female (28%).

There were 31% fewer misuse of facility frauds affecting plastic card accounts in 2017 than in 2016. The majority of the remainder were made up of those trying to set up regular payment instructions from accounts where they do not have the authorisations to do so – trying to get someone else to pay their bill (40% of cases), and those trying pay their bill with cheques they know will not be honoured (20% of cases).

Telecoms: big rise in impersonations to get phones

Fraud type	2017	2016	
Application fraud	586	782	↓ 25%
Facility takeover fraud	9,342	9.094	↑ 3%
Identity fraud	16,973	11,529	↑ 47%
Misuse of facility	4,608	21,919	↓ 79%

2017
31,509

↓ 27%
TOTAL

2016
43,324

The number of cases recorded by organisations in the telecoms sector decreased by over a quarter in 2017. This shouldn't, though, be taken as an indication that telecoms companies are no longer targets for those that seek to commit fraud.

The reduction can be attributed to fewer cases being recorded of misuse of facility fraud where the individual obtained a handset on a contract without ever intending to honour the contract. The reduction, however, is down to the telecoms sector embedding new recording practices rather than a reduction in attempts of this nature. It can be expected that in 2018 we will see the recording of these cases increase again.

Substantial increases were identified in cases involving the abuse of a genuine person's identity – mostly in applications for new contracts in the name of an innocent victim, but also in the number of instances of an existing customer's account being taken over.

The use of the telephone channel to perpetrate identity fraud remained the most common method, accounting for 46% of cases. But in 2017 there was an increase in the proportion of identity frauds which occurred through the abuse of click and collect services. This is where the impersonation takes place online, but the fraudster presents a high quality debit card in store to complete the fraud and take possession of the handset. This tactic allows the fraudster to effectively use the genuine current address of the victim of impersonation, but not have to be concerned with intercepting deliveries to that address. The use of high quality fake bank cards also highlights the level of organisation involved in these frauds.

There are two main reasons for taking over the existing mobile phone account of someone else. The first is to take advantage of the victim's upgrade; the second is to add another phone number to the account. While still the most common type of account takeover, in 2017 there was a decrease in the number of cases involving an unauthorised upgrade (47% of cases, compared with 56% in 2016). Conversely, there was an increase in the cases involving the unauthorised addition of a facility (32% of cases, up from 23% in 2016). Smaller in number but still notable were those instances where the fraudster took over a mobile phone account in order to intercept calls and text messages (439 cases). These are concerning as it is likely that the fraudster is trying to intercept

Continued on page 14

Continued from page 13

messages from the victim's bank, card issuer or other service provider in order to bypass the security on those accounts and take them over.

Victims of identity fraud, where the product applied for was a telecoms account, are younger than victims of identity fraud more generally. In 2017, this continued to be the case, with 30% of telecoms victims of impersonation 30 years of age or younger, compared with all victims of impersonation, where 17% were 30 years old or younger.

A mobile phone contract is a common product for a young person to apply for, which means that for an identity fraudster who wants mobile phones, those under the age of 30 make more viable victims. This emphasises that no one is immune from being a victim of impersonation – instead, a fraudster is merely more likely to target the product where they have the greatest chance of success.

Insurance: ghost brokers increasingly using real identities

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

Fraud type	2017	2016	
Application fraud	5,462	7,126	↓ 23%
False insurance claims	541	494	↑ 10%
Identity fraud	4,215	248	↑ 1600%
Misuse of facility	151	55	↑ 175%

2017
10,369

↑ 31%
TOTAL

2016
7,923

In 2017, the number of cases recorded by insurers to the National Fraud Database rose by 31%. This was mainly due to a substantial increase in identity fraud cases being recorded. We highlighted this emerging trend in last year's *Fraudscape* report and it continued throughout 2017.

These cases of identity fraud are often related to 'ghost brokers', the term given to individuals fraudulently acting as an intermediary for people seeking motor insurance. A ghost broker submits applications using a victim's personal information in order to increase the chances of the insurer offering a quote for policy.

Frequently, the ghost broker also supplies false or compromised payment details. This results in the policy being voided, but not before the policy certificate has been emailed. This is then altered and passed to the 'client'. As the communication occurs by email, the victim of impersonation will likely be none the wiser.

