cifas
Leaders in fraud prevention

FRAUDSCAPE 2017

External and internal fraud threats – essential reading for fraud and financial crime strategists.

Introduction

Contents

Introduction

The fraud landscape

By Sandra Peaston
Assistant Director, Insight, Cifas

With almost one in every two crimes a fraud or cybercrime* there has never been a more urgent time for organisations to be alert to both the external and internal fraud threat.

Through Cifas, our members contributed over 325,000 cases of fraud to the national picture: the highest number ever recorded to our databases – the National Fraud Database and the Internal Fraud Database.

At the core of the Cifas cross-sector data sharing model is the view that fraud should not be tackled in isolation. For example, a credit card provider will find benefit in knowing about previous frauds that have affected an insurer, as an insurer will obtain benefit from knowing about frauds against the telecoms sector. The fact that our members prevented over £1 billion in fraud losses in 2016 – for the fourth year running – is evidence that an integrated and collaborative cross-sector approach is an effective remedy to combat an ever-increasing threat.

In this report, for the first time ever, we have brought together frauds recorded by Cifas members to the National Fraud Database and the Internal Fraud Database into a single document: making Fraudscape the only publication providing analysis of internal and external fraud trends in the UK.

In 2016, we saw a 1.2% increase in overall fraud recorded to our databases. Identity fraud reached the highest levels ever recorded with almost 173,000 cases reported by our member organisations. Fraudsters continued to focus on online applications, with 88% of identity frauds being internet-enabled.

Additionally, facility takeover fraud has increased by a substantial 45%. In contrast to identity fraud, the majority of these frauds happen over the phone and it is these telephone facilitated takeovers that have driven the overall increase: the key trend being fraudsters targeting mobile phone accounts in order to obtain upgrades. This trend can also be seen in bank account takeovers – telephone facilitated takeovers now represent almost 50% of these frauds. Despite high volumes, identity fraud against bank accounts and telecoms products actually fell in 2016.

By sharing these confirmed fraud attempts our banking and telecoms members are taking positive steps in helping to build a more accurate picture of the frauds they are experiencing as well as preventing their customers from further fraud.

Last year we also continued to see an increase in 'mule' activity, where genuine account holders are complicit in allowing criminals to transfer illegally obtained money between different bank accounts. Our data shows it is younger people who are more likely to commit this type of crime and therefore fraud education continues to be a key priority for 2017. You can read more about 2016 trends from our National Fraud Database on page 11.

Members of the Internal Fraud Database undertook over 750,000 searches on potential applicants in order to employ people securely and protect their workforce.

Similarly to 2015, the most common internal fraud was simply staff stealing cash. Our members reported that people committing internal fraud tended to be at the younger end of the age spectrum, with 53% aged between 21 and 30. You can read more about 2016 trends from our Internal Fraud Database on page 24.

With fraud and cybercrime now rivalling car crime, robbery and burglary as the high volume crime of the twenty first century, it is clear government, law enforcement, businesses and consumers must work together to combat this growing threat.

In 2017, Cifas will continue to support the Take Five campaign and we will focus our own efforts on education for young people. We must make sure the younger generation are equipped to protect themselves from becoming either a victim or committing fraud themselves and we will continue to work with the government to prioritise fraud education.

Sandra Peaston has over 15 years' experience in fraud data analytics, research and intelligence, and has been the author of Cifas' annual publication *Fraudscape* since its launch in 2010.

Our members record all frauds, whether successful attempts or not, to both the National and Internal Fraud Databases.

*The Office of National Statistics (ONS) Crime Survey of England and Wales estimates that fraud and cybercrime now account for almost six million offences.

01.

Main findings

Frauds recorded to the National Fraud Database

The frauds recorded in this section are from the National Fraud Database and have been recorded by our 277 member organisations.

Definitions:

Frauds covered in this section

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

False insurance claims 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.

Main findings

Key statistics and victim findings

The fraud picture in 2016

324,683

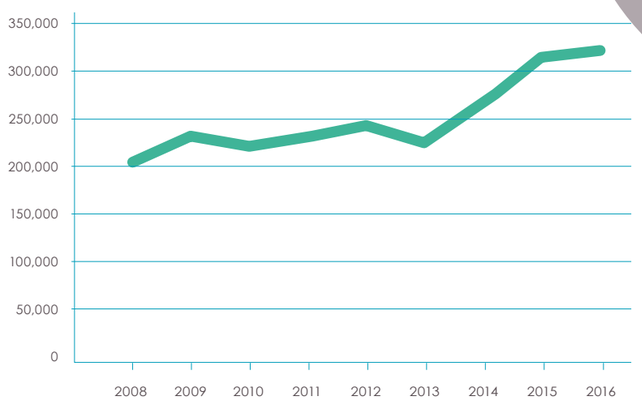
frauds recorded in 2016 – an increase on last year's record levels:

+1.2%

320,900

frauds recorded in 2015

The growth of fraud



Fraud by type

Asset conversion
2016 | 381
2015 | 258
+47.7%

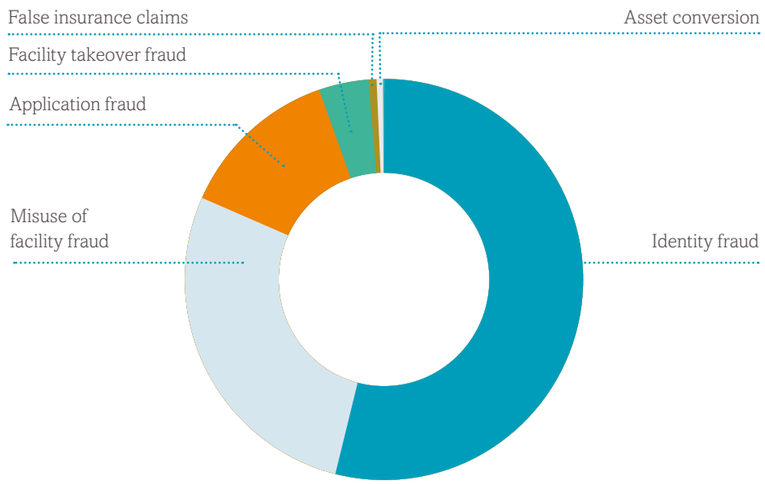
Application fraud
2016 | 31,559
2015 | 41,186
–23.4%

False insurance claims
2016 | 496
2015 | 366
+35.5%

Facility takeover fraud
2016 | 22,525
2015 | 15,497
+45.4%

Identity fraud
2016 | 172,919
2015 | 169,592
+2.0%

Misuse of facility fraud
2016 | 96,803
2015 | 94,001
+3.0%



Fraud by product

Bank account
2016 | 108,187
2015 | 112,613
–3.9%

Plastic card
2016 | 78,471
2015 | 72,895
+7.6%

Comms
2016 | 43,325
2015 | 50,357
–14.0%

Online retail
2016 | 37,534
2015 | 24,687
+52.0%

Loan
2016 | 22,953
2015 | 20,109
+14.1%

Other*
2016 | 12,026
2015 | 14,113
–14.8%

Asset finance
2016 | 10,860
2015 | 8,884
+22.2%

Insurance
2016 | 7,923
2015 | 12,621
–37.2%

Mortgage
2016 | 2,975
2015 | 4,238
–29.8%

All-in-one
2016 | 429
2015 | 383
+12.0%

Total
2016 | 324,683
2015 | 320,900
+1.2%

For a more detailed breakdown of frauds by product types please see pages 13-18 (Fraud in Focus) and Appendix A.

