LexisNexis®
RISK SOLUTIONS

cifas
Leaders in fraud prevention

Who are the victims of identity fraud?

Assessing the characteristics of impersonation to identify those most at risk

Table of Contents

1. Executive summary

Recent figures published by Cifas revealed that identity fraud continues to escalate with attempts reaching record levels in 2016. The data, recorded by Cifas members, shows that in the vast majority of cases fraudsters are using accurate personal data to apply for products and services through online channels. Preventing these attacks is challenging, but there are two areas where prevention activities can have an effect:

- Identifying which applications are more likely to be cases of identity fraud
- Preventing the fraudster from obtaining the personal data in the first place

To help achieve both of these objectives, it is important to understand who is most likely to be targeted by identity fraudsters. Understanding the most likely targets will help raise awareness with these groups so they can take steps to protect themselves. This will also help organisations prioritise investigations where an application can be considered higher risk.

Cifas and LexisNexis® Risk Solutions have collaborated on research that sheds more light on the characteristics of identity fraud victims. Cifas extracted three and a half years' worth of impersonation data from the National Fraud Database between 2012 and 2015, then appended supplementary data provided by LexisNexis Risk Solutions for additional insight. This included information such as the tax band of the victim's address; if they are a company director; and whether they have any County Court Judgments (CCJs) or are insolvent. This information provides a better picture of the victim as well as those most likely to be targeted. The key findings also include the most common type of accounts that fraudsters open with the victim's identity.

Key findings from the research

- **Company directors are targeted more than the population as a whole**
  Company directors account for roughly 9% of the population; however, they made up 19% of victims of impersonation. It must be recognised, though, that the degree to which they are disproportionately targeted has reduced over the three and a half year period.
- **Higher value properties lead to higher levels of impersonation**
  A disproportionate number of victims of impersonation lived in properties with higher tax brackets (indicating higher value properties), although it was most common for victims of impersonation to live in properties in tax band C with a value around the national average.
- **A CCJ reduces the likelihood of impersonation but insolvency doesn't**
  Those with an insolvency were actually impersonated more frequently than would have been expected, while those with CCJs were impersonated less frequently. This may be because those that have some form of insolvency display the characteristics in line with those of company directors, while CCJs are an indicator of debt problems making these individuals less attractive to identity fraudsters.

- **Credit files can influence fraudster behaviour**
  The victims of impersonation who were directors and whom were insolvent or had CCJs, were all targeted to obtain credit files more frequently than other victims of impersonation. If a fraudster is successful in obtaining a credit file in the name of their victim, then the victim's credit status will likely serve to influence the extent that a fraudster chooses to target a particular identity and what subsequent product or service they attempt to obtain in that name.
- **Company directors are actually younger than the average victim of impersonation.**
  Across the time period under consideration, the average age of victims of impersonation was 47 years old. Where the victim was a director, this dropped to 44 years of age. This contradicts the idea that the company director targeted by identity fraudsters is the stereotypical grey-haired denizen of the boardroom.
- **Fraudsters use directors' identities to acquire unexpected products**
  While it may have been expected that fraudsters are using directors' identities to predominantly obtain bank accounts and accounts that require a good credit score (e.g. loan applications, high-end credit cards), they actually have used these victims' identities to obtain a disproportionately high number of online retail and mobile phone accounts.

Summarised recommendations for consumers

- **Limit unnecessary publicly available information**
  Some data is public record, such as property ownership or company directorships. This can provide fraudsters with a starting point. It is likely, though, that they will need to build on this to make the information 'useable' – and it is here that people can make the fraudsters task more difficult by restricting the information about themselves and their lives that they make publically available online (for example, on social media).
- **Regularly check your credit file**
  This will highlight any anomalous accounts or searches that point towards having been a victim of impersonation.

Summarised recommendations for organisations

- **Targeted awareness**
  Company directors in particular are still impersonated more than others, so targeted awareness activities through bodies that work directly with those more at risk can help communicate the associated risks and ensure preventative steps are acted upon.
- **Look for patterns and similarities**
  This research has shown that 16% of victims are impersonated repeatedly. This shows that data sharing has an important part to play in effective fraud prevention and protecting victim's identities from further abuse. It is also important to look at other patterns and similarities within the identified frauds to prevent the fraudsters abusing multiple identities.

- **Intelligent use of data to score risk**
  There are sections of the population, such as company directors, who are impersonated more frequently than others. Identity management should make use of additional data sources to identify heightened relationship risk.
- **Prioritise investigations that have victim characteristics**
  The use of tracing and investigation software can be used to help identify characteristics of victimisation from within those applications that are subject to referral to fraud teams, which can help fraud investigators focus and prioritise their investigations.

Statement from Sandra Peaston, Assistant Director, Insight, Cifas

As any victim of identity fraud will tell you, falling victim can be a traumatic and frustrating experience. Although in most cases they are not liable for a loss of funds, it is the time it takes to rectify the situation that has the greatest impact on victims. Having to prove it was not you who applied for that bank account or credit card in the first place as well as the implications of repairing your credit history is what makes the whole experience so challenging.

Whilst we have seen growing numbers of young people falling victim in recent years, we know that every age group is at risk. Our research with LexisNexis® Risk Solutions shows that almost 20% of victims are company directors – this finding should serve as a stark warning to those individuals who are at increased risk and raise awareness of the importance of being alert to the threat. The research also affirms what many have already suspected - fraudsters will target those who bring the greatest yield – so we hope the more detailed findings will inform those responsible for developing fraud prevention strategies to implement an effective response.

From using strong passwords and downloading software updates to regularly checking bank statements and being careful of what we share online, we can all take simple but effective steps to protect our personal data.

We all remember to protect our houses and our physical belongings from people we don't know or trust. We need to do more protect our identities in every aspect of our lives if we are ever going to reduce the number of victims.