Another motivation for identity fraud is purely to get a vehicle insured so it will not be stopped by the police for being uninsured. For this, the perpetrator is just looking for the cheapest policy they can get.

Although the number of cases fell in 2017, application fraud remained the most commonly identified type of fraudulent conduct affecting insurers. These frauds predominantly related to individuals trying to artificially lower their premium.

45% of cases involved submitting a false address in order to make it appear that the vehicle will be kept at a safer location, and 24% involved falsely claiming a better no claims discount. 14% involved the fronting of an insurance policy, where the individual applying would not be the main driver of the vehicle, as the real primary driver would be seen as higher risk by the insurer and charged more.

The number of misuse of facility frauds identified by insurers almost tripled, albeit from a low base. The abuse of the Direct Debit Guarantee scheme accounted for more than 80% of these cases. This is where individuals pay for their insurance premiums for a year on direct debit, but at the end of the period attempt to reclaim those payments, claiming they never authorised the payment in the first place. Under the scheme, an individual is entitled to have their money repaid if the direct debit was not correctly set up. They still owe the insurer for a year's worth of insurance cover, but those making a fraudulent claim under the scheme are unlikely to pay it.

The number of false insurance claims recorded to the National Fraud Database also increased. The types of false claims remained in line with those recorded in 2016, there were just more of them. The three most common types were claiming for an event that did not take place (26% of cases), inflating the claim (22%), and staging an event (20%). The staging of an event is always of concern as these can involve 'crash for cash' road traffic accidents, which put road users at risk.

Online retail: identity fraudsters target goods online

The number of fraud cases recorded by credit-granting online retailers decreased by 12% in 2017 compared with 2016. This decrease was entirely due to a lower number of misuse of facility frauds, as all other types of fraud increased.

Fraud type	2017	2016	
Application fraud	119	94	↑ 27%
Facility takeover fraud	1,002	949	↑ 6%
Identity fraud	11,729	7,883	↑ 49%
Misuse of facility	20,108	28,608	↓ 30%

2017
32,958

↓12%
TOTAL

2016
37,534

The largest increase was seen in identity fraud, which rose by 49%. Similar to the increases seen in identity fraud to obtain mobile phone accounts, this will be a result of identity fraudsters considering a false application to an online retailer as having a higher probability of success compared with the likes of a credit card. Their objective will likely be to obtain goods that they can sell on.

Another similarity with telecoms is that the fraudster can bypass some of the issues that come with using the genuine current address of their victim of impersonation. If the fraudster is able to give a different delivery address, they can have the goods delivered to an address of their choosing and not risk the victim receiving the goods.

Continued on page 16

Continued from page 15

In some instances though, the fraudster will deliberately use the victim to take delivery of the goods. People are likely to accept delivery of (and sign for) a package that arrives addressed to them. The fraudster will then visit the victim posing as a courier, saying the package was delivered in error and they need to take it back.

The lower number of misuse of facility cases is down to a reduction in instances where the individual opened an account and purchased goods on credit without intending to pay for them – fraudulent evasion of payment. The reduction in this type of fraud is perhaps unsurprising, as where this conduct is identified and shared for fraud prevention purposes, the individual will find it difficult to get other accounts and repeat the act.

Chasing ghosts: organised crime groups involved in fraud

By Bina Bhardwa and Tiggey May
Institute for Criminal Policy Research, Birkbeck School of Law, University of London

The Institute for Criminal Policy Research recently completed a study, funded by Dawes Trust, on organised crime groups (OCGs) involved in fraud, which was published by Palgrave Macmillan earlier this year. The study examined the routes into fraud and organisational structures used by 31 organised criminals, alongside the investigative challenges encountered by 45 enforcement professionals.

Routes into organised fraud

The routes into organised crime and fraud are diverse and complex. Our research found two broad categories of offender:

- Those who are recruited and unintentionally drawn in by OCGs;
- Those who made an intentional and conscious choice to become involved in criminality.

The majority of our interviewees made a conscious choice to engage in organised fraud, and were predominantly driven by financial gain. Some committed fraud by exploiting loopholes within legitimate occupations; others committed fraud by building it into business plans and actively seeking fraud as a way of making money; others were either involved politically or had political connections and used these positions and networks to facilitate their route into organised economic crime.

