HILL DICKINSON | cifas

Leaders in fraud prevention

FRAUD REPORT 2015

ABOUT THIS REPORT

This report is a collaboration between Cifas and Hill Dickinson LLP, undertaken in order to develop a better understanding of the different types of fraud experienced by the insurance sector. By undertaking a series of comprehensive data matching exercises and analysing data on confirmed fraudsters involved in high level insurance claim fraud, our research has helped to deepen our understanding of the links to other criminality, and the nature and chronology of fraudulent activity both within and outside the insurance sector. It also provides insight into the demographics of insurance fraudsters and offers practical tips to help the insurance industry combat fraud.

Further information about the methodology used for this report can be found on page 18.

CONTENTS

ABOUT CIFAS

Cifas aims to make the UK a safer place to do business. For more than 27 years, Cifas has worked to prevent fraud 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 with over 300 members spanning the public and private sectors, including insurance, banking, grant giving, credit card, asset finance, online retail, telecommunications, vetting and contact centres. In 2014 alone, Cifas members prevented over £1 billion of avoidable fraud losses by using Cifas' National Fraud Database, which records confirmed fraud cases. Cifas works closely with law enforcement and runs a number of insurance specific working parties and groups, regularly undertaking research to explore fraud links between different UK industries.

Cifas offers Protective Registration for individuals whose identities are at risk of being used fraudulently. In 2014, Cifas launched a new 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.

ABOUT HILL DICKINSON

Hill Dickinson LLP is an award-winning international commercial law firm, offering advice and delivering strategic guidance spanning the full legal spectrum. Insurance is key to the Hill Dickinson business and its Counter Fraud Group provides cradle-to-grave counter-fraud services to the insurance industry, Lloyd's syndicates, passenger transport companies, self-drive hire companies and self-insured corporates. Hill Dickinson advises on all aspects of insurance fraud and has specialist teams dedicated to managing pre-litigated and litigated claims.

Effective deployment of intelligence is at the core of our approach to the prevention, detection and management of insurance fraud. Netfoil, Hill Dickinson's in-house counter-fraud intelligence database, is the largest privately owned relational claims database in Europe. It holds over 220 million claims records relating to approximately 12.5 million insurance claims; 150,000 new records are added every month. Across 12+ years of claims fraud management, Hill Dickinson has developed a further dataset, derived from Netfoil, called Netfoil ACE. Whilst Netfoil captures all claims, Netfoil ACE relates exclusively to proven fraud claims and the fraudsters behind them.

Netfoil ACE claim typologies can include, but are not limited to, organised 'crash-for-cash' fraud incorporating staged and induced motor accidents - through to the more opportunistic end of the fraud spectrum, such as the submission of a fraudulent claim for, or as, a 'phantom passenger' in a motor accident. Each claim and person within the dataset must pass through a series of rigorous tests, ensuring that the subjects contained within are unequivocally complicit in fraudulent activities. A lawyer with conduct of a claim may make a submission for an individual to be added to the Netfoil ACE dataset when they believe the individual and the circumstances meet clearly defined criteria; an example of which includes a judge making a finding of fraud or fundamental dishonesty at a trial.

FOREWORD

Fraud is never a victimless crime. Fraud can range from opportunistic behaviours; the chance to exaggerate an incident, right through to a conspiracy to completely fabricate an 'accident'. At the most serious end of the spectrum, the insurance industry has long known that crash-for-cash claims are repeatedly perpetrated by organised gangs, recruiting participants and carrying out claims fraud on an industrial scale.

The links between organised fraudsters operating in insurance and those operating in other sectors are less well-established. Previous research has shown that fraudsters do not target a single industry and the results of this study reinforce this fact, demonstrating that the links are more ingrained and prolific than previously imagined. One third of the Hill Dickinson claims that originally appeared to be isolated insurance fraud matched to one or more cases on the Cifas National Fraud Database.

These findings set motor insurance claim fraud into a much wider criminal context – beyond the insurance sector and into networks of fraudulent activity across sectors, geographical boundaries and products. For example, the results of the data match carried out between Cifas and Hill Dickinson highlight solid connections, sometimes spanning many years, between insurance claim fraud and activity including money laundering and identity theft. The case studies unearthed by our research reveal vast networks, sometimes connecting individuals through a phone number or email address, spanning multiple sectors and fraud types. One individual is linked to more than 30 fraud cases, targeting banking and individuals, as well as insurance.

We have also found evidence that insurance claim fraud acts as a gateway fraud. Intelligence analysis suggests that young people are firstly carrying out insurance fraud before moving on to other forms of financial crime, including activities such as money laundering.