*'Other' primarily relates to cases of identity fraud to obtain credit files – a precursor to further identity fraud.

In brief:

Identity fraud

Almost

173,000

highest level ever recorded

Represents over

78%

committed using victim's current address

9/10

fraudulent applications for bank accounts and financial products made online

96%

committed with genuine victim's identity

4%

committed with fake identities

+34%

increase in victims under 21

Incidences of identity fraud

Plastic card

2016 | 65,425
2015 | 59,423
+10.1%

Bank account

2016 | 56,084
2015 | 64,174
–12.6%

Loan

2016 | 18,736
2015 | 13,392
+39.9%

Other

2016 | 11,890
2015 | 13,736
–13.4%

Comms

2016 | 11,529
2015 | 12,341
–6.6%

Online retail

2016 | 7,883
2015 | 5,734
+37.5%

Asset finance

2016 | 1,053
2015 | 560
+88.0%

Insurance

2016 | 248
2015 | 50
+396.0%

All-in-one

2016 | 23
2015 | 141
–83.7%

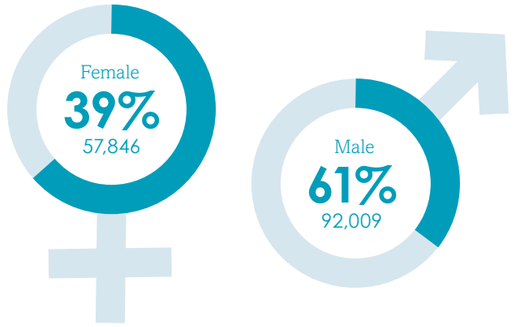
Mortgage

2016 | 48
2015 | 41
+17.1%

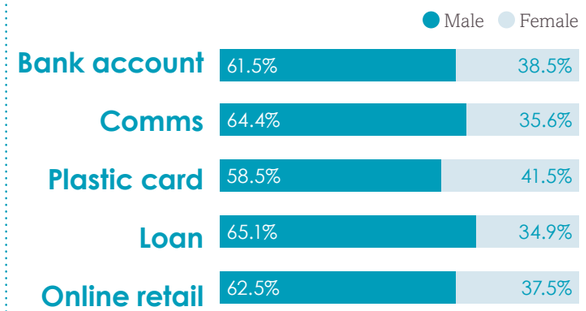
Total

2016 | 172,919
2015 | 169,592
+2.0%

Victims of impersonation



Gender of victims of impersonation, by product



Victims of impersonation by age*

+34%
Under 21
2016 | 1,803
2015 | 1,343

–0.2%
21-30
2016 | 22,572
2015 | 22,616

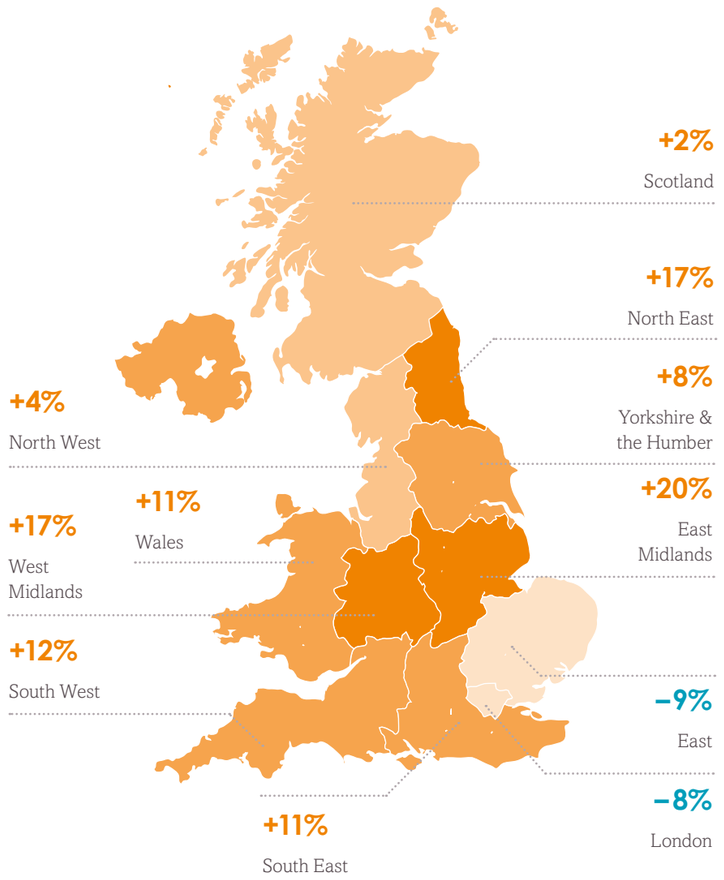
–7%
31-40
2016 | 33,883
2015 | 36,502

+0.9%
41-50
2016 | 34,010
2015 | 33,702

+5%
51-60
2016 | 29,818
2015 | 28,366

+0.4%
Over 60
2016 | 26,043
2015 | 25,934

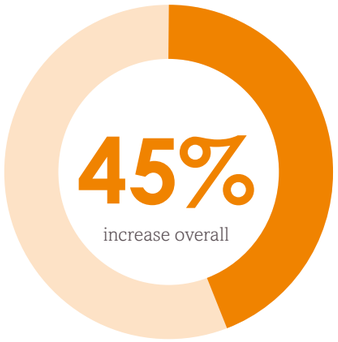
Victims of impersonation by region*



*Not all victims of impersonation are recorded with a valid UK address or date of birth, so not all cases can be attributed to a regional or age breakdown. Additionally, where the fraud involves the use of an entirely fictitious identity, no victim details are recorded.

In brief:

Facility takeover fraud



50%
committed over the telephone

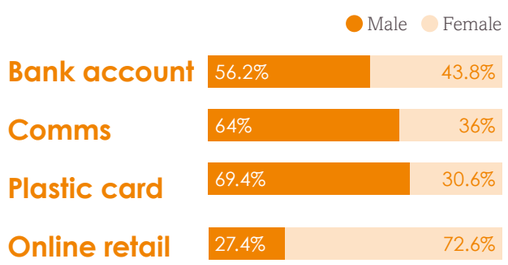
30%
committed online

49%
of bank account takeovers committed over the phone

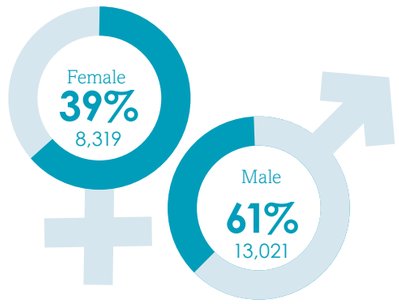
56%
of telecoms takeovers are fraudulent mobile phone upgrades

7,028
more cases recorded in 2016

Gender of victims of facility takeover fraud, by product



Victims of facility takeover fraud



Victims of facility takeover by age

In brief:

Misuse of facility fraud

In 2016 mule activity increased to

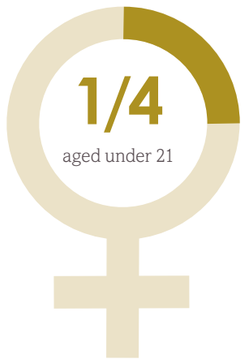
28,891
+9%

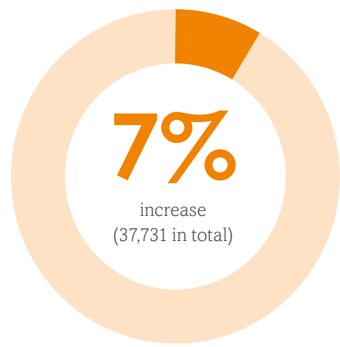
2015
26,431

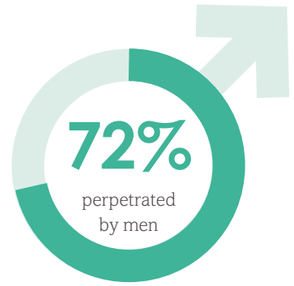
52%
of misuse of facility frauds are carried out by people aged 30 years or younger

Misuse of facility fraud against bank accounts

Of those perpetrated by women







Misuse of facility cases by product

Bank account
2016 | 37,732
2015 | 35,265
+7.0%

Online retail
2016 | 28,608
2015 | 17,488
+63.6%

Comms
2016 | 21,919
2015 | 34,738
–36.9%

Plastic card
2016 | 6,058
2015 | 5,104
+18.7%

Assest finance
2016 | 1,391
2015 | 753
+84.7%

Loan
2016 | 950
2015 | 346
+174.6%

Insurance
2016 | 55
2015 | 70
–21.4%

Other
2016 | 46
2015 | 61
–24.6%

Mortgage
2016 | 31
2015 | 159
–80.5%

All-in-one
2016 | 13
2015 | 17
–23.51%

Total
2016 | 96,803
2015 | 94,001
+3.0%

Main findings

Key external fraud trends in 2016

Identity related crimes

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

Identity fraud and cyber

There were almost 173,000 cases of identity fraud recorded by Cifas members in 2016, accounting for over 53% of all fraud cases. The vast majority of these cases (over 96%) involved the abuse of an innocent victim's identity, rather than a fictitious identity. In common with previous years, these frauds involved the use of the victim's genuine current address (78% of all identity frauds) as well as accurate personal details. The availability of large amounts of personal information obtained from hacking, phishing or data breaches continues to fuel this type of fraud. The proportion of identity frauds carried out through online channels also continues to increase – 88% in 2016, up from 86% in 2015 – no doubt due to the increase in online applications.

Clearly, use of the internet remains the key contributing factor to the continuing increase of identity fraud.

The internet provides the fraudster with the advantage of being able to apply in volume, at speed and with anonymity.

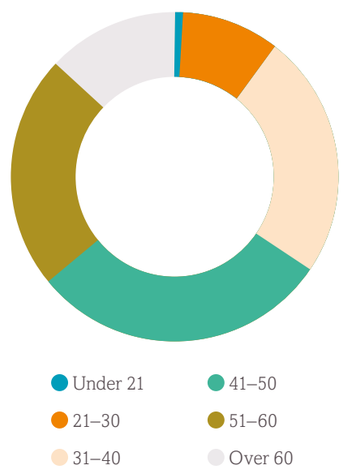
The nature and volume of identity fraud in 2016 means it is now predominantly carried out in an organised, industrialised manner.

However, not all identity fraud is carried out using the same organised methods. Almost 16,000 identity frauds (9.2% of all identity frauds) were attempted using the victim's previous address. The main reasons for this are detailed below:

Some of these frauds are likely to have been perpetrated by someone operating opportunistically. If someone who moves into a property finds that they are still receiving the mail, particularly financial mail, of the previous occupants, they could be tempted to use that information to apply for products and services before the previous occupant has got round to updating their address records with their bank or credit card provider.

Alternatively, it may well be that some of the personal data that a fraudster has obtained is simply out of date. Their victim has moved, and either failed to update their details with whichever organisation may have been the source of a data breach, or the information was compromised sufficiently long ago and the victim has since moved. It is generally accepted that data that has been compromised may not be used immediately.

Age breakdown of victims of impersonation



Facility takeover fraud – telephone is the channel of choice

The other fraud type where our member organisations identify abuse of identity information is facility takeover fraud. These are cases where a fraudster gains access to the accounts of innocent victims and then uses that access for their own benefit. This type of fraud had been on the wane following peak levels identified in 2012. By 2015, the number of facility takeover frauds identified over the course of the year had more than halved compared with 2012. This rapid decrease was largely attributed to increased account security, with initiatives such as card readers and device authentication strengthening access control. This means that the substantial increase identified in 2016, an increase of 45% up to over 22,500 cases, is notable.

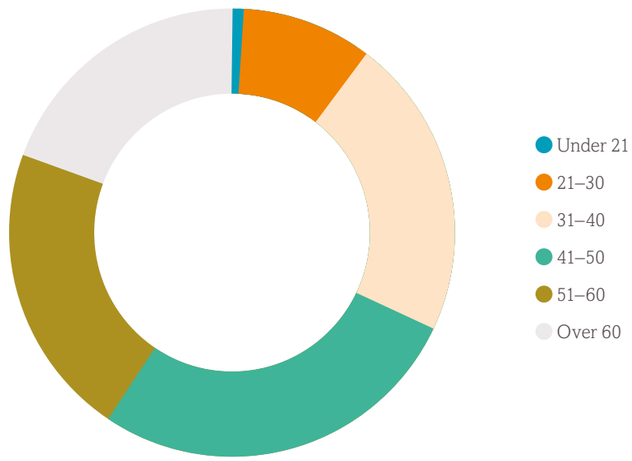
A key difference between identity fraud and facility takeover fraud is the extent to which it is perpetrated online. While 88% of identity frauds were perpetrated online, only 30% of facility takeover frauds targeted online access. Most commonly, and in over 50% of cases, takeovers were attempted through telephone channels. It is these telephone takeovers that have driven the overall increase in takeover fraud, and in particular the takeover of mobile phone accounts in order to obtain upgrades.

This targeting of the telephone channel reiterates the advances that have been made in securing online access to customer accounts. In fact, the number of identified attempted online takeovers decreased in 2016, demonstrating that so long as there are multiple different ways for customers to access their own accounts then fraudsters will attempt to gain access to those accounts using many different methods. The security of these channels cannot be neglected as fraudsters will target what they perceive to be the weakest point.

As technical innovations continue to improve online security, the weakest point appears to be the human being at the end of a phone line.

Investment in the deployment of voice recognition technology and other techniques to secure this point of access should be part of all members' armoury, as well as increasing awareness through training for call centre staff.

Age breakdown of victims of facility takeover



Fraud in focus:

Bank accounts

Identity fraud and the rise of the money mule

Bank accounts continue to experience the highest levels of fraud. However there was a 4% reduction in recorded levels of fraud against bank accounts, including an almost 13% drop in identity fraud.