For the remainder of our interviewees, their route into fraud and organised crime was through either ‘targeted’ or ‘serendipitous’ recruitment by existing OCGs. Some interviewees were recruited into organised crime by strangers, others by friends, acquaintances, or work colleagues. Four of our offender interviewees were targeted by organised criminals, and recruited to fulfil a specific function.

Once recruited, their level of awareness regarding their criminal involvement ranged from willingly complicit and active, to unknowing and duped. Three interviewees were purposefully targeted and recruited as professional enablers. The professional enablers were invaluable to their OCGs; they opened doors that would otherwise be closed to such groups to facilitate criminal activity. Solicitors, accountants, financial advisers, bank managers, and mortgage brokers all assisted the criminal activity of our interviewees, in addition to bank clerks, staff at retail outlets, postal workers, firemen, doormen, and casino staff.

A number of interviewees maintained that their route into fraud and organised crime was the result of taking up what they believed was a legitimate opportunity. Once recruited, however, they made a deliberate decision to exploit the criminal opportunities to which they were introduced. All but one of our interviewees was involved in organised economic fraud for financial gain and greed. Overlapping criminal, social, and business connections provided the requisite conditions to facilitate offender routes into fraud and organised crime.

The nature and structure of organised crime groups involved in fraud

The police officers we interviewed suggested that OCGs involved in fraud take on multiple organisational structures; this was reflected in our analysis.

Some police interviewees described the profile of offenders as older, from an educated or professional background and with little or no prior criminal involvement. This profile was

Continued on page 18

Continued from page 17

associated with what they viewed as the classic OCG structure: hierarchical and pyramidical in form.

Other police officers argued that a slightly different structure had emerged, one which was characterised by loose, slightly more dynamic networks of offenders who work together in a synchronised and complementary way to commit fraud.

Another OCG structure we found was the global network structure. This followed a similar business model to the classic structure but operated at a European and/or international level. The final derivative of the classic OCG structure was characterised by a hierarchical top tier with fluid or chaotic lower tiers.

In many respects, the classic, hierarchical structure is still the most dominant form of fraud-related OCGs, but it has adapted to account for the geographical spread of OCG operations across borders and for different types of organised fraud.

Our research found that OCGs involved in fraud are diverse in nature, rather than being either a hierarchical structure or loose network.

Cops and 21st century robbers

Our study examined the policing and sentencing of organised fraud, mainly from the perspective of policing professionals. We found that fraud investigations involving OCGs tended to be relatively complex and were reported to take many months or even years to reach a conclusion.

One recurring commonality on whether to investigate or prioritise a case was the vulnerability of the victim. The importance of containing and focusing investigations was viewed as significant. Deciding on an investigation's parameters often created the best possible chance of achieving a successful outcome for the victim(s).

Issues highlighted by our enforcement

interviewees as everyday difficulties were: the complexity of investigations, in particular cross-border or jurisdiction cases; the threat posed by new technologies; resource issues; and the problems associated with the low priority fraud is often afforded. The speed with which organised criminals adapt their business practices leaves the police with very little choice but to react to criminal activity rather than proactively try to prevent it. As one officer stated: “We [the police] are chasing Formula 1 cars with tricycles.”

Interviewees reported confiscation figures which ranged from a token £1 payment to estimates between £100 and £300 million in assets. Five interviewees said that as soon as the police started their investigation, their assets had been frozen.

No interviewee believed that enforcement agencies (including Police Forces, NCA, SFO, and HMRC) were effective at tackling OCGs involved in fraud. Nearly all expressed dissatisfaction with the trial by jury process and held the view that juries were unable to understand the complexities involved in fraud cases, were bored by the evidence, and often ‘switched off’ due to the length of the trial.

Whilst none of our interviewees disclosed any criminal activity whilst in prison, a surprising number were either sharing a cell with one of their co-defendants or were in the same prison establishment.

And finally…

Fraud, along with many other crimes, has, over the last 20 years, adapted to the increasingly online world that most of us now inhabit. With more of our lives being conducted online, the greater the distance between offender and victim can be (for example, cyber-bullying, sexual exploitation, fraud, theft, stalking and harassment). In short, offenders have the ability to commit their crime of choice without being seen or heard.