Statement from Steve Arnison, Commercial Director, LexisNexis Risk Solutions

With unprecedented levels of identity theft and corporate data breaches, identity fraudsters have ready access to personal identities on an industrial scale. The digital revolution has shifted consumer expectations to personalised service and on-demand fulfilment, but alongside these benefits comes a vulnerability to new waves of identity fraud through online channels that provide fraudsters with a less risky access point for impersonation to take place.

Now more than ever, data intelligence has an important role to play in identity fraud prevention. The more we know about the fraudsters' approach and their victims' identities, the more chance we have of protecting consumers and bottom lines.

Cifas' deep level of fraud knowledge, insight and extensive National Fraud Database combined with LexisNexis® Risk Solutions expansive consumer data universe, presented an opportunity to collaborate and learn more about how and why fraudsters target their victims. We also wanted to decipher whether certain identity attributes makes somebody more or less likely to fall victim to identity fraud.

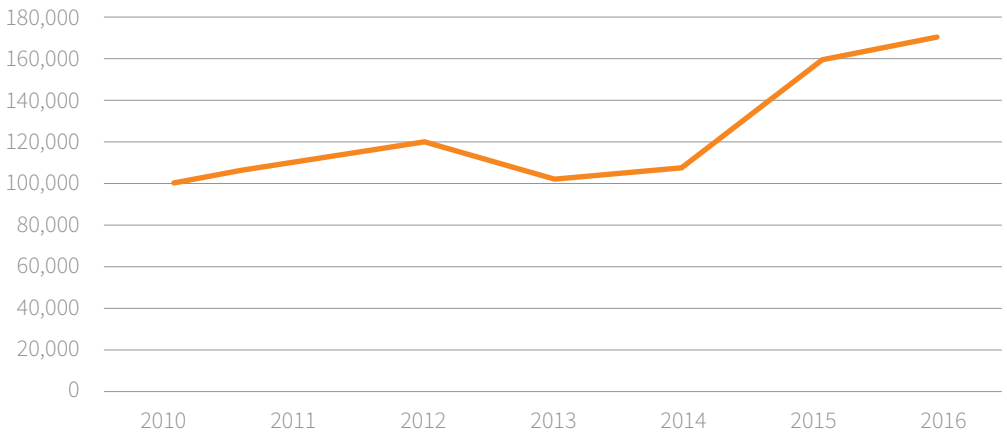
This report has helped to substantiate long held beliefs of a typical identity fraud victim as well as bring to light new findings. We hope it provides a reminder that intelligent fraud prevention methods and strong identity management practices are continually required to counteract this growing crime. We welcome a further dialogue for industry conversation and collaboration.

2. Introduction

Identity fraud is an increasing problem. With more and more individuals falling victim to impersonation, it's a problem that is affecting large numbers of the UK public - as shown by the trends in Figure 1.

Figure 1

Identity fraud



Are there some individuals who are more at risk than others? What makes someone a target for impersonation? To answer these questions Cifas and LexisNexis® Risk Solutions undertook a collaborative research exercise bringing together their complementary datasets relating to victims of identity fraud. This insight has allowed us to develop a better picture of the individuals who have been impersonated in order to identify how these individuals can better protect themselves and how organisations can look out for warning signs in order to protect consumers who are most at risk.

Of course, we cannot always know from where criminals get information about their victims. For example, we know that the methods used by identity fraudsters are varied, from the hacking of systems to the phishing and social engineering of individuals. What we can find out is the type of person that is most commonly targeted and what attributes fraudsters look for in order to carry out a successful impersonation and subsequently fraudulently obtain new products and/or services.

Identity fraud is rarely opportunistic, but instead is highly organised. It requires planning, acquisition of personal data and a certain amount of associated research to ensure that multiple fraudulent applications are successful. Organised identity fraudsters will often try and take advantage of as many identities as possible, so knowing what types of identities they typically use can be incredibly useful. By finding out as much as possible about the methods by which identity fraudsters are perpetrating their fraud, it is possible to shine a light on how organised fraudsters operate and, crucially, if there are any opportunities for organisations to raise awareness, implement new measures and keep one step ahead of them.

3. Methodology

Cifas extracted three and a half years' worth of impersonation data from the National Fraud Database, which contained the details of the victims of impersonation who had been recorded by Cifas member organisations. This data was then appended with supplementary data provided by LexisNexis Risk Solutions, which gave additional insightful information around the individuals who have been victims of fraud.

Table 1

Matched impersonation data by year

Year	No. of Cifas victims of impersonation submitted for matching	No. of Cifas victims of impersonation linked to LexisNexis Risk Solutions data
2012	99,882	93,273
2013	83,842	80,265
2014	87,071	84,662
2015 (to June)	26,256	25,613

The Cifas data included key information about the victims, such as age, gender and where they lived at the time of the fraud. Alongside this, the data also comprised information about the fraud itself, for example, the type of product that the fraudster targeted and the channel through which they carried it out, for example, online, in person or by telephone. All of this information can be used to build a picture about how and why the fraudster chose to use that individual, but there is also a wealth of additional data which can be used to enrich this information.

LexisNexis Risk Solutions provided extra information about the impersonated individuals, such as the tax band of their home address; if they are a company director; whether they have any County Court Judgments (CCJs) or are insolvent. This information gives a much clearer picture of who the victim is and, crucially, if they are more or less likely to be targeted based on these additional attributes.

Additional analysis was undertaken to determine which of these victims were more likely to become victims of impersonation more than once: for example, are the identities of certain types of individual more likely to be taken advantage of multiple times? The sequence of events was also investigated to see if the fraudsters changed the products they attempted to obtain depending on whether or not that individual had been impersonated before.