Insurance claim fraudsters do not work in silos, preferring the flexibility to exploit any weaknesses they can identify in the industry's counter-fraud defences. Conversely, the typical insurer operating model has inadvertently been built in silos around lines of business which are then further fragmented to reflect the specific insurance offering, such as motor, home, fleet or other lines. Insurers recognise that, to detect and prevent the organised, serial and opportunistic claim fraudsters targeting their organisations, they require a joined-up overview of their individual claims exposure combined with access to cross-industry claims data. There is increasing collaboration on industry counter-fraud strategies – a trend which is expected to continue – and the sharing of proven fraud data is already paying dividends.

These are welcome steps. This report is a reminder of the role that cross-sector collaboration has to play in combatting fraud. As fraudsters' networks and collaborations grow ever closer and interlinked, so too must our efforts to combat the problem.

Mike Haley
Deputy chief executive, Cifas

Peter Oakes
Head of fraud, Hill Dickinson LLP

KEY FINDINGS

Hill Dickinson released a date-specific data sample incorporating 618 proven fraud claims, involving 5,400 records related to 2,307 individual known fraudsters, from its Netfoil ACE database. This data has been cross-matched with 2,047,043 cross-sector confirmed fraud records held by Cifas. The key findings across the matching cases were:

1

Insurance fraudsters are committing fraud across a range of sectors

- The data match carried out between Cifas and Hill Dickinson shows that fraudsters perpetrating or involved in insurance fraud are highly likely to be involved in other types of fraud, from low level first party fraud such as application fraud, to higher level fraud indicative of serious organised crime, such as money laundering.
- 32% of false claims on motor insurance were made by individuals who were also found to be involved in other types of fraudulent activity.
- Of the matches, the vast majority (82%) were on fraud against other sectors than insurance, underlining the need to take a cross-sector approach to fraud prevention.

2

Involvement in insurance fraud often acts as a gateway to other types of fraud.

- 69% of the individuals found to be involved in both motor insurance claim fraud and other types of fraud committed the insurance fraud first. This suggests that involvement in insurance fraud acts for many as a gateway into other types of fraud, including money laundering, and underlines the importance of sharing data across sectors to catch fraud early and prevent further crime.
- The remaining individuals (31%) involved in both insurance claim fraud and other forms of fraud committed the other fraud first, showing that the sharing of cross-sector data could have alerted insurance fraud investigators to the fraud risk at an early stage.
- Individuals involved in motor insurance claim fraud were four times as likely to be involved in other types of fraud when compared to individuals who have made a genuine claim.

3

There are strong links between insurance fraud and serious organised crime

- 42% of matches were on activity indicative of money laundering. In particular, there was a high volume of cases matching, where the same individual committing insurance claim fraud was found to be connected to an account that had received illicit funds. This kind of activity can be linked to organised criminality, including mule herding, where numerous individuals are recruited to create networks through which the proceeds of crime can be laundered.
- 34% of matches occurred where the same individual carrying out insurance claim fraud was involved in application fraud. 49% of application fraud matches occurred where the same individual involved in insurance claim fraud also made a fraudulent application for motor insurance, indicating planned activity across the different stages of insurance fraud.
- Organised criminals are implicated in targeting common addresses to recruit those who are unable to work legally into roles in large scale insurance frauds.

4

Fraudsters demonstrate geographical mobility

- The data match carried out in this study found that fraud cases are linked across the country. Not only are some individuals involved in frauds at multiple addresses in the same region, many are linked to frauds in other cities. There is marked movement between London, Manchester, Birmingham, Nottingham and Sheffield, with the links particularly prominent from Manchester to Birmingham, as well as those between smaller cities, such as from Wolverhampton to Derby.

5

Complex fraud rings will escape detection without complete datasets

- When detecting fraud, many companies focus their matching on comparatively simple name and address based matches. However 11% of the matches in this study were due to common contact details used in both the insurance fraud case and the Cifas case. While it is not surprising that people will provide the same telephone or email address to multiple organisations, it is notable that 8% of matches were due to the matching of one or more common contact details alone - the names and/or addresses were not the same.
- This implies that there were a number of individuals involved in multiple frauds who were deliberately utilising different names, birth dates and/or addresses but a common mobile phone and/or email address in the details provided to the insurer.
- This highlights the importance of intelligent data matching techniques when investigating possible fraudulent activity. If searching only matches to the same name, date of birth and address, previous fraudulent activity can be missed and organised fraud rings are more likely to go undetected.