Nearly all of the frauds discussed in our study were assisted by a professional enabler and were able to be committed without the offender coming into contact with the victim. There is a growing importance in generating a more textured understanding of enablers; in particular, their routes in and motivation to assist OCGs. Without this knowledge, it is likely that their significance to an OCG will remain at an abstract level, as will the enforcement and regulatory response.

There is also a need for enforcement professionals and their partner agencies (corporate, private and public) to consolidate, share and act upon information and data. Together they can help to tackle the misperception that organised fraud is a victimless crime.

Tiggey May and Bina Bhardwa’s book ‘*Organised Crime Groups Involved in Fraud*’ is available in ebook and hardcover from Palgrave Macmillan.

Helping Parliament tackle the growing problem of fraud and scams

By Conor Burns

MP for Bournemouth West, Parliamentary Private Secretary to the Foreign Secretary, and Chair of the All-Party Parliamentary Group on Financial Crime and Scamming

Fraud and scams are growing crimes. The Office of National Statistics England and Wales Crime Figures showed that 662,519 police-recorded fraud offences took place between October 2016 and September 2017, and in their Crime Survey it's recorded that there were 3.2 million estimated incidents of fraud in the same period.

Fraud is the twenty-first century volume crime and the issue is not going to go away. With more and more people sharing data, transacting, setting up businesses, dating, and chatting online, this trend is only going to continue.

That's why, in 2017, the All-Party Parliamentary Group (APPG) on Financial Crime and Scamming was set up. This group acts as a voice in Parliament on scams, fraud and wider financial crime. The APPG will act as a channel to educate and raise awareness of fraud and scams to MPs and Peers. It will also act as a channel to challenge and work with government, law enforcement and industry to ensure our response to financial crime is joined up.

I am delighted to be chairing such an important cross-party group. The numbers of frauds and scams are on the rise and can affect any single one of us. Numerous constituents have contacted me with their harrowing cases of being victims of fraud and scams.

The APPG is supported by a number of bodies – Age UK, Trading Standards, Which?, Bournemouth University, and Cifas to name just a few. This, I think, highlights that fraud, scams and financial crime is a huge issue that cuts across different sectors and generations.

This year the APPG on Financial Crime and Scamming will hold two inquiries: one on young victims of financial crime, and the other on older and vulnerable victims of fraud and scams. Both of these inquires will seek to look at why both issues exist, what best practice is already in place to tackle the issues and how government, industry and law enforcement's response to these matters could be improved.

Visit the APPG website at www.appgfinancialcrime.org for more information on the group.

Consumer questions

I've started receiving mail in my name about accounts I didn't open. What should I do to resolve this?

It could be that you have been a victim of identify fraud – but don't panic! If you have been a victim, you will not be liable for debts that have been built up in your name. The first thing you should do is contact the organisation concerned and explain what's happened. Also, get a copy of your credit report: this will allow you to see if any other accounts have been opened in your name that you don't recognise. Most credit reference agencies offer a free service to victims of identity fraud to help resolve the problem.

You should also report it to Action Fraud on 0300 123 2040 or on their website, where you can also find more information about protecting yourself from fraud. Additionally, you can contact Victim Support for free, and confidential advice and support. Victim Support is the independent charity for victims and witnesses of crime in England and Wales. Find out more about how they can help you at their website.

You could also consider getting Cifas' Protective Registration as an additional way to reduce your risk of becoming a victim again in the future. Find out more on our website.

I'm concerned about the amount of identity fraud going on and want to make sure I'm fully protected. What should I do?

You're right to be concerned, as the amount of identity fraud people are experiencing continues to increase. Your identity is a valuable commodity and it should be treated as such; but it isn't just your name, address and date of birth that is valuable to a fraudster – they also want your contact information, passwords, or information that might help them guess the answers to security questions.

So, be careful what you share on social media and check your privacy settings. Be wary of any unexpected calls, emails and texts that claim to come from your bank or other service provider asking you to confirm your personal details.

Use strong passwords and make sure that your anti-virus software is up to date. Download software updates to your devices. Avoid using public Wi-Fi for banking or online shopping. Also, don't forget to shred sensitive documents when they are no longer required and be wary of unsolicited phone calls. If in doubt, phone the organisation back on a number you trust and from a different line.