4. Results

Fraudsters do not operate indiscriminately, and instead focus their efforts on methods that they know will yield a better result. As such, it is known that identity fraudsters will target victims who are more likely to be accepted for products and services because of who they are, where they live or what they do. Often individuals are likely to be chosen on their overall 'credit-worthiness' and, if successful, fraudsters may also attempt to utilise this successful identity multiple times in order to take full advantage of it. Whether or not they are successful more than once will often depend upon whether the victim finds out or if suspicions are raised at the organisations to which the fraudster is applying. This section looks at each of the positive and negative attributes an individual might have and whether this makes them more or less likely to be targeted by identity fraudsters.

4.1 Company directorships

Anecdotal evidence suggests that fraudsters find company directors prime targets for impersonation, but this hypothesis hasn't really been fully tested before. One of the datasets provided by LexisNexis Risk Solutions concerned company directorships and was used to identify how many victims of impersonation could be linked in some way to a company director (be that themselves, a family member or a household member).

As of March 2015, roughly 9% of the UK population was registered as a company director[1]. However, this number more than doubles with 19% of all victims of impersonation (across the three and half year period) being company directors. This substantiates the belief that an individual is more likely to be targeted based on the fact that they are a company director. Not only are they perceived to be more likely to be credit worthy (owning assets, more established in their careers, and so on), but there may also be more openly available information about these individuals compared with the average person due to the fact that company information is published publicly and the director can therefore be associated with it. One possibility is that the fraudsters use the publicly available data as a starting point and then obtain further information in order to successfully commit the fraud.

It is notable, though, that the extent to which company directors are targeted appears to be diminishing over time, as can be seen from Figure 2. It is likely that this is a factor of the increasing availability of personal data and increasing levels of impersonations across the general population as a whole rather than a reduction of fraudsters targeting company directors. Whilst, the proportion of victims who are directors is falling, they still represent almost 16% of victims in 2015 and so remain substantially over-represented.

1. Companies House https://www.gov.uk/government/organisations/companies-house/about/statistics

Figure 2

Proportion of company directors

The consistent high level of company director victimisation can be explained by the fraudsters' possible modus operandi. By gleaning enough information about the company director, fraudsters can then attempt to fraudulently obtain their credit file in order to access more detail, and build a more convincing picture before fraudulently applying for other products and services. Credit files can hold lots of valuable information about potential victims and once a fraudster has this, then their applications will appear more credible and will be less likely to arouse suspicion when committing further fraud.

Map 1 shows the distribution of company directors impersonated for credit files in 2015. Whilst there is considerable fraudulent activity in the major towns and cities, it's clear that a large proportion of the identity frauds have been carried out on individuals living in the south east of England. This mirrors what we know about how fraudsters target their victims; the average income of individuals living in London and the South East is considerably higher[2] than in other areas of the UK, so for fraudsters to be successful in their impersonations, it would make sense for them to choose victims who live in these areas in order to maximise the financial gain.

2. https://www.equalitytrust.org.uk/scale-economic-inequality-uk

Map 1

Company director credit file impersonations map

Figure 3 below shows a real example of how the fraudster's methods work. Person A (a company director) was successfully impersonated for a credit file in early 2015 (Case 1) and three days later, was impersonated with varying degrees of success for four different products/services (two unsecured loans, a credit card and a vehicle on finance – Cases 2 to 5). Not only does this highlight the sequence of events described previously, but also the speed at which the fraudster acts. Once the individual knows that they have been impersonated then their identity will become useless to the fraudster, so utilising it as much as possible in such a short space of time is key if the fraudster is to maximise success.

Figure 3

Identity fraud case study

In this example, it is clear that this individual has been impersonated multiple times, but how common is this? Will fraudsters try and use the identity of a company director multiple times or do they consider them to be no less disposable than that of any other victim? Across the three and a half year period, 16% of all identity fraud victims were found to have been impersonated more than once, while the figure for company director victims was virtually the same at 17%. So the fact that an individual is a company director doesn't change the amount of times a fraudster will (on average) re-use their identity on multiple applications. This is most likely due to the fact that an identity is only useful for as long as the victim is unaware they are impersonated and not how credit worthy the individual is in the first place.

Another aspect that could be affected by whether or not an individual is a company director, is what products the fraudsters choose to target. It is possible that due to their directorship and associated credit worthiness, fraudsters might choose to use these identities to apply for products and services which have a higher threshold for credit scoring, for example, personal loans or asset finance products (compared with the likes of payday loans which would have a much lower threshold). However, the results show that company directors are proportionally less likely to be victims of impersonation for products such as plastic cards and bank accounts compared with all victims as a whole. Across the three and a half year period, 26% of company director victims were impersonated for plastic cards, while the figure for all victims was 35%. Similarly, 7% of company director victims were impersonated to open bank accounts compared with 17% for all victims. Although using a credit worthy identity is useful for obtaining a plastic card, the sheer volume of fraudulent applications that criminals make to credit card companies is so high that the number of company directors are lost in the large number of applications. Applying for credit, especially online, is quite efficient for the fraudster so they may have concluded that it is not worth the effort to single out company directors for this particular purpose. It is a similar story for bank accounts as almost any individual is able to open one (particularly basic accounts or those with reduced facilities). Identity fraudsters have possibly realised that it is not necessary to single out and impersonate a company director in particular for a bank account but instead can use almost any identity in order to open a new banking facility.

