Home Office

The scale and drivers of attrition in reported fraud and cyber crime

Research Report 97

Dr Angie Scholes

June 2018

Acknowledgements

With thanks to the following: Samantha Dowling, Tom Bucke, Rob Street, Sam Brand, David Mair, Kari Davies, Anna Sanktjohanser, Steve Almond, Ian Caplan, Piers Harrison, David Silke, Tim France, Jon Williams, Laura Williams, Chris McKee, Jenny Allen, Detective Superintendent Matt Bradford, Detective Superintendent Pete O'Doherty, Jonathan Frost, Pauline Smith, Steve Proffitt, Professor Brian Francis, and Professor Matt Williams.

Also thanks to all those in police forces, and other organisations, who so willingly gave up their time to contribute to this project.

Contents

The views expressed in this report are those of the authors, not necessarily those of the Home Office (nor do they reflect Government policy).

Executive Summary

In 2013, following the centralisation of the reporting and recording of fraud and cyber-dependent crime to Action Fraud, concern arose about the level of attrition in these reports, and the low outcome rates police were reporting for these crimes. Between April and September 2013 (the period of study), 115,991 crimes were reported to Action Fraud. In the same period, the proportion of cases reported to Action Fraud that achieved an outcome was around 2%.[1] [2] This project was commissioned in order to establish overall attrition rates, to understand why attrition was happening, and to identify potential improvements in the process.

There were three phases to the analysis:

- First, quantitative analysis of over 3,000 cases reported to Action Fraud between April and September 2013.
- Second, quantitative analysis of a second sample of over 1,500 cases that were reported between April and September 2013, and disseminated to one of seven forces.
- Third, qualitative analysis of interviews and focus groups with Action Fraud and National Fraud Intelligence Bureau staff, police, and other stakeholders, to develop a deeper understanding of the process and the challenges.

Combined, the analysis showed four stages at which attrition occurs:

1. When reports are initially made to Action Fraud;

[1] This is based on the 9-outcome framework used by police. The 9 outcomes are charge / summons; adult caution; youth caution; Taken Into Consideration (TIC); Penalty notices for disorder (PND); the offender has died; cannabis warning (obviously not relevant to fraud); community resolution; prosecution not in the public interest (CPS).

[2] These outcome rates are calculated by comparing the total number of frauds and cyber-dependent crimes reported in this period, to the total number of outcomes assigned to fraud and cyber-dependent crimes in this same period. This is not a 'true' outcome rate (as that would be calculated by comparing outcomes assigned to offences that took place in the same period). However, as data are not yet available to calculate a 'true' outcome rate, this approach is the recommended one, to allow fraud to be compared to other crime types in a fair way, giving a general picture of outcomes.

2. In the scoring process that determines whether reports are reviewed by an NFIB Crime Reviewer;
3. At the point at which crimes are disseminated to law enforcement (and other agencies) for investigation and enforcement;
4. At the point at which law enforcement return outcomes to NFIB.

Drivers for attrition at each of these stages are set out and recommendations made for how they could be addressed.

Key Findings: The Stages of Attrition

Stage 1: Reporting to Action Fraud

At this stage, attrition occurs chiefly because of difficulties the general public, and some Action Fraud and police call handlers, have in completing the Action Fraud crime reporting form and providing good quality, reliable and timely information about the crime. Issues included:

- A lack of clarity on how to complete the reporting form;

- Some Action Fraud and police staff having a poor understanding of the overall process by which Action Fraud / NFIB / local police deal with reports of fraud and cyber-dependent crimes;

- Local forces not reporting crimes to Action Fraud promptly / at all; and

- Lack of functionality in the reporting tool, including an inability to update reports once they have been completed.

Thus it is possible that there are delays in making reports to Action Fraud, or even that Action Fraud do not receive reports at all. When reports are received they can be of varying quality, with missing or incomplete information. Resolving such issues could help to reduce attrition at this stage, and improve the quality of reports that reach the next stage, where they are reviewed by NFIB Crime Reviewers.