Continued on page 22

Continued from page 21

My teenage son has been buying a lot of new trainers and I don't know where he got the money. I'm worried he might be a money mule.

First off, ask your child how they have earned enough money to afford such items. You might want to supervise their bank account in order to keep a close eye on financial transactions and make sure all of them are accounted for.

If your child is acting as a money mule, it's crucial that they realise what they have got involved in. Explain that acting as a money mule is not only a criminal offence, it could also affect their ability to gain credit. In the short term it could affect simple things like getting a mobile phone contract or opening a bank account; in the long term it could stop them getting a mortgage.

If there is another explanation for the trainers, it's still worth educating your child on what to look out for, so they are not lured into becoming a money mule by offers of 'easy money'. Advise them to never to give their bank account details to anyone unless they trust them, and to be cautious of any unsolicited emails or approaches over social media promising 'quick cash' opportunities. If an offer sounds too good to be true, it probably is.

I've been contacted about what looks like a really lucrative investment opportunity, but I'm concerned it might be a scam. How can I tell?

Scams can be incredibly convincing. Whether you have a 'gut feeling' that something is wrong or not, you should always approach these opportunities with caution. Keep it simple, don't allow yourself to be rushed into making a decision, and check the Financial Conduct Authority's ScamSmart warning list to see if the organisation you're thinking of dealing with is listed, or if they are regulated by the FCA. Ultimately, if you have doubts, don't do it. Take five minutes to stop and think.

Further guidance can be found at www.takefive-stopfraud.org.uk.

The fraud landscape is increasingly complex – we need to step back and look at the bigger picture together

By Sandra Peaston
Assistant Director, Insight, Cifas

By the end of 2017, the network of organisations sharing fraud data through Cifas had grown to 412 organisations, widening the protective net that is provided by approaching fraud prevention from a non-competitive, reciprocal perspective.

This approach helped to prevent almost £1.3bn being lost to fraud over the course of the year. The adoption of increasingly sophisticated, data-driven fraud prevention techniques is also increasing the success rate in identifying fraudulent attempts earlier and faster – protecting more organisations and individuals from fraud. However, making things more difficult for those perpetrating fraud is unlikely to stop them; rather it is likely to drive them to commit other types of fraud and target other victims.

It is clear from the findings from this year's *Fraudscape* that the fraud threat facing the UK continues to evolve. We have seen a greater targeting of younger people in some areas but older people in others.

Cifas, on behalf of the Home Office-led Joint Fraud Taskforce has produced fraud education lesson plans in association with the PSHE Association. It is hoped that these lessons will be adopted as part of the national curriculum in order to equip those entering adulthood with the knowledge and understanding they need to successfully identify when someone is trying to fraudulently take advantage of them – be that inducing them to become money mules or defraud them more directly.

Fraudscape also makes it clear that the messages of the Take Five campaign continue to be highly relevant, particularly for those groups who are starting to interact with their service providers more remotely. People are being encouraged to adopt more online services, which then puts them at risk in new and unfamiliar ways. Someone may be suspicious of an individual coming to their front door and telling them that their roof needs fixing, but not recognise that someone purporting to be calling from their bank and asking them to confirm their online banking user name and password isn't who they say they are.

These two areas, more than any other, reinforce the interconnectedness of fraud and fraud prevention efforts. When an older person is deceived into making a payment by a fraudster, that money is likely to be paid into a mule account, where the account holder is a young person who in their naivety hasn't fully appreciated that they are committing a crime.

The establishment of the All-Party Parliamentary Group on Fraud and Scamming, and its inquiries into fraud affecting young people and, later this year, fraud and the elderly, could not be timelier. Cifas is pleased to be providing the secretariat to this group. Fraud prevention efforts may also mean that those wanting to defraud organisations increasingly need the active involvement of those within the organisations they are targeting. The work being undertaken by Tiggey May and Bina Bhardwa on behalf of crime-fighting charity the Dawes Trust has shed light on the ways in which people are drawn into working with organised groups perpetrating fraud and the role that professional enablers play in facilitating this type of crime.