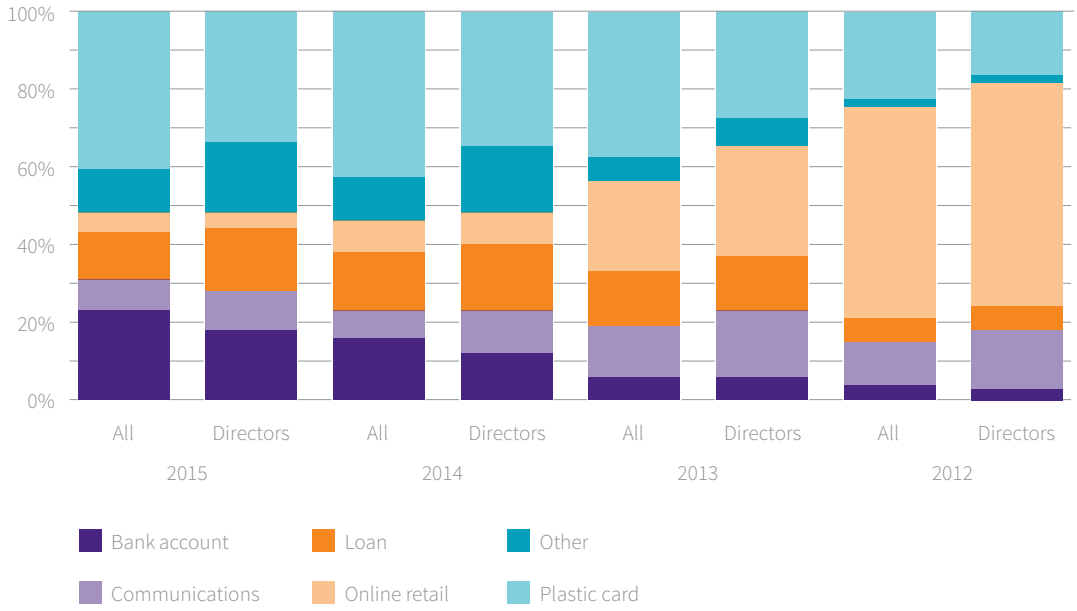
So if company directors are not being impersonated for credit cards or bank accounts, what are they being targeted for? As mentioned previously, fraudulent credit file requests are proportionally much higher for company directors than for all victims as a whole, showing that fraudsters will go to the effort of building up an identity if they believe it is worth it. Interestingly, impersonations of company directors for online retail accounts is disproportionately high with 32% of company director victims being impersonated for this product type compared with just 20% for all victims as a whole. It is unclear why this might be the case, but it is possible that the volume/value of any online orders that the fraudster makes may be easier to explain by virtue of the fact that they appear to be a company director.

Another product that was slightly overrepresented by company directors was that of communications products (for example, mobile phones). Although (like online retail) this seems counterintuitive, this once again could be due to fraudsters taking advantage of company contracts to obtain multiple mobile phones per single impersonation. If they are impersonating a company director, then they know that it would probably look less suspicious if they were buying large company contracts for multiple phones rather than buying multiple phones just as a single, individual customer.

But have the products targeted by those impersonating company directors changed over time? It must be borne in mind that, overall, the products targeted by identity fraudsters change, so we need to ask if the impersonation of company directors changes with these variations.

Figure 4

Director impersonations by product



As impersonations to obtain online retail accounts have decreased overall, so has the over-representation of company directors as victims of these frauds. They were over-represented in 2012 and 2013, but by 2014 and 2015 company directors are targeted for these accounts in line with overall trends. The extent to which directors have been targeted for loans has increased over the period though, with the levels of over-representation increasing in 2014 and 2015. However, company directors are always over-represented as victims of impersonation for communications (mobile phones) and, tellingly, credit files.

4.2 Council tax property bands

The second aspect of this research looked at tax bands and the extent to which fraudsters target their victims based on the type of property they live in and not just where in the country they live. We know that in certain circumstances and for certain products, fraudsters can be selective about who they impersonate in order to succeed in their fraudulent applications. Does finding out the property type and associated wealth of an individual change whether or not a fraudster impersonates them, and is it worth their while to find out?

Council tax property bands[3] are based on the value of properties not used for business purposes. The value is based on the value the property would have sold for on the open market. Properties were put into a band based on their market value on 1st April 1991 in England and 1st April 2003 in Wales.

In 1991 the average house price was £62,000, which was above the midpoint of band C. Bands A-B contained properties below the average, while in D-H properties were above the average

Figure 5

Impersonation by property tax band (A-H)

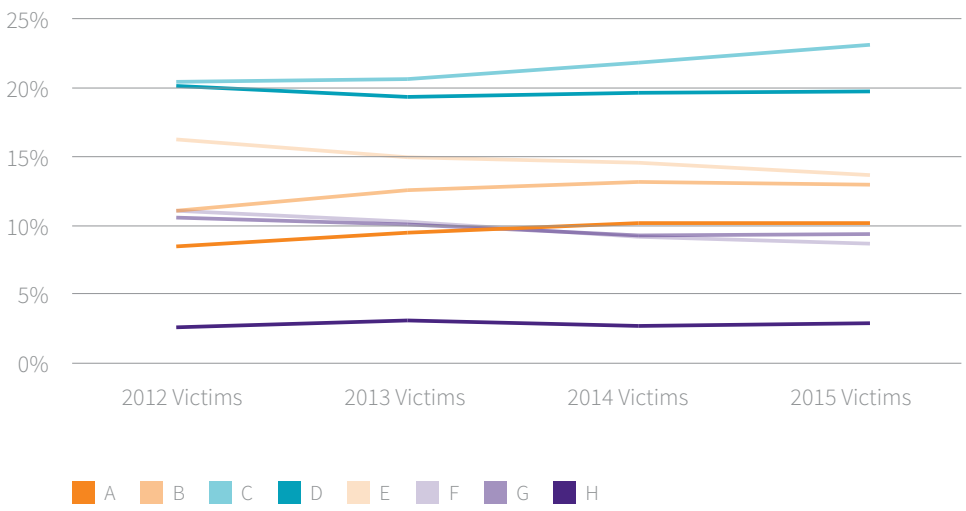
3. https://www.gov.uk/guidance/understand-how-council-tax-bands-are-assessed

On the whole over the three and a half year period, council tax property bands A-C are underrepresented in the victims of impersonation results set, with band A making up 24% of households in the country (based just on England for comparison) but just 9% in the victims of impersonation results set. Up at the other end of the scale, bands D-H were overrepresented in the results (property band I contains very low numbers and is omitted from these results due to having a percentage close to 0%). For example, band G contained 4% of all households but 10% of all victims of impersonation over the three and a half year period (see Chart 2). This isn't, perhaps, too surprising. We know that fraudsters target more credit worthy individuals, so by association, these individuals are more likely to live in bigger and higher value properties as a result of their wealth. How the fraudsters know who to target is another matter, but the research suggests that there is an element of targeted selection when it comes to the impersonation of innocent parties.