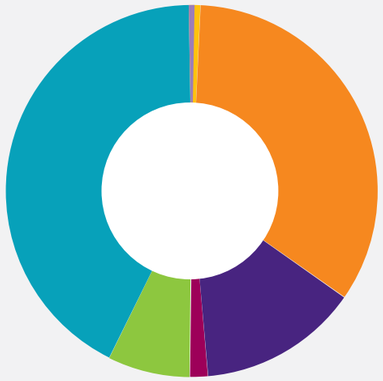
The main data matching exercise found a strong synergy between the data sets with 196 of the Hill Dickinson cases matching details within 347 Cifas National Fraud Database cases; equating to 1.8 Cifas cases returned for each matching Hill Dickinson case. This demonstrates a persistent fraud threat where individuals involved in insurance fraud were often involved in more than one other fraud case.

The 196 matches covered a number of different fraud types, detailed in the next section of this report.

Subsequent data matches using differing time periods were then carried out to ensure that the results of the main data match could be put into context and any anomalies accounted for. A detailed methodology is on page 18.

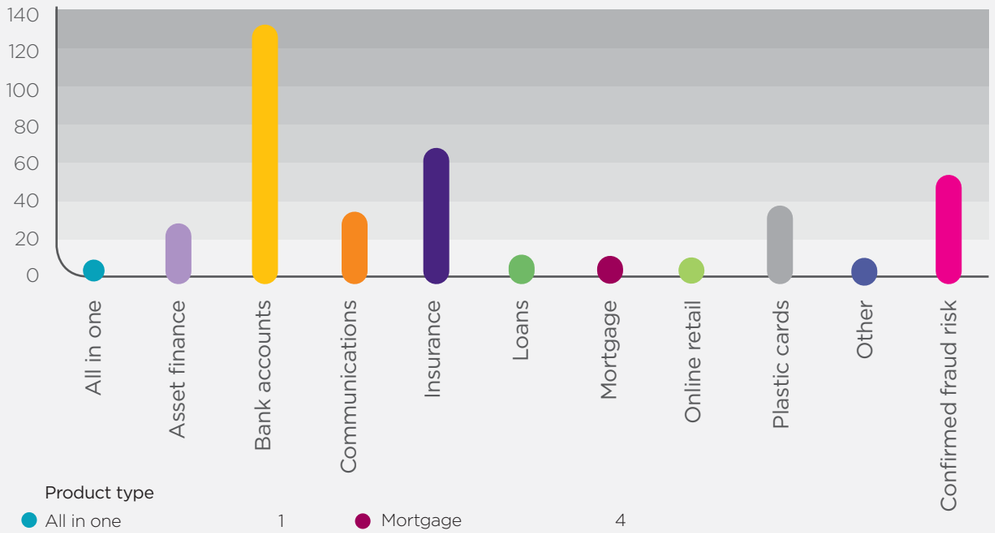
IN DEPTH:
UNDERSTANDING THE MATCHES

CHART 1 MATCHED CIFAS CASES BY FRAUD TYPE



Match type	
Asset conversion	0.6%
Application fraud	34.3%
Confirmed fraud risk	13.8%
False insurance claim	1.4%
Identity fraud	7.2%
Protective registration	0.3%
Misuse of facility fraud	42.4%

CHART 2 MATCHED CIFAS CASES BY PRODUCT TYPE



Product type			
All in one	1	Mortgage	4
Asset finance	24	Online retail	2
Bank accounts	128	Plastic cards	33
Communications	30	Other	5
Insurance	63	Confirmed fraud risk	49
Loans	8		

Cifas fraud types – definitions

Asset conversion
The unlawful sale of an asset subject to a credit agreement – for example where a person has bought a car on finance and sold it on before paying it off.

Application fraud
When an application for a product or service has been made with material falsehoods (lies) using false supporting documentation (but where the name provided has not been identified as false).

Confirmed fraud risk
A record that has been confirmed to the Cifas standard of proof and represents a risk of fraud to the membership.

False insurance claims
False insurance claims occur when an insurance claim, or supporting documentation, contains material falsehoods (lies).

Identity fraud
When a fraudster abuses personal data or identity details in order to impersonate an innocent party, or creates a fictitious identity, in order to open a new account or take out a new product.

Protective registration
Victims of a fraud or crime who suffer the loss or theft of personal identification details may seek to have these identification details registered with Cifas. Protective registrations are not records of actual or attempted fraud, but act as precautionary measures for individuals who believe that their identity/details are at risk.

Misuse of facility fraud
The misuse of an account, policy or product, such as paying in an altered cheque or knowingly making a payment that will bounce, but where the identity/owner has not been identified as false.

IN DEPTH:
UNDERSTANDING THE MATCHES

Money laundering and insurance claim fraud: understanding the misuse of facility fraud matches

Almost half of the matching cases (42%) were misuse of facility frauds. These kinds of frauds occur when individuals use their own identities to fraudulently abuse facilities, such as bank accounts, retail accounts, mobile phone contracts or other financial facilities.