Those facilitating fraud from the inside can be employed at any level,

Continued on page 24

Continued from page 23

so it is increasingly important that an individual who has been dismissed for fraudulent conduct, such as facilitating fraudulent applications or compromising personal data, are not allowed to move onto the next organisation to do the same again with impunity. Sharing this information through Cifas' Internal Fraud Database is a vital step in preventing criminal groups getting a foothold in your organisation.

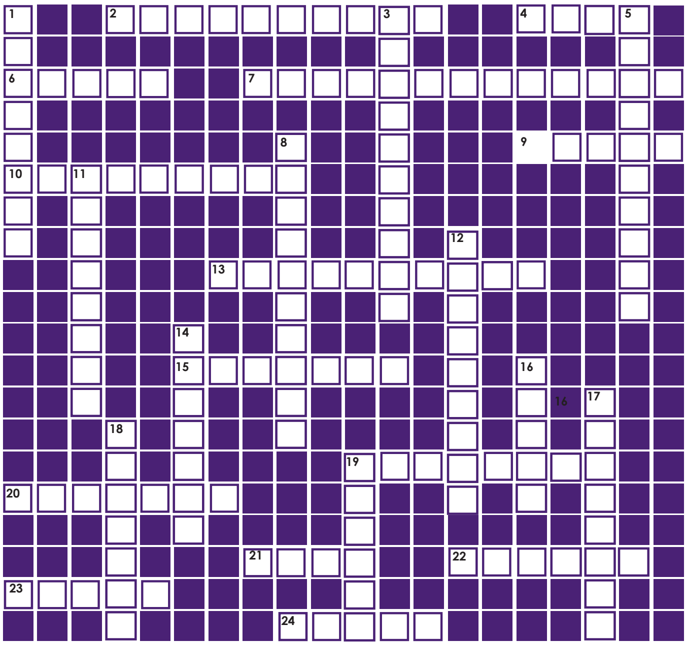
As a final point, our data shows that the number of impersonations is still increasing. The information a fraudster requires to make an application in another person's name or take over an account is too widely available. Data breaches continue to be too common and fraudsters are increasingly successful at socially engineering both customers and call centre staff to gain further personal data that can be used to evade knowledge-based authentication.

Despite the good work of our fraud prevention partners to raise awareness of the dangers of social engineering, malware and oversharing of personal information, this alone is not sufficient to curtail the problem.

As a fraud prevention community we need to give further consideration to the way in which we identify people online. Consumers are unlikely to want to go back to a time when they couldn't apply remotely for products and services – alternatives to knowledge-based authentication are more and more urgently required.

There are organisations through which individuals can assert their identity (including the Government Verify scheme) and in some countries digital signatures are being used. Finding effective solutions will require the collaboration and expertise of all players – from industry to government to consumers themselves. With collaboration and co-operation at the heart of Cifas, we will continue to lead the way in the fight against fraud and financial crime.

Crossword



Across

2 Facts (10)
4 Regulating the use of personal data across Europe (4)
6 Illegal activities (5)
7 Acting as another individual (13)
9 Relating to the culture of computers (5)
10 Providing protection against a possible eventuality (9)
13 Observing and checking progress (10)
15 A report of an event or experience (7)
19 A structured set of information (8)
20 Keep from happening (7)
21 Unlikely to be harmed (4)
22 A person who has been duped (6)
23 Wrongful or criminal deception (5)
24 Discourage (5)

Down

1 The state of being free from danger (8)
3 Dishonest conduct typically involving bribery (10)
5 Buffer against possible threats (10)
8 Machinery developed from scientific knowledge (10)
11 A means of solving a problem (8)
12 Relating to money (9)
14 Gaining unauthorised access to a computer (7)
16 Leaders in fraud protection (5)
17 Who or what a person or thing is (8)
18 A person or company that saves someone (7)
19 Discover or identify (6)

Answers on page 27

Fraud by product breakdown

All-in-one

- In 2017 there was an increase in the number of facility takeover frauds affecting all-in-one products (as there was in 2016 compared to 2015). This has resulted in an overall increase in the number of frauds against all-in-one accounts identified. These facility takeover frauds predominately relate to unauthorised electronic payment instructions;

- The number of identity frauds increased slightly in 2017;

- The numbers constituting these totals are low in comparison to other products, which therefore means that small changes in numbers lead to a more substantial percentage change.