It is worth highlighting that, consistently over the period, those living in properties in the C tax band are most frequently impersonated, and the proportion of victims living in properties in this band is increasing year on year, as can be seen in the graph below.

Figure 6

Victims by property tax banding over time



Clearly, the graph shows that there are no seismic shifts in the property bands of victims of impersonation over the three and a half years, but (in common with the extent of victimisation of company directors) the victimisation of those in B and C properties is increasing while those in E and F is slowly reducing.

When it comes to products, there are similarities between the types of products targeted at higher tax bands and those targeted when impersonating company directors. Once again, online retail and communications products are overrepresented for those individuals who are perceived to be wealthier; for example, who live in properties in higher tax bands. In fact, 62% of impersonations for online retail products have targeted individuals living in properties in tax bands D and above, and 61% of impersonations for communications products also involved individuals living in properties with tax bands at D or above. When looking at the country as a whole, roughly 34% of properties fall in bands D and above, showing a marked overrepresentation for victims of identity fraud involving communications and online retail products. This ties in with the products fraudsters apply for when using the identities of company directors; clearly fraudsters targeting wealthy individuals (identified through either being a company director or living in an expensive property) do so for these types of products above others.

The proportion of victims living in higher value properties (D or above) across all of the products exceeded 34%, so the over-representation of victims at higher value properties was common to all products. The extent of over-representation was lowest against insurance and mortgages with 38% and 46% of victims living in those properties respectively. These are the only two products where there were more victims living in properties in bands A-C.

One point to bear in mind, however, is that the level of identity fraud carried out on these products is much, much lower than other products. The stringency of verification and affordability checks for mortgage applications is very high and it is very unlikely that an identity fraud would be successful, explaining the low level of identity frauds to obtain a mortgage. Insurance is slightly different in that there is no immediate payoff for identity fraudsters. Organised identity fraud leading to large, lucrative 'cash for crash' scams does happen, but generally insurance is not the obvious target for the more opportunistic identity fraudster looking to make some quick cash with relative ease.

4.3 Insolvencies and CCJs

What has been apparent so far is that identity fraudsters are more likely to impersonate individuals who are seen as wealthy and/or have a good credit rating. On that basis, it is perhaps to be expected that individuals who are bankrupt or who have CCJs are less likely to be impersonated, but to what extent is this actually true? Does an insolvency or CCJ dramatically change the chances of being impersonated?

Insolvencies

Bankruptcy/Sequestration[4] – a way of clearing debts that cannot be repaid and usually lasts for a year.

Individual Voluntary Arrangement (IVA)[5] - an agreement with creditors to pay all or part of debts. An agreement is made to make regular payments to an insolvency practitioner, who will divide this money between the creditors.

Trust Deed[6] - a formal, legally binding document that transfers part or all of the debtor's assets (money and property) to a trustee to manage for the benefit of the creditors.

Debt Relief Order (DRO)[7] - a way for individuals to deal with debts if the individuals owe less than £20,000, don't have much spare income and don't own their own home.

Overall, just 0.25% of the victims of impersonation over the three and a half year period were recorded with some kind of insolvency (either bankruptcy, IVA, Trust Deed or DRO – see the text box of definitions). The average figure for all individuals in the UK is somewhere around 0.14%, so although still small, the proportion of victims of impersonation who are insolvent is somewhat higher than the national average. Based on what we already know about identity fraudsters targeting wealthy, credit-worthy individuals, this seems counterintuitive. It is possible that these individuals have not been targeted because they are insolvent, but because the demographic, geographic and economic profile of these individuals fits that of the 'worthwhile' identity. Individuals that have some sort of insolvency are likely to be economically active and in business, and are likely to be of a certain age, and so are targeted for these reasons. An identity fraudster will use a number of identities that fit a certain profile, and they probably will not even be aware that some of these identities are associated with bankruptcy but will utilise them anyway because they fit the criteria that they are looking for.

It is also important to note that the results that we see here will not necessarily be a full picture of all identity fraud occurring in the country. This is because, for some products, the frauds on the Cifas National Fraud Database will only have come to the attention of fraud investigators after the application has passed the credit scoring process and has been referred for further investigation. This means that there may be many more fraudulent attempts that are being screened out earlier and therefore never being looked at or recorded to the database. When looking at identity frauds linked to individuals with poor credit (in this case bankruptcies) this scenario is particularly likely, so in reality the proportion of these identity frauds associated with bankrupt individuals could be much higher due to the fact that many might be being screened out at the credit scoring stage. Looking at the tax bands in conjunction with insolvencies, the greatest proportion of identity fraud victims lived in

4. https://www.citizensadvice.org.uk/debt-and-money/debt-solutions/bankruptcy-2/bankruptcy-explained/bankruptcy-overview/
5. https://www.gov.uk/options-for-paying-off-your-debts/individual-voluntary-arrangements
6. https://www.dasscotland.gov.uk/about/different-ways-deal-debt/what-trust-deed
7. https://www.gov.uk/options-for-paying-off-your-debts/debt-relief-orders

properties in band C (27%), while the greatest proportion of properties in the country as a whole are sat in band A. Although not as obvious as the tax bandings for company directors (where all of the higher tax bands were overrepresented), there is still evidence to suggest that the individuals targeted are still considered somewhat wealthy despite having some sort of insolvency.