The highest proportion (37%) of these matching cases involved the misuse of bank accounts. The majority of these cases occurred where individuals have received illicit funds into their accounts – activity which is highly indicative of money laundering.

Money laundering can occur as either a one-off event or as part of a much larger operation: at one end of the spectrum there are individuals acting for their own gain, while at the other, there are sophisticated and serious organised criminal networks.

Looking at the data, the implication is that those involved in motor insurance fraud (although unsuccessfully in these cases) are also organised enough to have processes in place to launder the proceeds of crime in order to hide them from any investigation. This suggests a level of sophistication beyond the 'opportunist', with money mules (see insert on page 10) being used by organised criminals to wash the proceeds of serious criminal offences (see case study 2, page 13).

IN DEPTH:
UNDERSTANDING THE MATCHES

WHAT ARE MONEY MULES?

The term 'money mule' is most commonly used to describe an individual who allows their bank account to be used to facilitate the movement of criminal funds. The mule either knowingly helps, or is tricked, into moving money through their account and then to a third party, who is often located in another country. Acting as a mule, however, is illegal. And the law does not accept ignorance as a defence. Current regulation and legislation requires banks and other financial institutions to report any suspicion of money laundering and close accounts used in that way.

Further targeted intelligence analysis in this area may be able to shed more light on the extent and range of such cases, along with the associated threats.

Misuse of facility involving mobile phones often occurs when an individual commits to a mobile phone contract that they never intended to honour in order to obtain a high value phone. Online retail fraud occurs when fraudsters order goods online, the goods arrive but the fraudster never pays for them or says they never received them. The objective behind these types of misuse of facility fraud is the same – to obtain a tangible product without any genuine intention to pay for it.

Organised crime has been linked to these frauds, particularly where high quality goods such as new phones are involved. Criminals are practised at recruiting people to obtain items in exchange for cash. It is attractive to organised criminals as they are distanced from the fraud (in these cases the fraud is committed in the account holder's name) and their 'mules' are likely to be approved because their identity is genuine and history may not give rise to any specific concerns.

The matches in this category suggest that organised criminals may be perpetrating multiple frauds across a number of sectors – insurance, communications, retail and finance. Without analysing data across sectors, the extent and nature of their fraudulent activity would remain undetected.

Fraud committed at every stage of the insurance pathway: understanding the application fraud matches

34% of the matches between insurance claim frauds and Cifas data were in application fraud cases. These frauds occur when individuals using their own identity make a fraudulent application for a product or service – including fraudulent applications for motor insurance, bank accounts, credit cards and asset finance. Typically the fraudster in these cases has provided false details during the application process; this will vary according to the product being requested but typically includes address history, employment details or history relating to previous claims.

Across all categories, the majority of matches (82%) were in sectors outside of insurance. However, the most common application fraud matches occurred where the same individual involved in an insurance claim fraud also made a fraudulent application for motor insurance. This happened in 49% of application fraud match cases (58 cases) and demonstrates that fraudulent activity across the different stages of insurance fraud is linked. The same individuals that are making fraudulent applications for motor insurance are also making fraudulent claims.

Of those involved in both insurance claim fraud and motor insurance application fraud, more than half (55%) were successful in their application for motor insurance. With staged accidents frequently costing insurers upward of £20,000[1] this shows that a considerable amount of fraud might be prevented through improved fraud controls when policies are first set up. The planned nature of the activity suggests that many fraudsters are carrying these frauds out in an organised way in order to gain financial benefit at every stage, rather than being solely perpetrated by more opportunistic fraudsters looking to make quick cash. The data match also found that 7% of the matches on application frauds were with applications for asset finance. This is more than double the prevalence of asset finance frauds in the Cifas database as a whole, with fraudulent applications for asset finance making up just 3% of the National Fraud Database.

1. Estimates from Hill Dickinson's claims fraud handling analysis.

This points to organised operations: the same individuals that are fraudulently making motor insurance claims are connected to fraudulent insurance applications, as well as fraudulently obtaining a vehicle on finance. Better use of data at each stage of this pathway could make a significant impact on fraud reduction.

Organised fraudsters targeting common addresses: understanding the confirmed fraud risk matches

Confirmed fraud risk records include:

- False document records, such as fake passports or driving licences: provided by the Metropolitan Police Amberhill team;
- Home Office immigration records: cases where the individual has absconded or has overstayed illegally and is no longer able to open a UK bank account legally;
- Deceased data: GRO data used to prevent fraudsters abusing the identities of deceased individuals; and
- Fraudulent Royal Mail redirections: a confirmed enabler for identity fraud.

In total, 14% of the matches were against confirmed fraud risk cases. The dataset with the highest match rate was the Home Office immigration data.