7%

increase in misuse of facility fraud

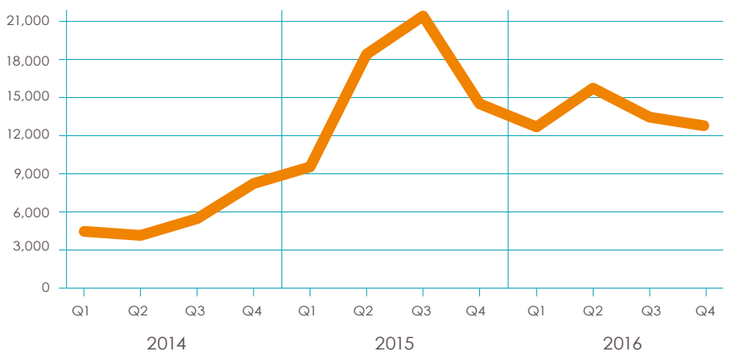
12%

increase in facility takeover fraud

49%

of takeover perpetrated through the phone channel

Identity frauds against bank accounts



Fraud against bank accounts, by fraud type

Identity fraud
2016 | 56,084
2015 | 64,174
–12.6%

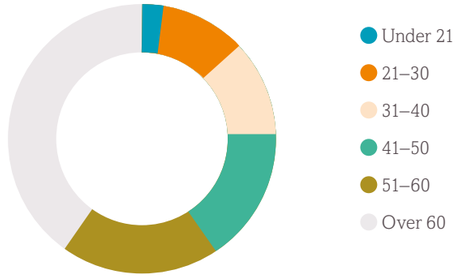
Misuse of facility fraud
2016 | 37,732
2015 | 35,265
+7.0%

Application fraud
2016 | 7,641
2015 | 7,191
+6.3%

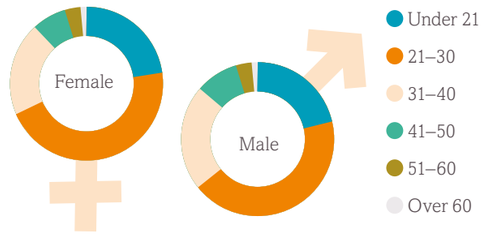
Facility takeover fraud
2016 | 6,730
2015 | 5,583
+12.5%

Total
2016 | 108,187
2015 | 112,613
-3.9%

Victims of bank account takeover by age



Age and gender breakdown of those fraudulently abusing bank accounts



The reasons that identity fraudsters target bank accounts could be for purely acquisitive reasons – for example to obtain an overdraft facility and spend the cash. However, there is growing concern that these accounts are being opened to facilitate the laundering of criminal proceeds, including as the destination accounts of fraudulently obtained funds from scams or as a link account within a mule network. These fraudulently obtained funds will often have been the result of scamming members of the public, convincing them to pay their own money (in some cases their life savings) over to fraudsters. This is clearly harmful to the individuals involved, but it also poses a problem for banking and law enforcement in unpicking whose money is whose, and ensuring that no one accidentally gives the proceeds of crime back to criminals.

Mule networks are not just made up of accounts in the name of innocent victims, often the account holder is complicit in these activities, being paid by organised criminals to allow their account to be used. These type of cases increased by 7% in 2016.

This type of fraud continued to be mainly carried out by young men, but there has been a notable increase in the number of young women becoming involved in this activity, increasing from less than 26% in 2015 to 28% in 2016. The women involved in these offences are younger than men, with a higher percentage of women being under 30 years of age.

Cifas has been leading work with Government through the efforts of the Home Office-led Joint Fraud Task force to establish fraud and financial crime education as part of the National Curriculum. The findings of this report serve to illustrate just how vital this initiative would be in safeguarding the future of a large number of young people.

Another area where there has been an increase in the number of frauds against bank accounts has been in account takeover. There has been a 12% increase in 2016 compared with 2015, although the numbers are substantially below those for identity frauds. However the impact of an account takeover can often be financially more harmful for the victim than a case of identity fraud as, although the victim will be reimbursed when a fraudster loots their account, there will be a period of time when that money is gone. There may be practical impact in that direct debits or standing orders may not go through while the account has less money in it than it should, and no doubt there will be some psychological impact on the victim from essentially having their money stolen.

In common with the general trend for facility takeover fraud, there has been an increase in the proportion of attempted takeovers that occurred through the phone channel – up to 49% of cases in 2016 compared with just 27% in 2015. Fraudsters have been manipulating call centre staff and/or their victim in order to gain access to the account.

It is this social engineering that is likely to have fuelled the rise in the takeover of bank accounts as well.

It is recognised that while everyone can be vulnerable to the most targeted or believable scam or social engineering approach, the elderly are considered more susceptible. This, unfortunately, is reflected in those that have been victims of account takeover, with the over-60s the most common age bracket. Working to protect the most vulnerable in society from fraudsters remains an area of priority.

Fraud in focus:

Plastic cards

Plastic cards remain a target for identity fraudsters

Plastic cards, predominantly credit cards, remain the second most commonly targeted product.

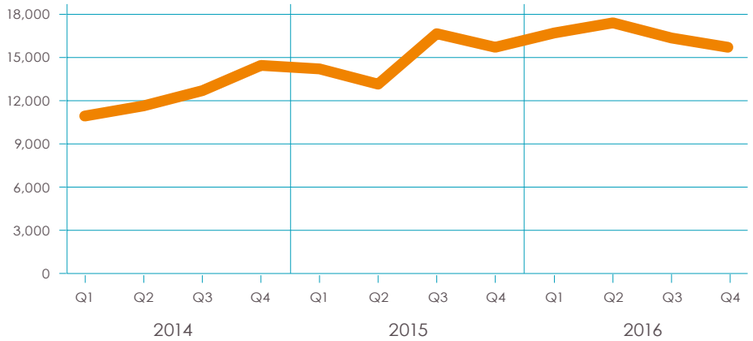
10%

increase in identity fraud

77%

use victim's genuine address

Identity frauds to obtain plastic cards



A credit card will always be an attractive product for an identity fraudster, and in 2016 it became the most commonly targeted product. Not only can fraudsters make applications behind an anonymous computer screen, but once they have obtained the card they can also make the most of it from the same position of security by buying goods online.

There is, though, one necessary step for the fraudster that they cannot take from such a position of comfort - the need to take receipt of a physical card. They will most likely have used the victim's genuine current address (77% of the time in 2016), as this increases the chances of their fraud being successful. So, they therefore need to intercept or redirect the mail before the victim receives a credit card that they did not apply for. There are a number of ways the fraudster achieves this. They have been known to target blocks of flats, or houses in multiple occupation, where they can gain access to mail boxes and impersonate a number of people within that building, and there have also been reports of false mail boxes being mounted to the walls of homes in order to intercept the mail.

Fraud in focus:

Telecoms

Mobile contract fraud on the decline and takeover fraud on the rise

Overall, the telecoms sector recorded 14% fewer frauds in 2016 than in 2015, predominantly due to a reduction in the number of misuse of facility frauds. These are cases where an individual takes out a contract with a mobile phone provider in order to obtain an expensive handset cheaply, but never had any intention of honouring the contract. In many cases the phone is then shipped abroad. These frauds were often orchestrated by organised criminals who recruited individuals to walk into branches and take out the contracts - thereby ensuring that the risk falls to that individual. However, although there has been a 37% decrease in this type of fraud being identified, indicating that fewer young people are being induced to take part in this activity for a short term financial gain - there were still almost 22,000 of these cases recorded.