It is notable that over the duration of the three and a half year period, there is little difference in the proportion of victims with insolvencies, or indeed the tax banding of the property that they live in. While there are slight fluctuations, considering the small numbers involved it is actually surprising that the fluctuations are not greater – between 0.27% of victims in 2014 and 0.23% of victims in 2012 and 2015. Unlike other criteria considered in this report, there is no discernible pattern emerging.

Looking at the product breakdown of identity frauds against insolvent individuals, there are some differences compared with the product breakdown of identity fraud victims as a whole. Although broadly following the same pattern, one big discrepancy is that the proportion of frauds carried out on insolvent individuals on 'other' products (which are comprised almost entirely of fraudulent credit file requests) is much higher than the baseline proportion for all impersonated individuals (15% for insolvent individuals compared with 6% overall). We know that, in some cases, individuals are impersonated for credit files in the first instance in order for the fraudster to harvest more data about them to enable further fraud on a variety of products. What could be happening here is that individuals are being impersonated for credit files and the fraudster finds out about their poor credit history and subsequently does not try to impersonate them for anything else due to the fact that they think that they would not be successful in their fraudulent applications.

County Court Judgments (CCJs)

Although being bankrupt means that a fraudster is less likely to be successful in impersonating them, the profile of a bankrupt individual often fits that of somebody the fraudster would consider worth impersonating. It's unlikely that the same can be said for CCJs, so is the level of impersonations among individuals with CCJs drastically lower than the national average?

A **County Court Judgment (CCJ)**[8] is a type of court order in England, Wales and Northern Ireland (NI) that may be registered against an individual if they fail to repay money they owe.

8. https://www.gov.uk/county-court-judgments-ccj-for-debt/overview

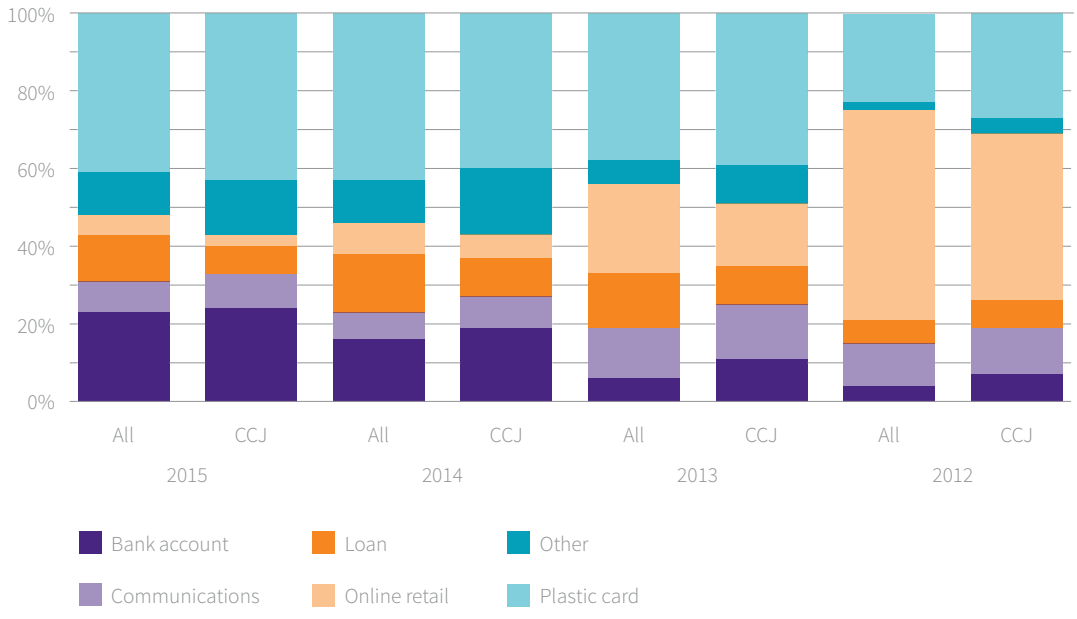
Over the three and a half year period, 2% of impersonated individuals had a CCJ compared with 5% of the England, Wales and NI population as a whole having a CCJ. This is perhaps to be expected: an individual with a CCJ is less credit worthy than an individual without a CCJ, so the chances of a successful impersonation resulting in a new product or service for the fraudster is quite remote. As mentioned previously, however, it's also worth remembering that some organisations will screen out the fraudulent applications before they reach investigation stage based upon their credit score alone. This means that the number of frauds using the identity of an individual with a CCJ could actually be much higher. It is not known just how many fraudulent applications are refused at credit stage, so the true scale of this type of fraud is likely to be under-reported and the proportion of impersonated individuals who have a CCJ may well be much higher and therefore more reflective of UK population as a whole.

What we do know from looking at the products targeted by identity fraudsters when impersonating individuals with a CCJ is that (just like insolvencies) they're more likely to fraudulently apply for credit files. Across all impersonations, around 6% are for fraudulent credit file requests, while for impersonations of individuals with CCJs this figure rises to 11%. All other product types remain broadly in line with impersonations as a whole, showing that the major discrepancy does appear to lie with fraudulent credit file requests. As with insolvencies, this is perhaps what we would expect: fraudsters attempt to access an individual's credit file and, if successful, they subsequently find out that the individual has a CCJ and is therefore not worth impersonating.

This finding is consistent over the course of the three and a half years, as can be seen from Figure 7.

Figure 7

CCJ impersonations by product



It is notable that the instances of someone with a CCJ being impersonated for an online retail account, particularly in those years where there were substantial levels of impersonation to obtain those accounts, is somewhat less than would be expected. What is also interesting is the extent to which those with CCJs are increasingly targeted for bank accounts. It may be that financial inclusion policies and the advent of the basic bank account has meant that those with CCJs are still viable as victims of impersonation for these products.