Home Office immigration matches

The Home Office reports cases of illegal overstayers and absconders to the Cifas National Fraud Database in order to prevent these individuals from obtaining access to products and services which they are not entitled to receive.[2] In this data matching exercise, 9% (31) of matched Cifas cases were Home Office immigration confirmed fraud risk cases.

2. The Immigration Act 2014

A large proportion of the matches relating to Home Office immigration data are address based, where the individuals share (or have once shared) common addresses and temporary accommodation. The occurrence of multiple insurance claim frauds occurring at the same address is synonymous with the more serious and organised part of the fraud spectrum. Illegal overstayers are likely to find it difficult to obtain legal employment, making them potential targets for organised criminals to attempt to engage them in criminal activity, for example, to fulfil passenger and third party claimant roles in large scale insurance frauds.

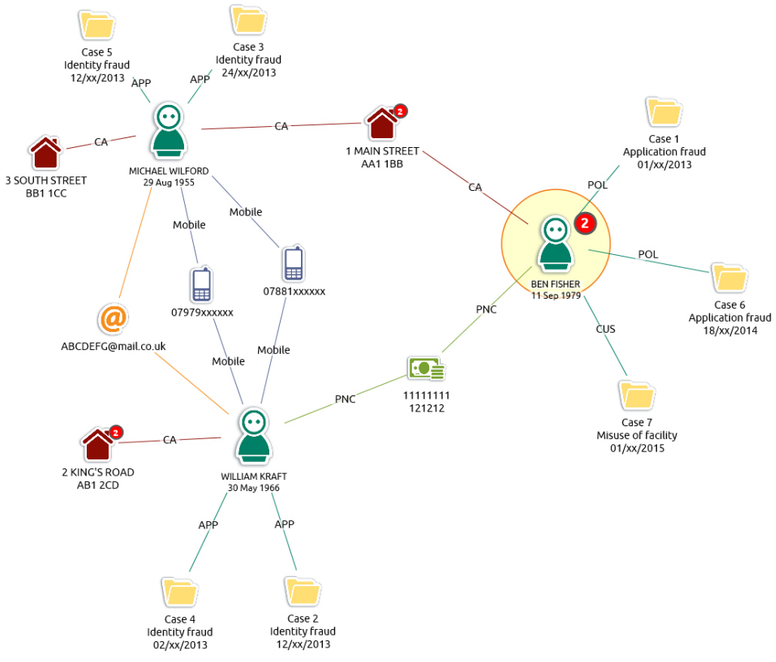
Metropolitan Police Amberhill law enforcement alerts

The Metropolitan Police Amberhill team supplies Cifas with regular alerts relating to false or fraudulently obtained genuine documentation which they know has been produced and issued, such as passports, driving licences and other identity documentation. Cifas records these as confirmed fraud risk cases for the purpose of alerting Cifas users to false documentation, which could be supplied as a proof of ID when an individual fraudulently applies for a product or service. In this data matching exercise, 4% of the returned Cifas cases were Amberhill alerts (12 cases). While the match rates are slightly lower for these cases than for other types, it is notable due to overt criminality of obtaining of false and fraudulent documents to facilitate crime. Although a small number, the individuals involved in the insurance frauds have either used a false document or are connected to an address where a false document is known to have been issued.

Identity fraud and other matches

There were a small number of matches to other Cifas categories, including identity fraud, false insurance claims, asset conversion and protective registration. The matches in these categories did not reveal any significant trends. 7% (25 cases) matched to Cifas identity fraud cases. With identity fraud making up 50% of the Cifas database as a whole, this is a relatively small match rate. This is indicative that claims fraud typically needs to involve real people on both sides and this is something the industry can exploit as part of its counter-fraud strategy. Further investigation into some of the cases revealed that identity theft can, however, play a role in the wider fraud network. This is explored in the case studies in the following section.