This is another area where fraud and financial crime education for young people may well be one of the most effective ways of reducing this type of activity.

One area where telecoms members recorded more cases was facility takeover fraud. The number of cases increased from just over 2,000 in 2015 to more than 9,000 in 2016. The fraudsters' intent is to obtain unauthorised upgrades, which they perpetrated largely over the telephone, through the social engineering of call centre staff. This increase in takeover attempts, where the objective is to obtain a handset, may be the fraudsters' response to the lower number of instances where someone was able to obtain the handset for them at application stage. As we have commented previously, when one avenue is closed (or the opportunities reduced) fraudsters will find an alternative method of achieving their aims.

As telecoms companies are focusing their attention on improving fraud prevention and identification, as well as prioritising the reporting of fraud cases, a truer picture is emerging of the real level of attacks on the sector.

37%

reduction in misuse of facility

7,000

more facility takeover frauds recorded

Fraud in focus:

Online retail

Flexible delivery addresses play a role at Christmas

The figures in this section relate to cases that have been recorded by credit granting online retailers who are Cifas members. The totality of fraud experienced by the online retail sector as a whole will be substantially greater. FFA UK reported that in 2015, UK retailers were targeted with remote purchase frauds (card not present transactions) to the value of £155.5m. The underlying cause of these frauds is the same as the cause of the high levels of identity frauds suffered by organisations in the UK – the compromise and abuse of large volumes of data: be that personal information, credit or debit card information or (most likely) a combination of both.

The number of frauds recorded to the National Fraud Database by the credit granting online retailers increased by 52% in 2016 compared with 2015, with the increase primarily due to the growth in the number of cases of misuse of facility fraud. These are cases where the individual has opened an account and proceeded to spend against it, without ever intending to repay the money owed. There were 28,608 cases of this nature identified in 2016. This increase may be due to more individuals believing that they will be able to get away with their offence without it having any knock-on effects on either their credit rating or on their ability to obtain other goods and services. They may also view an online retail account in a different way compared to credit card account, for example, where they might expect more data to be shared among lenders.

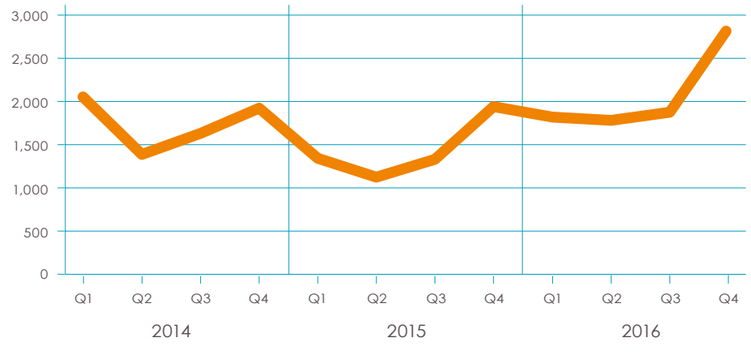
Unlike other types of fraud, identity fraud to obtain online retail accounts demonstrates a marked seasonality. 2016 is the third year in a row where there has been a noticeable peak in the number of cases recorded in the last quarter of the year.

Typically, a fraudster who commits identity fraud to obtain an online retail account will do so for the cash they can raise when selling the goods on. It is not unreasonable for the fraudster to surmise that in the run up to Christmas the busy online retailer will not scrutinise applications and orders with the same rigour as in the rest of the year. They will also take advantage of the fact that many retailers offer an alternative delivery address to get around the problem of how to physically obtain the goods when they've used the victim's genuine current address to make the application.

52%

increase in frauds recorded by online retail members

Identity frauds to obtain a retail account



Fraud in focus:

Insurance

False address still remains most common fraud

Cifas figures on insurance fraud are smaller than those for other sectors and should be considered in conjunction with other insurance fraud recording sources, such as the Insurance Fraud Bureau.

Most of the insurance cases recorded to Cifas involve individuals providing false addresses to make it appear their vehicle is kept in an area attracting a lower premium. For example, someone whose parents live in an area that would result in lower premiums, or where the individual could claim that the vehicle would be kept overnight off the street, may attempt this type of fraud. This occurred in 44% of application frauds to obtain insurance, up from 40% in 2015.

Also increasing in terms of percentage of cases were the instances of individuals claiming false levels of no claims discount (22% of cases). Again, this is very simply an attempt to pay less money for insurance cover.

There was a proportionate decrease in the number of cases where another person has 'fronted' a policy. These are cases where the principle policy holder is not going to be the main driver of the vehicle, in order to take advantage of the lower premium associated with that person. This dropped from accounting for over a quarter of cases in 2015, to just 15% in 2016.

While application frauds represent a large proportion of cases recorded by insurers, the number of instances of some other fraud types has increased. The number of false insurance claims recorded by insurers increased by 35% in 2016, to nearly 500 cases.

The largest increases in false claims involved the claimant making claims relating to events that simply did not take place. These increased from 21% of false claims in 2015 to over a quarter in 2016. Encouraging, though, is the decrease in the number of instances of events being staged – both in absolute numbers and as proportion of the total. These decreased from 95 cases in 2015 to 86 in 2016. These cases can relate to 'crash for cash' scams in which organised criminals orchestrate accidents on UK roads in order to make substantial claims against insurance policies. Given the danger that these events present to innocent road users, any decrease in the number of these instances must be seen as a positive for the insurance industry and law enforcement.

The number of identity fraud cases against insurers also increased in 2016, albeit from a low base. There were almost 250 cases in 2016 compared with just 50 in 2015. These fraudulent attempts to obtain insurance in a different name are likely to be a precursor to making fraudulent claims. It must also be considered a possibility that those perpetrating these frauds are looking to use insurance documents as a building block towards establishing an address history for that identity – and being able to use those identities for further fraud or other criminal activities. We must wait to see if this is a pattern that continues into the future.

396%

increase in identity frauds

44%

of application frauds recorded are false address

Spotlight on

Policing and organised crime

For fraud strategists and those responsible for financial crime prevention in their organisations, knowing who is perpetrating the fraud is an important factor in determining what prevention strategies should be deployed. Previous research indicates that only a small percentage of fraud was being conducted by organised crime, but recent research from Perpetuity Research and the Police Foundation shows that this may have been an underestimate.

Organised fraud in local communities

Authors
Research Team from Perpetuity Research and the Police Foundation

Mike Skidmore, Ruth Crocker, Sarah Garner, Sarah Webb, Martin Gill, John Graham

The Police Foundation and Perpetuity Research recently completed a research study looking at the scale, nature and impact of organised crime on local communities, a key strand of which focused on fraud. It found that a significant proportion of fraud could be attributed to organised crime and that the levels of financial harm experienced by the victims were considerably higher than for victims of non-organised fraud. The effectiveness of the response from local police and partners was also examined and significant gaps were identified, which led to new research on improving the response to fraud impacting at the local level.