CASE TYPE

	Application fraud
2016	1
2017	3
change	200%

	Facility takeover fraud
2016	392
2017	522
change	33%

	Identity fraud
2016	23
2017	45
change	96%

	Misuse of facility
2016	13
2017	11
change	-15%

TOTAL

2016	2017	change
429	581	35%

Asset finance

- The total number of frauds against asset finance products increased by 27% in 2017 compared with the previous year;

- The largest increase was in the number of application fraud cases. This increase was primarily due to a higher number of instances of addresses with adverse credit information not being disclosed by the applicant when they were required to be;

- Misuse of facility frauds also increased, with the majority in relation to evasion of payment;

- Asset conversion frauds increased in 2017 compared with 2016, as they did in 2016 compared with 2015. These cases relate to the unauthorised selling or disposal of a finance company asset.

CASE TYPE

	Asset conversion
2016	360
2017	520
change	44%

	Application fraud
2016	8,050
2017	10,791
change	34%

	Facility takeover fraud
2016	6
2017	6
change	0%

	Identity fraud
2016	1,053
2017	970
change	-8%

	Misuse of facility
2016	1,391
2017	1,487
change	7%

TOTAL

2016	2017	change
10,860	13,774	27%

Bank account

- Although identity frauds to obtain bank accounts decreased by 8% in 2017, they still accounted for 48% of the frauds against bank accounts. Most commonly, these identity frauds involved the impersonation of an individual using their genuine current address;

- Misuse of facility cases saw a 13% increase in 2017. Three quarters of these are highly likely to be linked to 'money mule' activity;

- Bank accounts were the most targeted product in 2017.

CASE TYPE

	Application fraud
2016	7,641
2017	7,203
change	-6%

	Facility takeover fraud
2016	6,730
2017	5,490
change	-18%

	Identity fraud
2016	56,084
2017	51,544
change	-8%

	Misuse of facility
2016	37,732
2017	42,803
change	13%

TOTAL

2016	2017	change
108,187	107,040	-1%

Telecoms

- The total number of frauds reported against telecoms products decreased by 27% in comparison to 2016. This was due to a dramatic decrease in the number of misuse of facility cases involving evasion of payment that were reported by the sector;

- The most notable increase was the number, by 47%, of identity fraud cases. A large proportion of these were in relation to the impersonation of an individual at their current address.

CASE TYPE

	Application fraud
2016	782
2017	586
change	-25%

	False insurance claim
2016	1
2017	0
change	-100%

	Facility takeover fraud
2016	9,094
2017	9,342
change	3%

	Identity fraud
2016	11,529
2017	16,973
change	47%

	Misuse of facility
2016	21,919
2017	4,608
change	-79%

TOTAL

2016	2017	change
43,325	31,590	-27%

Fraud by product breakdown

Plastic cards

- The number of frauds relating to plastic card products decreased by 9% from 2016 to 2017;
- Facility takeover fraud saw a 40% increase in 2017. A large proportion of these were in relation to unauthorised electronic payment instructions and unauthorised address changes;
- Although the number decreased by 10% in 2017, plastic cards remain the products most commonly targeted by identity fraudsters.

CASE TYPE

	Application fraud
2016	1,726
2017	1,385
change	-20%

	Facility takeover fraud
2016	5,262
2017	7,365
change	40%

	Identity fraud
2016	65,425
2017	58,788
change	-10%

	Misuse of facility
2016	6,058
2017	4,209
change	-31%

TOTAL

2016	2017	change
78,471	71,747	-9%

Insurance

- Insurance related frauds increased by 31% in 2017, in comparison with 2016;
- Identity fraud saw a substantial increase in 2017. A large number of cases in 2017 related to the impersonation of real people, whereas in 2016 a large proportion related to fictitious identities. It is understood that those acting as 'ghost brokers' see the use of a genuine identity as a more reliable way of fraudulently obtaining policies;
- Misuse of facility also saw a large increase this period. Many of these were in relation to fraudulent claims against the Direct Debit Guarantee scheme, with policyholders fraudulently trying to claim back direct debit payments.