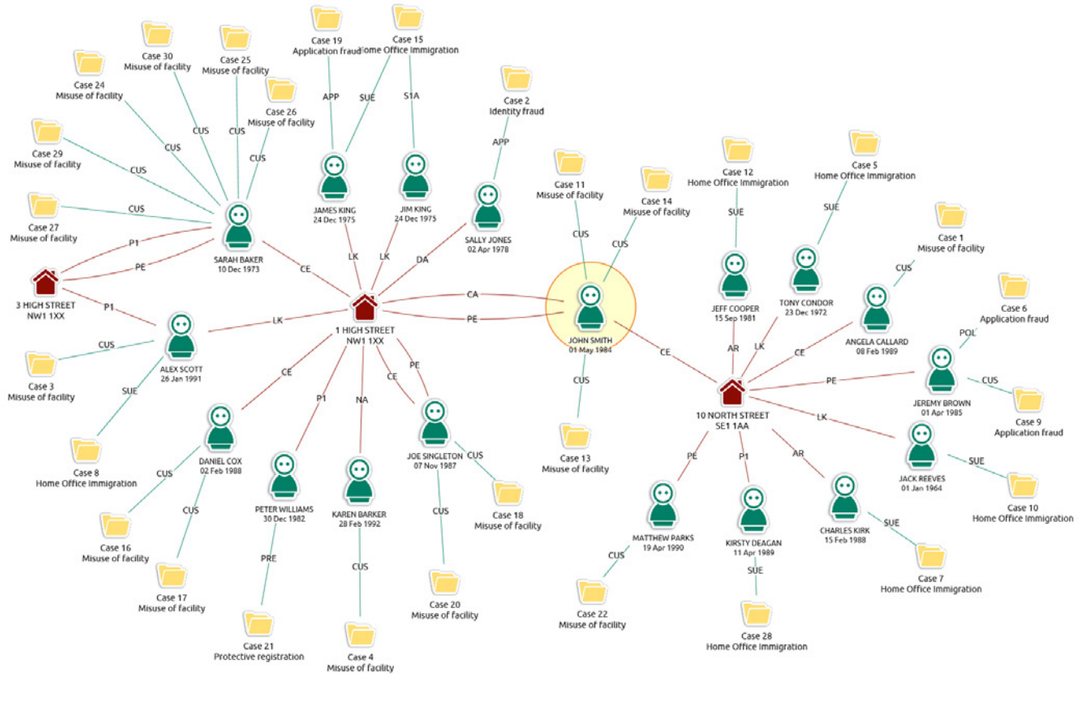
CASE STUDIES



Case Study 1*

- The above network shows the Cifas cases associated with the highlighted subject 'Ben Fisher', the claimant in a Hill Dickinson case in April 2013. Following the Hill Dickinson incident, Ben Fisher was later recorded in the Cifas National Fraud database three times; twice for insurance application fraud in May 2013 and August 2014 (for failing to disclose previous claims) and the misuse of a home media contract in May 2015. The fraudulent application made in May 2013 was for motor insurance and Fisher failed to disclose three previous claims (and subsequently could not provide any supporting proof for his no claims discount), which indicates that the false Hill Dickinson claim was not the first that this individual had been involved in. In August 2014, the individual tried to obtain motor insurance again, but still failed to disclose any of his previous claims.
- This individual was applying for various products and services over a two year period, but was probably aware that he was not going to be granted credit facilities in his own name due to his previous fraudulent activity. Looking at the network, it becomes apparent that he used the identities of innocent victims in order to attempt to gain credit (either a personal loan or personal credit card) between July and August 2013. Interestingly, the only thing linking Ben Fisher and one victim, 'Michael Wilford', was an address provided by Fisher. In another case, the details linking Fisher with the second victim, 'William Kraft', were the bank details, again provided by Fisher. The final piece of the puzzle is the contact details shared between the two victims; the telephone numbers and email address. Each has a different address, so it is highly unlikely that there would be a legitimate reason for two separate individuals living in different areas to be sharing mobile phones and email addresses, unless they were the unfortunate victims of identity theft.
- This network highlights the varying nature of fraud carried out by a single individual. Fisher clearly committed further fraud to hide previous frauds (failing to declare the likes of previous insurance claims), but crucially, perpetrated some much more sinister forms of crime, namely the theft of two identities, in order to gain credit. Cross-sector data sharing allows us to see not just an individual who was involved in fraudulent insurance claims, but also an identity fraudster who might have otherwise gone undetected.

* All names have been changed and anonymised. Any resemblance to real persons, living or dead, is purely coincidental.



Case Study 2*

- The subject highlighted in the above chart, 'John Smith', was the claimant in a Hill Dickinson insurance fraud case in December 2012. The chart highlights the associated fraud that this individual and associates were also involved in before, during and after the time when the Hill Dickinson fraud was recorded.
- The three frauds associated with John Smith were all misuse of facility frauds carried out between January and March 2014 on various different products at two different addresses: regular payment fraud on a personal credit card; retaining wrongful credit on a personal current account; and the evasion of payment for a mobile phone contract. The case involving a current account used to retain wrongful credit occurred because John Smith had set up a false company purporting to offer loans and scamming individuals. The account was used to collect advance fees from individuals who thought that they were obtaining a genuine loan by paying a small amount up front. This is known as 'advance fee fraud'. It is carried out by individuals who prey on innocent (often vulnerable) victims, indicating a high level of organised criminality.
- Between January 2012 and January 2014, a number of frauds were carried out at both the '1 High Street' and '10 North Street' addresses, ranging from the misuse of bank accounts, fraudulent applications for motor insurance and included a number of individuals recorded within Home Office immigration cases. Following the frauds committed by John Smith, the '1 High Street' address becomes much more prolific, particularly for frauds involving the misuse of bank accounts or plastic cards. The high numbers of individuals at a single address misusing their bank accounts in this way (by paying in false instruments) provides evidence that illicit funds are being laundered through multiple accounts.
- The organised element of this network is demonstrated by the inclusion of an identity fraud related case. In early 2012, an identity fraud case ('Sally Jones') was reported. Her identity had been stolen and used to order goods online with the delivery address listed as the '1 High Street' address. This shows that '1 High Street' is very likely to be the address at which the fraudster resides or has access in order to pick up deliveries. Much later, in March 2015, an individual living elsewhere who *used* to live at 1 High Street ('Peter Williams') at the time of some of these other frauds took out a protective registration with Cifas as he believed himself to be at risk of identity fraud. It is likely that these events are related and the individual was aware of the fraud going on at his previous address and sought to protect himself from falling victim to these criminals.