The proportion of different fraud categories linked to organised crime

Fraud Category	Total no. of incidents	% Linked to OC	
		Lower Estimate	Upper Estimate
Mass marketing fraud	251	38%	59%
Fraudulent sales	266	23%	34%
Investment fraud	67	69%	70%
Identity fraud	72	13%	25%
Abuse of Trust	33	12%	21%
Fraudulent sales in person	32	16%	38%
Fraudulent applications	10	30%	50%
Total	**731**	**31%**	**45%**

Introducing the study

In addition to developing improved estimates for the scale of fraud (for example, the recent introduction into the Crime Survey for England and Wales) there has been increasing recognition, certainly from government and national enforcement agencies, that organised crime groups are responsible for much of the fraud impacting on the UK. A significant proportion of the £24 billion cost of organised crime to the UK was attributed to fraud by the Home Office (2013). However, there was little robust and empirical research aimed at understanding the precise scale and nature of this overlap, particularly in relation to fraud impacting locally. This research sought to address the gap.

Whereas previous studies had used practitioner estimates for determining the links between fraud and organised crime, an entirely data-driven approach was adopted for this analysis. The government definition of organised crime was broken down into its constituent parts to form a criterion, against which the information provided by fraud victims could be tested:

- The presence (or likelihood) of multiple suspects;
- The seriousness of the fraud offending;
- Persistence of offending over time;
- The sophistication of the modus operandi.

This study focused on specific locations in two police force areas: Avon and Somerset and West Midlands. It applied this analysis to a sample of fraud reports recorded by the National Fraud Intelligence Bureau.

The scale and nature of organised fraud

The analysis estimates that between a third (31 per cent) and nearly half (45 per cent) of frauds were linked to organised crime groups, considerably higher than the previous government estimate of 15 per cent. Specific categories of fraud were also analysed and revealed wide variation in the degree to which they were linked to organised crime.

The majority of investment fraud, a low volume but very impactful fraud-type, was found to be rooted in organised crime. Mass marketing fraud accounted for a significant proportion of all reported fraud and up to 59 per cent of these cases were attributed to organised crime. The indication is that there are organised crime groups causing a disproportionate amount of the fraud-related harm.

The financial harm to victims of organised fraud was considerable and they lost significantly more money than other fraud victims; an average of £10,260 compared to £3,982 for each offence. It is estimated that victims of organised fraud lost, on average, nearly half (48 per cent) of their annual income.

The local response to fraud

The volume and nature of modern fraud makes policing this type of offence extremely challenging, and the extent of the volume has only recently started to be reflected in police recorded crime figures. This previous lack of recognition of the scale of the problem will have adversely affected the degree to which fraud has been seen as a policing priority.

Multiple barriers to establishing a comprehensive and cohesive response to fraud at the local level were identified. These included a lack of prioritisation by local police forces, a lack of clarity on remit (a particular issue due to the physical separation of victim and offender and the centralisation of reporting through Action Fraud), a general lack of appetite and perceived capability for tackling fraud within local police teams, and the fragmentation of the response across multiple local agencies, with no-one taking ownership of the fraud problem locally. In the context of enforcement, fraud was barely present in both local practitioner views and strategic assessments for organised crime.

There was a lack of convictions in following up and investigating cases received from the National Fraud Intelligence Bureau. This research also raised issues around the standards of service received by victims who reported fraud; many received little support or advice from police or other local teams.

Next steps

In recognition that the existing response to fraud does little justice to the scale of the problem, the Police Foundation and Perpetuity Research are currently involved in follow-up research which is focused on improving the response to fraud impacting locally. For further information on this and any other issue raised in the article please contact:

michael.skidmore @police-foundation.org.uk or **m.gill@perpetuityresearch.com**

02.

Main findings

Frauds recorded to the Internal Fraud Database

The frauds recorded in this section are from the Internal Fraud Database and have been recorded by our 172 member organisations.

Definitions:

Frauds covered in this section

Account fraud

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

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.

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.

Being bribed

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

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.

Main findings

The insider fraud picture in 2016

An organisation's employees are one of the strongest forms of fraud defence. They are uniquely placed to scrutinise the activities of customers, suppliers and, of course, their colleagues. Given the right channels to raise concerns, staff can provide an additional layer of protection alongside more technical forms of monitoring.

Less honest members of staff can present a major threat to an organisation. In the most extreme cases, a dishonest staff member can endanger the financial stability of the company or destroy its reputation (for example, through stealing customer data or being the cause of a data breach). However, they can also facilitate a number of other external frauds, such as disclosing processes and procedures to the fraudsters so they are better armed to take advantage of any weak points, or even just using their position to ensure that fraudulent applications are approved or fraudulent abuse of products and services is overlooked.

172 organisations use the Cifas Internal Fraud Database to create a strong anti-fraud culture within their organisation by sharing the details of those members of staff or employment applicants who have committed fraud against them.

This section of Fraudscape examines the internal fraud cases that were recorded to the Internal Fraud Database in 2016 and provides an indication of the types of internal fraud trends Cifas members saw in 2016. These cases, as with the National Fraud Database, are backed by sufficient evidence to support the standard of proof required for a report to the police.

There were 409 cases recorded to the Internal Fraud Database in 2016. The table shows the types of fraud which were recorded.

Fraud by type

Account fraud (ACF)

2016 | 31
2015 | 50
–38.0%

Being bribed (BBR)

2016 | 1
2015 | 2
–50.0%

Dishonest action by staff to obtain a benefit by theft or deception (DIS)

2016 | 172
2015 | 188
–8.5%

Employment application fraud (Successful) (EAS)

2016 | 39
2015 | 34
+14.7%

Employment application fraud (Unsuccessful) (EAU)

2016 | 159
2015 | 313
–49.2%

Unlawful obtaining or disclosure of commercial data

2016 | 0
2015 | 2
–100.0%

Unlawful obtaining or disclosure of personal data (UDP)

2016 | 31
2015 | 36
–13.9%

Total cases

2016 | 409
2015 | 585
–30.1%

Main findings

Key internal fraud trends 2016

For the first time since 2012, dishonest actions by staff to obtain a benefit by theft or deception was the most common type of insider fraud. Often believed to be opportunistic or impulsive, this may explain why cases of this type have not declined in line with other types of internal fraud.

As in 2015, the most common dishonest action performed by staff is simply stealing a customer's cash.

This accounted for 22% of these cases in both 2015 and 2016. With these frauds it may be that the opportunity presented to the employee is simply too tempting and in that moment, the danger of being recorded to the Internal Fraud Database and getting a criminal conviction is superseded by the potential for financial gain.

The second most common dishonest action in 2016 is the manipulation of third party accounts. This is where the employee abuses their position in order to remove charges or change limits on accounts, frequently on behalf of friends and family. These cases accounted for just under 19% of dishonest actions in 2016 compared with under 14% in 2015.

By contrast, the number of cases where the member of staff is facilitating transaction fraud fell from over 17% in 2015 to less than 12% in 2016. It can be expected that in these cases, the member of staff is likely to be operating on behalf of other fraudsters and it could be a positive indicator that the number of more 'organised crime' cases appear to be falling. The threat of ever more sophisticated monitoring techniques being employed by organisations may mean that criminals are being forced to find alternative ways to facilitate transaction frauds.