Stage 2: The Scoring Matrix and Manual Review criteria

Due to the volume of reports that Action Fraud receive, and the fact that not all reports will contain viable leads for investigation, it is not feasible for NFIB staff to look at every crime report. Instead two automated approaches are used to identify the cases that (in theory) are most likely to have viable lines for enquiry:

- A scoring matrix, which automatically scores crimes based on the presence or absence of certain information, such as suspect's bank account details, telephone number, or vehicle registration. Crimes with this information score higher than crimes without.

- Additional ‘manual review’ criteria, which the system uses to automatically identify any other cases that NFIB has determined should be reviewed. These are based on things such as level of monetary loss (any losses over £100k should be reviewed), or the type of crime reported (e.g. pension liberation fraud). These crimes are reviewed because of the potential severity of impact on the victim, and to develop the intelligence picture and support collaborative activity.

All crimes are automatically assessed according to the scoring matrix, and the manual review criteria. The system then flags any crime that meets either the scoring matrix threshold, or one (or more) of the manual review criteria, to NFIB to be reviewed by a Crime Reviewer. Crime Reviewers then decide whether to send the case to a local police force for further investigation/enforcement.

The findings at this stage suggest that this process is not working as well as intended. Looking at what gets to NFIB Crime Reviewers, it is evident that more crimes are getting through to them because the cases meet manual review criteria rather than because they meet the scoring matrix threshold.

In contrast, more of the crimes that are sent to police forces for further investigation tend to have met the scoring matrix threshold rather than the manual review criteria.

This suggests that the scoring matrix is far ‘better’ at identifying viable crimes than the manual review criteria, and that Crime Reviewers are spending considerable amounts of time working on crimes that will not actually be sent out to a police force for further investigation. From an attrition perspective, improving the SM and manual review criteria would be beneficial, so that Crime Reviewers can focus their limited resources on cases that are more likely to be disseminated, and therefore generate a criminal justice outcome.

Stage 3: Dissemination of crimes to local police forces (and others) for enforcement

The third stage of attrition is the point at which cases are disseminated to local forces, and others such as Trading Standards, for investigation and enforcement. A number of issues contribute to attrition at this stage:

- Confusion in police forces about who is responsible for investigating these crimes;

- Concerns about the quality of the case information that is disseminated;

- The amount of case information that is disseminated, and the risk that there are so many crimes they are unmanageable for forces;

- The speed of the dissemination, with older crimes being perceived as being more difficult to investigate;

- A lack of recording non-Criminal Justice outcomes (such as police forces visiting victims to provide reassurance, even when cases cannot be investigated);

- The need to double-key[3] disseminated cases onto force systems, and there sometimes being limited resources to do this, resulting in delays in progressing cases; and

- A lack of clarity around how inter-force cooperation should work, when cases cross force boundaries (e.g. witnesses being located in Force A, when Force B is conducting the investigation).

As a consequence of these issues there is attrition, either because crimes are not investigated, or if they are because delays in the process affect the police's ability to achieve an outcome. Making improvements in these areas should increase the number of crimes investigated by local forces, and others, therefore reducing attrition.

Stage 4: Crimes being investigated by, and receiving an outcome from, local police forces

The final stage at which attrition was identified was the point at which crimes achieve an outcome (or not) and whether that outcome information is returned to NFIB. The main issue at this stage is that, at the point at which the analysis was done, many forces were not returning outcome information on a regular and consistent basis. In addition, where cases were sent to other agencies, such as Trading Standards, there is no protocol by which any successful outcomes can be returned to NFIB, so those successes cannot be reflected in outcome rates.

Underpinning the findings from police forces in the sample in particular is the suggestion that in many forces fraud is not a high priority, with some respondents reporting reductions in staffing in their own teams, and expectations of further reductions. Perhaps understandably, other crimes take a higher priority, e.g. more 'serious' crimes such as child sexual exploitation, and crimes *perceived* by officers to have a greater impact on the victim, e.g. burglary. However, research (e.g. Sentencing Council, 2013) has shown that victims of (online) fraud can experience a number of 'soft' impacts, such as emotional and psychological issues, fear of physical threats, physical health problems, and damage to relationships.

[3] Double-keying refers to the process by which police forces have to record cases on their own systems, as well on the Action Fraud / NFIB systems. For example, when reports are made direct to police they have to record them on their own Crime Management Systems and then 'double-key' them onto the Action Fraud system.