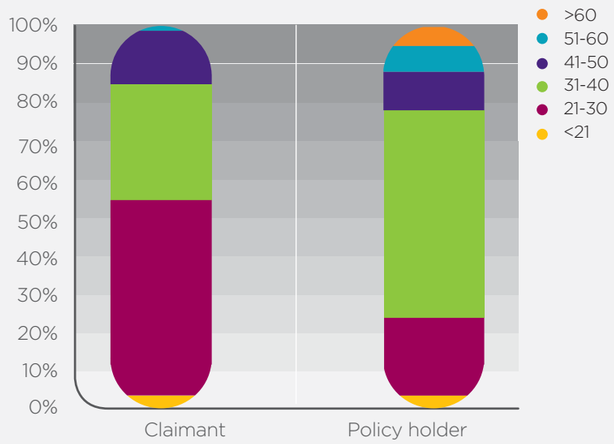
* All names have been changed and anonymised. Any resemblance to real persons, living or dead, is purely coincidental.

UNDERSTANDING THE DEMOGRAPHICS

AGE DIFFERENCES

Successful insurance fraud can involve a number of different roles. Chart 3 highlights the differences in age of individuals who undertook one of two particular roles in the fraud: either the claimant or policyholder. Older fraudsters appear to take on the role of policyholder, often because they can more easily obtain insurance and generally speaking it is cheaper, reducing the costs of setting up a fraud.

CHART 3 PROPORTIONS OF HILL DICKINSON CLAIMANTS AND POLICYHOLDERS, SPLIT BY AGE GROUP



At the other end of the spectrum are the younger members of the group, often featured as claimants.

This study did not examine the motivations or reasons behind why young people are involved in these frauds. However, previous research has found that for many younger individuals, criminal behaviour can be linked to their 'maturity of judgement' and that incentives (such as the promise of financial gain) can draw them into fraudulent activity. Studies have found that an individual's decision making processes are affected by cognitive and physiological development, which explains why younger individuals (particularly adolescents) can be more easily influenced and drawn into crime due to a lack of socially responsible decision making as a result of their age.[1]

By way of further context, Hill Dickinson has previously dealt with cases featuring gangs offering relatively modest up-front sums of money for the use of a person's ID for a staged/ contrived fraud claim. If the claim is successful, the gang retains the full pay out. This can also extend to serious coercion or indoctrination to a gang. Usually, in the claims space, this type of fraud is driven by a rogue claims and accident management firm who typically stand to benefit the most financially.

Of the individuals in the matched Cifas cases, 39% were between 21-30 years old and 39% were between 31-40 years old. Differences start to appear once the actual types of fraud are compared. Individuals in the 31-40 years age group were more likely to match on application fraud (38%), while those in the 21-30 age group were more likely to match on misuse of facility frauds (46%).

Older individuals are more prominent among matches on applying for goods and services. The reasons for this were not explored as part of this study, however this may be because fraudsters believe that older individuals are more likely to be granted insurance policies, asset finance agreements or other facilities, because of their age and associated 'credit worthy' attributes (for example, owning their own home or being married). For those matching frauds relating to asset finance products in particular, around 64% of the individuals involved were over the age of 30 years.

1. "(Im)maturity of Judgment in Adolescence: Why Adolescents May Be Less Culpable Than Adults", Elizabeth Cauffman and Laurence Steinberg, University of Pittsburgh, http://www.oja.state.ok.us/SAG%20Website/MacFound/(Im)maturity_of_Judgment_Article.pdf

CHART 4 PROPORTIONS OF INDIVIDUALS INVOLVED IN THE MAIN CIFAS CASE FRAUD TYPES, SPLIT BY AGE GROUP

GEOGRAPHICAL DIFFERENCES

The flow map shows the movement of fraud based on the addresses used by the fraudsters in the Hill Dickinson case to the addresses supplied in the matched Cifas cases (where the Hill Dickinson incident occurred prior to the recording of the Cifas cases). The red lines show links between these addresses; the stronger the red line, the greater the level of movement to that particular location on the map.