As highlighted elsewhere in this report, the number of identity frauds recorded in 2016 reached the highest level ever recorded, and the fuel for these frauds is personal data. It is therefore vital that organisations remain alert to the value of personal data and the risks of it being handled by dishonest staff. Our data shows that 31 employees were recorded for this offence.

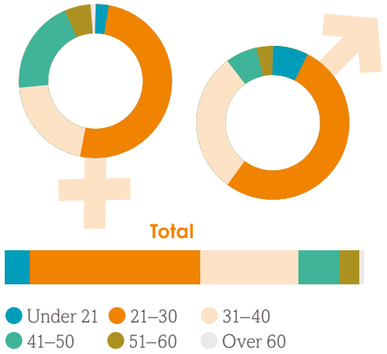
While these frauds often present no immediate financial cost to the organisation, the reputational fallout from a large scale data breach can be substantial, not only when the breach first comes to light, but also every time that the breached information is used to phish and scam those whose data has been compromised. Moreover, if the breached personal data relates to customer account information, then the risk of the accounts held by those customers being taken over is greater – and if those takeovers are successful then there will certainly be a financial cost to the organisation. Lastly, the fines that can be imposed in the event of a breach will increase when the new General Data Protection Regulation comes into force – up to 4% of global annual turnover or £20 million. In this context, ensuring your employees are not tempted into the unlawful and fraudulent disclosure of information should be a high priority for any organisation.

Who committed internal fraud?

Overall, almost 64% of internal fraudsters recorded to the IFD in 2016 were men, which is largely unchanged from 2015. There has been a slight increase in the number of women involved in the compromising of personal data – 13 in 2016 compared with eight in 2015.

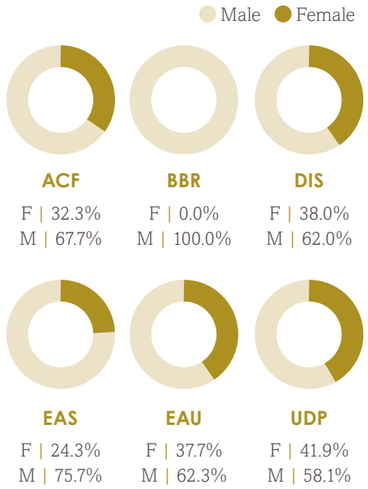
This means that the proportion of men committing this crime has dropped to less than 60% from 75% in 2015. This is a fraud type that has previously been significantly male dominated so this shift will require some monitoring to establish if this is merely an anomaly resulting from low numbers or if there is some other rationale. For instance, are organised identity fraudsters specifically targeting women to compromise personal data in the belief that they are less likely to be suspected?

Age of internal fraudsters



The graph above clearly shows that internal fraudsters tend to be towards the younger end of the age spectrum, with 53% of internal fraudsters aged between 21 and 30. For those that have been compromising personal data, this figure increases to 65% (20 out of the 31 people).

Internal fraud by gender



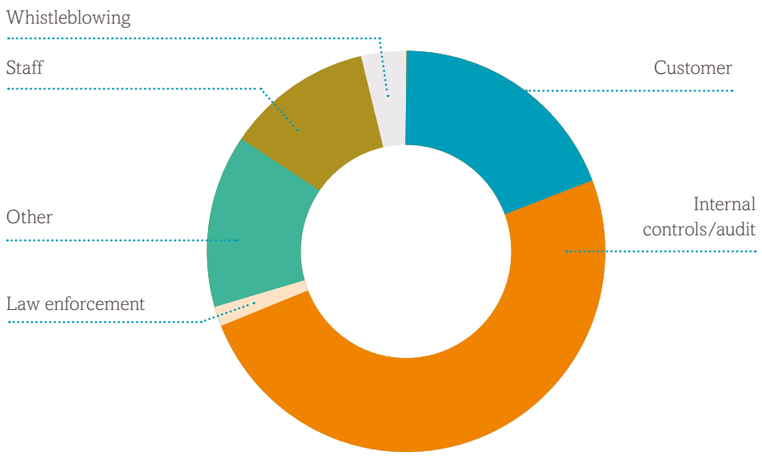
See previous page for acronyms (Fraud by type).

How are the internal fraudsters caught?

The most common means of discovering the internal frauds recorded in 2016 was internal controls and audit (47%). This is reassuring as it means that the investments made by organisations in these processes and, in some instances, software solutions are providing value. It is also likely that these systems are at least partially responsible for the lower levels of recorded internal fraud. If staff believe that the chances of getting caught are high, then some are less likely to perpetrate the fraud in the first place – particularly if this is backed up with the prospect of being recorded on a fraud prevention database and their fraudulent past being made clear to future employers. Of course, this fear of getting caught and the possible repercussions will not deter all potential internal fraudsters. Researchers who interview convicted internal fraudsters frequently find that the fraudsters simply did not expect to get caught. They believed that they were smarter or that they had found an infallible loop-hole. It is this mentality that means that investment in monitoring systems and data sharing schemes continues to be vital.

A positive finding from the cases recorded in 2016 is that more of them came to light through members of staff raising concerns, either directly through line management or through whistleblowing lines. Over 17% of cases came to light in this way (47 in 2016, up from 34 in 2015). For an organisation's reputation this can only be a good thing and goes to show that efforts to raise awareness among staff of the importance of raising concerns is bearing fruit. And it also goes to prove that, as we stated at the beginning of this section, mobilising the honest majority in a workforce can provide one of the strongest defences against fraud.

Means of discovery



Spotlight on insider fraud and cyber

Cyber security is ultimately a people issue

By Peter Cheese, CEO of the Chartered Institute of Personnel and Development

As well as being important to fraud and security specialists, HR professionals require an understanding of the human dimension when it comes to understanding the fraud and cyber risks.

Yet many businesses think they won't be targets for attack, and most breaches go unreported because they would compromise reputation and trust, and therefore risk further damage.

Ultimately, whilst technology is the first line of defence, fraud and security breaches are down to the actions of people – either those inside our organisations, or those outside. The harsh reality though is that the so-called insider threat is responsible for a high proportion of breaches, from the intended or unintended actions of employees.

For cases of deliberate fraud by employees, historically many of these (unless of major consequence) would tend to be dealt with through summary dismissal and nothing further. Cifas' Internal Fraud Database provides a way of recording these events and many employers have signed up to it, providing a means to check on the background of potential employees in the future.

Growing data privacy legislation based on prevention through compliance is the overarching solution many regulators are seeking, and EU legislation is clearly pushing further in this direction. However, many breaches occur through ignorance or lack of awareness. They can be as simple as employees becoming victims of phishing or even ransomware attacks, or taking data out of the secure environment and then 'losing' it, or working outside through insecure channels that are easily hacked, or even just trying to be helpful and not questioning outsiders' right to access. As we build more diverse workforces and more flexible ways of working, these threats continue to grow.

Cyber security through technology will need to work better in all these circumstances, but technology in itself can never be the only answer. And nor can rules and regulations be sufficient in themselves. We have to capture hearts and minds, to create a wider culture of understanding and responsibility from the top down, not just tickbox compliance.