Attrition could be reduced at this stage by increasing the number of forces that consistently provide good quality outcomes data, and also by identifying ways that positive outcomes from other organisations (such as Trading Standards) can be reflected in this.

Some other notable findings arose from this work, and whilst not directly related to attrition, they were still important to Action Fraud / NFIB operations and processes:

- Issues in the ways that vulnerability can be identified (and should be defined) in victims, and how those victims are / should be dealt with.

- Challenges NFIB have around data management, for example in knowing where on their system data is recorded.

Themes of the findings

The findings at each stage of attrition, and the findings related to vulnerable victims and NFIB's data management, can be summarised into three 'themes':

1. Accurate and timely recording of information

The accurate and timely recording of data, decisions and other key information is critical to an accurate understanding of the scale of reported fraud and cyber-dependent crimes, and associated outcome rates. Issues recording information were identified across all four stages of attrition, such as:

- Crime reports;
- Decisions taken by NFIB Crime Reviewers;
- Disseminations (date, force, etc); and
- Outcomes.

An example of this theme at the first stage of attrition is the finding that Action Fraud call handlers and the general public did not always know how best to complete the reporting tool. This was evidenced in the quantitative data (via missing data, and data entered in the wrong fields), and confirmed in focus groups with Action Fraud call handlers. If information is not recorded correctly in the first place, the automated Scoring Matrix may 'miss' cases that otherwise would have met the threshold. Similarly, the Manual Review criteria may be met, but if the information is not recorded correctly the system may not identify cases as such. These cases therefore did not reach Crime Reviewers, thereby increasing attrition.

2. Understanding roles and responsibilities

For the whole process (from reporting to outcomes) to work smoothly, all parties (Action Fraud, NFIB, police, other stakeholders) need to have a clear understanding of their own roles and responsibilities, as well as knowledge of how other parts of the system works. However, findings from all stages showed a common theme – a lack of understanding by police and Action Fraud staff of their role in the wider process, through to staff in police forces understanding their responsibility to return outcome information to NFIB.

An illustration of this problem came from interviews with staff and officers in local forces:

- With the roll-out of Action Fraud, despite guidance being issued some forces were left with the impression that they were no longer responsible for investigating fraud;

- Others believed that they would be sent ‘arrest packages’ containing sufficient information to immediately go out and arrest suspects; and

- In some forces, the person(s) responsible for returning outcomes did not realise that this was a part of their role, meaning that the work was sometimes not done, impacting on outcome rates.

Overall, these issues can lead to increases in attrition, either as disseminations that are not actioned, or outcomes that are not returned to NFIB for inclusion in statistics. Indeed, when Action Fraud was first rolled out nationwide, it took some time for all forces to consistently return outcomes data on a monthly basis. Improvements in each could increase the number of cases investigated and outcomes returned.

3. Variation in approaches between forces

The final theme was present in findings relating to the later stages of the process, when crimes are disseminated to local forces, and when outcomes are returned by police to NFIB. The research showed that there is considerable variation in the way that forces deal with cases referred to them by NFIB, and therefore scope for sharing ‘best practice’ between forces. For example, forces take different approaches to gathering outcomes data and returning it to NFIB. Some forces have automated their outcomes returns process, reducing the time and resource required for this task. If there is scope for sharing expertise amongst forces, to increase the number of crimes with outcomes that are returned to NFIB, this could reduce attrition.

Actions Taken (as of 2015)

While reading this report, it is important to bear in mind that steps have already been taken to act on the findings of this work. Throughout the project findings were fed back to Action Fraud and NFIB, in order that they could act on them as soon as practicable. A summary of findings and recommendations was also presented at the Strategic Fraud Group, attended by HO officials and senior policing. A detailed set of recommendations were provided to Action Fraud and NFIB, which have fed into day-to-day practice, a new Improvement Plan agreed between the Home Office and City of London Police and monitored at a regular tactical governance group. Findings have also informed the commission of a new Action Fraud / NFIB system.