Looking at the tax bands of the addresses of the individuals with CCJs who have been impersonated indicates a similar pattern to what we have seen so far. Although these individuals have credit related issues, the results show that, proportionally, they are still living in more expensive properties than the country as a whole. The proportion of impersonated individuals with CCJs living in tax bands A-B is low at 35% (for the UK this figure is 44%), with every tax band over B being overrepresented when compared with the UK as a whole. Once again, this shows us that although these individuals have CCJs, the fact that they generally appear to be wealthier (for example, living in expensive property) makes them a target for fraudsters. Again, this could be a symptom of only the most credit worthy individuals passing credit scoring - it could be that individuals living in less expensive homes are still being impersonated but they fail to pass credit scoring and are therefore the attempt is never identified as fraud and never recorded to the Cifas National Fraud Database.

4.4 Victim ages

The age of impersonation victims was assessed to see if there were any notable variations of age distribution in general, as well as those that were directors, were insolvent or had CCJs.

Overall, the average age of a victim of impersonation (at the point which the fraud was identified and recorded, and where the individual matched to LexisNexis Risk Solutions data) was 47 years of age. Table 2 below shows the average ages across the different subsets.

Table 2

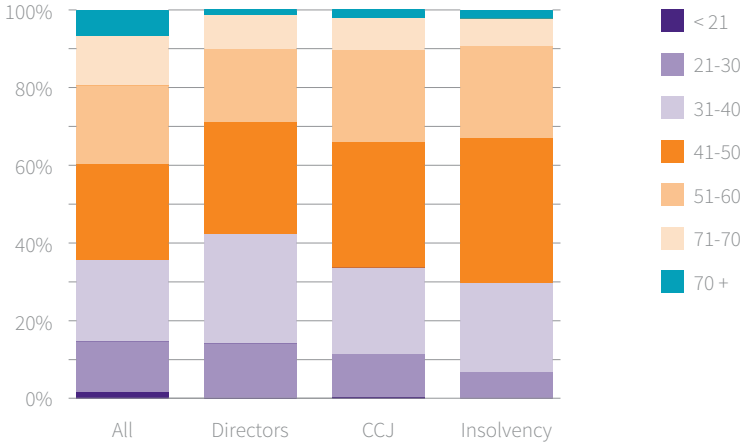
Average age by subset

	Average age (years)
All	47.2
Company Director	44.0
CCJ	45.7
Insolvency	46.4

Of interest here is that victims of impersonation who are company directors actually have a lower average age than all victims generally. Most commonly, victims fall into the 31-40 year old age bracket (28% of director victims) while for all victims, it is the 41-50 age range that is the most common. The understanding is that company directors are targeted due to the availability of their data and the perception of their status in life – and therefore credit-worthiness. This finding, though, very much indicates that age is not a determining factor in this perception. For context, the average age of a UK citizen is now 40, so it is clear that fraudsters are not targeting the 'older' company directors.[9]

Figure 8

Ages of victims of impersonation

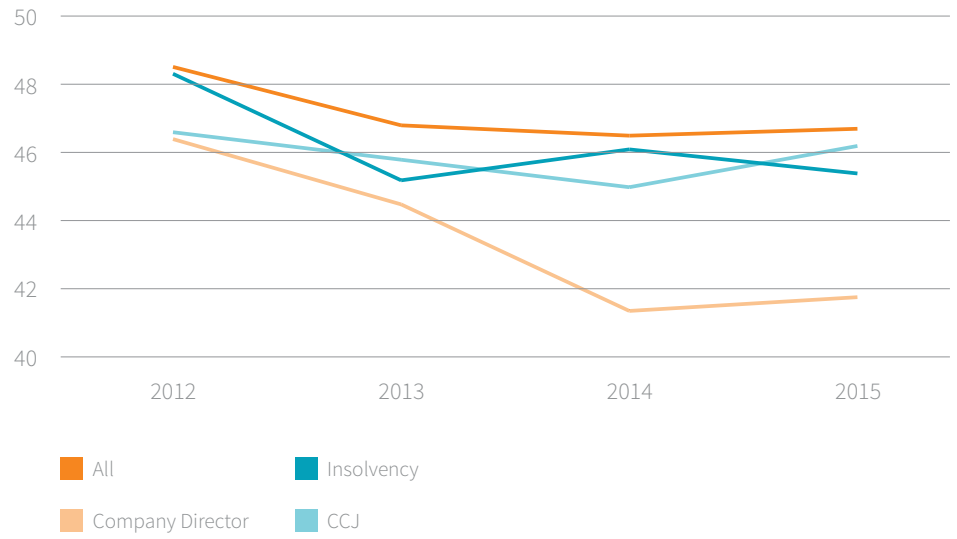


It is also of interest that there has been a general decrease in the average ages of victims of impersonation over the period. Cifas has observed this trend previously and it has led to increased efforts to target prevention messaging towards younger people. The reason for this decreasing age profile has been attributed to the greater availability of personal data, leading to less targeting of any specific demographic. The extent to which the average age of company director victims is falling faster than the average of victims in general is surprising – however it must be considered that the age profile of company directors may also be changing, and it is this that is influencing the average age of those directors who are victims of impersonation.

9. http://webarchive.nationalarchives.gov.uk/20160105160709/http:/www.ons.gov.uk/ons/rel/pop-estimate/population-estimates-for-uk--england-and-wales--scotland-and-northern-ireland/mid-2014/sty-ageing-of-the-uk-population.html

Figure 9

Average age of victims over time



Victims of impersonation with CCJs or who are insolvent are also younger than victims of impersonation in general, although the difference is less marked. Any trend is also less discernible. This further supports the view that the targeting of these individuals (particularly those with CCJs) is not deliberate, and is more a factor of availability of data and also potentially proximity for the fraudster – particularly those impersonations where the fraudster needs to intercept mail.