Awareness and education

We must begin, therefore, with educating our workforces about their role and responsibilities in protecting information and access to data. This must include the principles and policies of data privacy – what data is being held, transparency about why the data is needed, and expectations from those about whom data is held: be they customers or any other external groups, but also our employees themselves.

But to really change behaviour we have to make it personal. We have to help our employees understand about their own 'cyber wellbeing' – how to protect their own data and identity and why this is important. If they understand that, they will much better understand the importance for the organisation's data, and be more likely to engage.

Inside our organisations, HR has a huge role to play. Cifas highlighted in their 2016 Employee Fraudscape report that after the risk and fraud functions, HR is seen as the most accountable. Recruitment, monitoring of employees, policies and processes, communications and training, as well as access to hotlines and whistle blowing are all areas that HR needs to understand.

However, HR hasn't always been engaged on these issues and too many departments still see cyber security as a technology issue first and last. Programmes like Cyber Essentials or the National Cyber Awareness course are good places to start in upping our awareness, and the CIPD, as the professional body for HR, has been talking more about the issues and has launched short programmes such as 'Cyber Security for HR Professionals' working together with the Department for Culture, Media & Sport.

Cyber security needs to be approached like any risk to business today - we must take a holistic view. We need to connect our understanding of people and behaviour, culture and organisation, with the technology, the operations, and our risk and control functions to better protect all our stakeholders for the future.

Appendix A

Fraud by product breakdown

All-in-one

- There has been an increase in the number of facility takeover frauds affecting all-in-one products. These cases are predominantly related to unauthorised electronic payment instructions.
- The number of identity frauds decreased substantially in 2016.
- The numbers constituting these totals are low in comparison to other products, which means that small changes in numbers leads to more substantial percentage changes.

Product	2015	2016	%
Application fraud	24	1	–96%
Facility takeover fraud	201	392	+95%
Identity fraud	17	13	–24%
Misuse of facility fraud	141	23	–84%
Total	**383**	**429**	**+12%**

Asset finance

- The total number of frauds related to asset finance products increased by 22% in 2016 in comparison to the previous year.
- The largest increase was in the number of identity fraud cases. This increase was primarily due to a higher number of current address impersonations.
- Misuse of facility frauds also increased, with more instances of fraudulent evasion of payment.

Product	2015	2016	%
Asset conversion	253	360	+42%
Application fraud	7,318	8,050	+10%
Facility takeover fraud	0	6	–
Identity fraud	560	1,053	+88%
Misuse of facility fraud	753	1,391	+85%
Total	**8,884**	**10,860**	**+22%**

Bank accounts

- Identity fraud cases for bank account products decreased by 13% in 2016. However, this follows the unusually high levels seen in 2016. The number of cases recorded in 2016 is still substantially higher than seen in the years prior to 2015.
- 77% of misuse of facility cases for bank account products are highly likely to be linked to 'money mule' activity.

Product	2015	2016	%
Application fraud	7,191	7,641	+6%
Facility takeover fraud	5,983	6,730	+12%
Identity fraud	64,174	56,084	–13%
Misuse of facility fraud	35,265	37,732	+7%
Total	**112,614**	**108,187**	**–4%**

Communications

- The total number of frauds committed on communications products decreased by 14% in comparison to 2015.
- The most notable change is seen in facility takeover frauds, where there was a substantial increase in the number of cases of fraudsters obtaining unauthorised facility upgrades.

Product	2015	2016	%
Application fraud	1,124	782	–30%
False insurance claim	0	1	–
Facility takeover fraud	2,154	9,094	+322%
Identity fraud	12,341	11,529	–7%
Misuse of facility fraud	34,738	21,919	–37%
Total	**50,357**	**43,325**	**–14%**

Plastic cards

- The number of frauds relating to plastic card products increased by 8% from 2015 to 2016.
- In 2016 plastic cards were the products most targeted by identity fraudsters, following bank accounts being the most targeted in 2015.
- The decrease in application frauds was down to a reduction in the number of cases being filed for applications with undisclosed residential information.

Product	2015	2016	%
Application fraud	2,558	1,726	–33%
Facility takeover fraud	5,810	5,262	–9%
Identity fraud	59,423	65,425	+10%
Misuse of facility fraud	5,104	6,058	+19%
Total	**72,895**	**78,471**	**+8%**

Insurance

- Insurance-related frauds decreased by 37% in 2016 in comparison to 2015.
- Despite the overall decline in insurance-related cases being filed, identity frauds for insurance products increased substantially. These cases may relate to making fraudulent claims in another name, or to obtain proof of address in that name and facilitate further fraud.
- The lower level of application fraud was primarily due to a lower number of cases relating to the fronting of insurance policies and the provision of false payment information.

Product	2015	2016	%
Application fraud	12,135	7,126	–41%
False insurance claim	366	494	+35%
Identity fraud	50	248	+396%
Misuse of facility fraud	70	55	–21%
Total	**12,621**	**7,923**	**–37%**

Loans

- The number of loan-related frauds increased by 14% in 2016.
- The number of identity frauds to obtain a loan increased, primarily due to a particularly high number of cases recorded in the fourth quarter of 2016.
- The number of misuse of facility frauds increased by 175% in 2016, due to more loan payments being fraudulently evaded.

Product	2015	2016	%
Asset Conversion	5	21	+320%
Application Fraud	6,360	3,202	–50%
Facility Takeover Fraud	6	44	+633%
Identity Fraud	13,392	18,736	+40%
Misuse of Facility Fraud	346	950	+175%
Total	**20,109**	**22,953**	**+14%**

Online retail

- The total number of frauds for online retail products increased by over 50% in 2016.
- Identity fraud and misuse of facility percentage changes were down to significant increases in current address fraud and evasion of payment respectively.

Product	2015	2016	%
Application fraud	173	94	–46%
Facility takeover fraud	1,292	949	–27%
Identity fraud	5,734	7,883	+37%
Misuse of facility fraud	17,488	28,608	+64%
Total	**24,687**	**37,534**	**+52%**

Mortgages

- The number of cases of mortgage fraud decreased by 30% in 2016.
- The facility takeover fraud cases were mostly due to a substantial rise in cases where there was an unauthorised change of security/personal details. Had this been successful, it would have been a precursor to further abuse of the account – such as remortgaging the property.
- The decrease in application frauds for mortgages was down to fewer cases of undisclosed adverse credit data on applications.

Product	2015	2016	%
Application fraud	4,037	2,874	–29%
Facility takeover fraud	1	22	+2100%
Identity fraud	41	48	+17%
Misuse of facility fraud	159	31	–81%
Total	**4,238**	**2,975**	**–30%**

Other

- The amount of fraud against 'other' products decreased by 15% in 2016.
- 'Other' primarily relates to cases of identity fraud to obtain credit files – a precursor to further identity fraud. These cases decreased by 15% in 2016 compared with 2015.

Product	2015	2016	%
Application fraud	266	63	–76%
False insurance claim	0	1	–
Facility takeover fraud	50	26	–48%
Identity fraud	13,736	11,890	–13%
Misuse of facility fraud	61	46	–25%
Total	**14,113**	**12,026**	**–15%**

Why your organisation should 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 businesses 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 most 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.

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

cifas.org.uk