CASE TYPE

	Application fraud
2016	7,126
2017	5,462
change	-23%

	False insurance claim
2016	494
2017	541
change	10%

	Identity fraud
2016	248
2017	4,215
change	1600%

	Misuse of facility
2016	55
2017	171
change	175%

TOTAL

2016	2017	change
7,923	10,369	31%

Loans

- The number of loan-related frauds increased by 6% in 2017;
- Facility takeover saw a 602% increase in 2017 (albeit from a low base). This was due to an increase in instances of the unauthorised addition of a facility;
- The number of identity frauds to obtain a loan continued to increase in 2017, following a sizeable increase in 2016 compared with 2015. This is mainly due to a rise in current address impersonations;
- The number of misuse of facility frauds increased by 47% in 2017, with the majority in relation to loan payments being fraudulently evaded.

CASE TYPE

	Asset conversion
2016	21
2017	27
change	29%

	Application fraud
2016	3,202
2017	2,416
change	-25%

	Facility takeover fraud
2016	44
2017	309
change	602%

	Identity fraud
2016	18,736
2017	20,082
change	7%

	Misuse of facility
2016	950
2017	1,399
change	47%

TOTAL

2016	2017	change
22,953	24,233	6%

Online retail

- The total number of frauds against online retail products decreased by 12% in 2017;
- Identity fraud saw a 49% increase, which is mainly due to an increase in current address impersonations;
- Misuse of facility fraud saw a decrease, with fewer cases of evasion of payment.

CASE TYPE

	Application fraud
2016	94
2017	119
change	27%

	Facility takeover fraud
2016	949
2017	1,002
change	6%

	Identity fraud
2016	7,883
2017	11,729
change	49%

	Misuse of facility
2016	28,608
2017	20,108
change	-30%

TOTAL

2016	2017	change
37,534	32,958	-12%

Fraud by product breakdown

Mortgages

- The number of cases of mortgage fraud increased by 2% in 2017;
- The number of misuse of facility cases increased due to an increase in instances of misuse of a mortgaged property. This now includes cases where the mortgage holder is resident in a property subject to a buy-to-let mortgage as well as the unauthorised renting out of properties subject to a residential mortgage;
- Frauds around declared levels of income continue to be the most common application frauds.

CASE TYPE

	Application fraud
2016	2,874
2017	2,915
change	1%

	Facility takeover fraud
2016	22
2017	9
change	-59%

	Identity fraud
2016	48
2017	45
change	-6%

	Misuse of facility
2016	31
2017	70
change	126%

TOTAL

2016	2017	change
2,975	3,039	2%

Other

- The amount of fraud against 'other' products decreased by 14% in 2017;
- 'Other' primarily relates to cases of identity fraud to obtain credit files, which can be a precursor to further identity fraud. These cases decreased by 15% in 2017 compared with 2016.

CASE TYPE

	Application fraud
2016	63
2017	115
change	83%

	False insurance claim
2016	1
2017	
change	0%

	Facility takeover fraud
2016	25
2017	25
change	0%

	Identity fraud
2016	11,889
2017	10,132
change	-15%

	Misuse of facility
2016	46
2017	42
change	-9%

TOTAL

2016	2017	change
12,024	10,314	-14%

CROSSWORD ANSWERS

Across

2 Statistics (facts)
4 GDPR (regulating the use of personal data across Europe)
6 Crime (illegal activities)
7 Impersonation (acting as another individual)
9 Cyber (relating to the culture of computers)
10 Insurance (providing protection against a possible eventuality)
13 Monitoring (observing and checking progress)
15 Account (a report of an event or experience)
19 Database (a structured set of information)
20 Prevent (keep from happening)
21 Safe (unlikely to be harmed)
22 Victim (a person who has been duped)
23 Fraud (wrongful or criminal deception)
24 Deter (discourage)

Down

1 Security (the state of being free from danger)
3 Corruption (dishonest conduct typically involving bribery)
5 Protection (a buffer against possible threats)
8 Technology (machinery developed from scientific knowledge)
11 Solution (a means of solving a problem)
12 Financial (relating to money)
14 Hacking (gaining unauthorised access to a computer)
16 Cifas (leaders in fraud protection)
17 Identity (who or what a person or thing is)
18 Saviour (saves someone)
19 Detect (discover or identify)

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.