The most striking aspect of the map is the locations of the individuals within the Cifas cases (the 'brighter' end of the red line) which appear to be found within major cities. London is one of the major areas highlighted on the map, which is unsurprising due to the exceptionally high (and often transient) population of the city. Manchester, Birmingham, Nottingham and Sheffield are similarly prominent. There is marked movement between these cities, with the lines particularly prominent from Manchester to Birmingham, as well as those between smaller cities, such as from Wolverhampton to Derby.

Fraud often spans more than one address and these can be very different locations. Even the case study of 'John Smith' (page 13), who appears rather settled, used more than one address.

PRACTICAL APPLICATIONS

PRACTICAL APPLICATIONS FROM THIS RESEARCH

This collaborative study looked at a subset of insurance claim fraud data. The findings of this study suggest links between organised insurance fraud and other criminality. Practical applications from this study include:

Do not underestimate the importance of utilising cross-sector fraud data -

when investigating instances of insurance fraud, cross-sector confirmed fraud data can be exceptionally powerful. Of the insurance frauds matched in this exercise, 82% were to frauds carried out against a different sector, highlighting the intelligence that can be gained by organisations looking at data outside of their sector.

Search other data sources aligned to high fraud risk to help get the fullest picture possible -

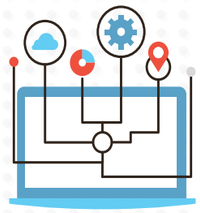
using extra data sources such as the possession of a false identity or the illegal obtaining of products or services by individuals who are not eligible to be in the country can help to identify fraud that otherwise goes undetected. Keep searching across different stages of the customer journey. Using fraud data at policy inception and claim stage is common but there is the potential for fraud to slip through at renewal (customers not making the insurer aware of changes in their circumstances) or mid-term adjustment.

Capture and maintain up to date accurate subject data -

capture data at each stage when subjects are in contact. Changes of address, bank details, additional drivers – it is important to retain historic as well as current data in these fields for all searching of fraud databases. For some of the intelligent data matching outlined to work, insurers and other businesses need to have captured the data in fields such as: mobile phone number, email address/es, bank details. It is also important to search all individuals involved – searching policy holders alone will not identify all frauds.

Utilise intelligent data matching -

fraudsters often change the details they use and methods by which they commit fraud. By using intelligent data matching techniques (i.e. not just name, date of birth, address) attempted fraud can be uncovered that otherwise goes undetected. 8% of matches in this exercise were as a result of matching on contact details alone; a worthwhile indicator for linking frauds where criminals often change their identities. This may require internal system changes so that this extra information is entered when cases are recorded and logged – be that to internal systems or to other external fraud prevention/ data sharing platforms.



Bank details may also provide vital links. Many of the insurance fraudsters in this study are also associated with money laundering cases, however the study did not match bank details. Adding financial details to search data is likely to increase the propensity to match an existing fraud case from another sector.

Geography is not a barrier to fraudsters -

although fraud levels are understandably highest in densely populated areas, the fact that the linked frauds span the whole country shows that fraudsters can (and will) utilise addresses across the country to commit fraud. Investigations cannot be constrained by geographic boundaries and investigators should look beyond the area where the fraudster is currently known to them.

ANNEX

Methodology – timelines and matching

Hill Dickinson extracted 5 years' worth of data from their Netfoil ACE dataset, which was searched against the Cifas National Fraud Database on 14 May 2015 (2,047,043 records were live on the NFD at this point in time, dating from January 2012). The Netfoil ACE dataset was then matched for a second time, but instead of using a search date of 14 May 2015, each entity was searched for at the recorded 'incident date' the date when the incident triggering the false insurance claim occurred. As the records on Cifas National Fraud Database change on a daily basis (as cases of fraud are added, deleted or expired), this method offered a snapshot of what links the entity had *at the time that the incident occurred*. This was important to include, as it would give much more information about the actions of the fraudsters prior to committing insurance fraud and whether anything could have been identified to indicate their involvement in the Hill Dickinson case which subsequently followed.

A third data matching exercise was undertaken, this time using a Hill Dickinson dataset (of a comparable size to the ACE dataset) known to consist solely of 'clean' data, i.e. there was nothing to indicate that any of the entities included in this dataset were fraudulent. This data was matched to establish a benchmark for the previous matching exercises and to provide context for the rate of matches returned, i.e. to identify to what extent the previous match rates differed from what would be considered 'normal'.

HILL DICKINSON | cifas
Leaders in fraud prevention

Printed October 2015