5. Conclusions

Identity fraud is a problem that can affect anybody and it is clearly a problem that isn't going away. With over 170,000 identity frauds perpetrated in 2016 alone, many people have already become victims and many more will fall victim in the future. Members of the public are becoming increasingly aware of the dangers of identity theft but often the point of data compromise is unknown, which makes it very difficult to guard against the dangers and for consumers to fully protect themselves. What we can do, however, is to learn more about how and why fraudsters target their victims and to understand whether having certain attributes makes somebody more or less likely to fall victim to identity fraud.

By conducting this research, it has been possible to learn a lot more about the victims of identity fraud. When it comes to assessing the likelihood of company directors being targeted by identity fraudsters, we can now say with some certainty, and substantiated by \the evidence, that this is the case. With open source information readily available, an established credit history and associated wealth, company directors are a target for identity fraudsters: 1 in 5 victims were company directors in the three and a half year period explored here. It is important that company directors recognise their risk and are able to limit the amount of information that can be gleaned by fraudsters. The risk may never be eradicated, but targeted awareness could help these individuals keep themselves safe.

There are certain individuals, however, for whom the risk is lowered. Individuals with poor credit (for example those with bankruptcy records and CCJs) are generally less likely to be targeted, although this certainly doesn't mean that the risk is non-existent. To save time and effort, some identity fraudsters still favour a more 'scattergun' approach, firing off huge amounts of applications for as many identities as they have, regardless of whether or not these individuals are likely to be credit worthy. The idea is that if the fraudster has access to hundreds of identities and sends off hundreds of applications, the likelihood is that they'll get some which are successful, which saves them the need to spend time investigating and building up more credit worthy identities. Individuals should always ensure that they keep a close eye on their credit files, which could hold the first clues to having been impersonated. Even if the individuals in question do not think that they are a viable target, the results show that as 2% of impersonated individuals in the three and a half year period have a CCJ, it is always better to be safe than sorry.

6. Recommendations

Despite the varying methods used by identity fraudsters, there are still some key points which can be taken away from this research and which can be used as pointers to help both consumers and organisations guard against identity fraud in more effective ways.

Targeted awareness

Although it has been shown that anybody can become a victim of identity fraud, there are clearly some individuals who are much more likely to be targeted. Company directors and individuals who live in more expensive properties (based on tax bandings) have a certain display of wealth that allows fraudsters to recognise and take advantage of them. More targeted awareness campaigns could be really useful in educating those who are not necessarily defined as 'vulnerable' but are much more exposed to impersonation than other types of individual. There is clearly an opportunity to engage with those bodies that represent and communicate with these groups, in order to ensure that messages that resonate are delivered directly to those that need them.

Look for patterns and similarities

When an identity fraudster discovers an identity that they go on to have a certain amount of success with, it's not uncommon for them to recycle it for as long as it is useful to them. In this report, it was discovered that 16% of individuals had been impersonated more than once over the three and a half year period, highlighting the continued value of organisations checking identities against confirmed fraud databases. Additionally, though, organisations can also check for multiple applications in different victims' names but with repeated use of other pieces of information - for example, screening the contact information provided on applications - in order to help prevent some of the frauds that affect the 84% of impersonation victims whose name is only used once.

Take extra pre-cautionary steps to identify higher risk individuals

There are sections of the population who are impersonated more frequently than others. Identity management procedures should factor these characteristics into their risk scoring to identify heightened relationship risk: for example, by digitally on-boarding a new customer with a step-up authentication approach. The identity verification stage can identify those who are company directors, then adopt an extra level of authentication to further mitigate identity fraud risk.

Intelligent use of data to target investigations

The findings in this report have highlighted criteria more or less common with those that have been victims of impersonation. By extension, where applications have been referred for further investigation then investigation tools that draw in additional data sources can help organisations queue and prioritise cases based on whether their applicant possesses those criteria that may indicate a higher likelihood of impersonation. For example, a loan provider may choose to prioritise investigating a referral where the applicant is a company director, aged 31-40 and living in a property in tax band F. It must always be recognised, though, that fitting these criteria will never be enough, on its own, to be the sole indicator of impersonation.

Limit unnecessary publicly available information

For certain individuals, such as company directors, there will always be more publicly available information about them compared with other individuals. By owning a company, for example, the details of company directors will always unavoidably be listed on open registers and where this data is available, fraudsters will take advantage. Individuals can make things more difficult for fraudsters by limiting what personal information is available about them - such as not disclosing their home address - not only on these registers but also in other areas such as social media websites and/or professional networking sites. The more pieces of the puzzle the fraudster can get hold of, the easier it will be for them to build up a complete picture of the individual that they are targeting.

Check your credit file

A quick and easy piece of advice to consumers would be to 'always keep a close eye on your credit file'. This research has found that irrespective of an individual's credit history, fraudsters will sometimes access a victim's credit file first before applying for anything further to see if it's an identity worth utilising. By keeping a close eye on their own credit file, consumers are more likely to spot any suspicious activity before the fraudster causes too much damage.

lexisnexis.com/risk/tracesmart

www.cifas.org.uk

LexisNexis® RISK SOLUTIONS

cifas Leaders in fraud prevention

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions is a leader in providing essential information that helps customers across all industries and government assess, predict, and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information and analytics for professional and business customers across industries.

About Cifas

Cifas aims to make the UK a safer place to do business, by enabling organisations in every sector to prevent fraud and protect the public through the sharing of confirmed fraud data. Cifas is a not-for-profit organisation and has almost 400 members spanning the public and private sectors. In 2016 alone, Cifas members prevented over £1 billion of avoidable fraud losses by using Cifas databases. Cifas also offers Protective Registration for individuals whose identities are at risk of being used fraudulently, for instance after a burglary.
In 2014, Cifas launched a scheme called Protecting the Vulnerable. This service is offered free of charge to local authorities to protect those under the care of Court Deputies who are unable to access financial products and whose identities may be at risk.