1. Background

As of April 2013, Action Fraud became the national centre for reporting and recording fraud and cyber-dependent crime. Action Fraud record all such crime, whether it is reported to them by the victim, or another party (e.g. police or a family member). Reports can be made via the Action Fraud call centre, or using their online reporting tool.[4] Information reports are also taken, for incidents that don't reach the threshold for a crime.[5]

All reports (crime and information) received by Action Fraud are transferred to the National Fraud Intelligence Bureau (NFIB), and ingested into their Know Fraud system. Know Fraud does two main things: it builds networks of the reports, based on common entities (e.g. bank account numbers, suspect names), and then 'scores' the networks according to a matrix, which identifies which are most likely to be viable for investigation.

Those networks which meet the scoring threshold are then placed into 'queues', which NFIB staff, known as Crime Reviewers, review to establish whether there are sufficient leads for the network to be sent to a police force for investigation and enforcement. Packages can also be sent to other organisations such as Trading Standards or the Insolvency Service.

There are also 'manual review' criteria which were introduced to mitigate weaknesses in the scoring matrix. These criteria are designed to identify cases of high financial loss, or where the suspect is likely to be known to the victim (e.g. corporate employee fraud). Such crimes are also considered by NFIB Crime Reviewers, and where appropriate are disseminated for enforcement.

Once police forces receive the disseminations, what happens to them is dependent on, amongst other things, how cases are allocated in forces (e.g. whether a fraud / economic crime team deal with NFIB disseminations, or whether they are allocated

[4] www.actionfraud.police.uk

[5] For example:

When an individual has been subject to plastic card fraud, but has been refunded by the card issuer, they will not be considered the 'victim' of the crime, and instead the financial institution becomes the victim.

The use of another person's identification details (or the use of false identification details), often referred to as identify theft, is not in itself an offence in law. It is only when a fraud is committed using those details, that a crime is considered to have occurred

See: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/515640/count-fraud-april-2016.pdf.

to a neighbourhood team), resources available, and local force priorities. When an outcome is achieved, forces send this information back to NFIB via a monthly return. NFIB collate this data to build a national and force-level picture of outcomes for fraud and cyber-dependent crimes. (For more detail on the overall process, see Annex A).

Figure 1 shows this process, split into four stages. Attrition[6] occurs throughout this process, with the number of crimes at each stage falling. Based on data between April and September 2013, 115,991 crimes were reported to Action Fraud. Of these, approximately 44% reached the second stage, where cases are reviewed by a NFIB Crime Reviewer. Approximately 41% of those cases reached the third stage of dissemination to a local police force (or other organisation, such as Trading Standards). Finally, approximately 16% of all crimes that were disseminated resulted in an outcome that was returned to the NFIB. Although some of this attrition is unavoidable, there are also areas for improvement at all four stages.

When reading this report, readers are asked to remember the time period in which the research was carried out. All quantitative analysis was based on data reported between April and September 2013. Any qualitative findings were drawn from interviews and focus groups that took place in the summer of 2014. During this period, wider work was underway by NFIB, and the Home Office, chiefly to improve practices around recording crimes and to improve the return of outcomes (also referred to below). In addition, throughout the period of work findings and recommendations were fed back to Action Fraud and NFIB, and therefore a number of measures have already been put in place to address these. A detailed Improvement Plan has been agreed between the Home Office and the City of London Police. This is monitored via a regular tactical governance group chaired by the Home Office, and included many of the recommendations that came from this project. The number of forces that are returning outcomes has also improved, with all police forces now making outcome returns. Outcome rates are also improving (discussed in more detail in Annex B).

Over the period in which the project took place, there was an improvement to attrition rates, although it is likely that much of this was down to improvements in recording practices driven by the Home Office National Crime Registrar (as part of a wider programme of improvements in the recording of fraud and cyber-dependent crimes). For the period April – September 2013, the proportion of cases reported to Action Fraud that achieved an outcome (based on the 9-outcome framework) was around 2%. The most recent data, for 2014/2015, shows that the outcome rate has

[6] Attrition refers to the process by which cases ‘fall out’ of the system at different stages. Attrition can occur before reporting, with cases not being reported at all, and then for various other reasons, including reports not being crimed, not being investigated, an offender not being identified, and so on.

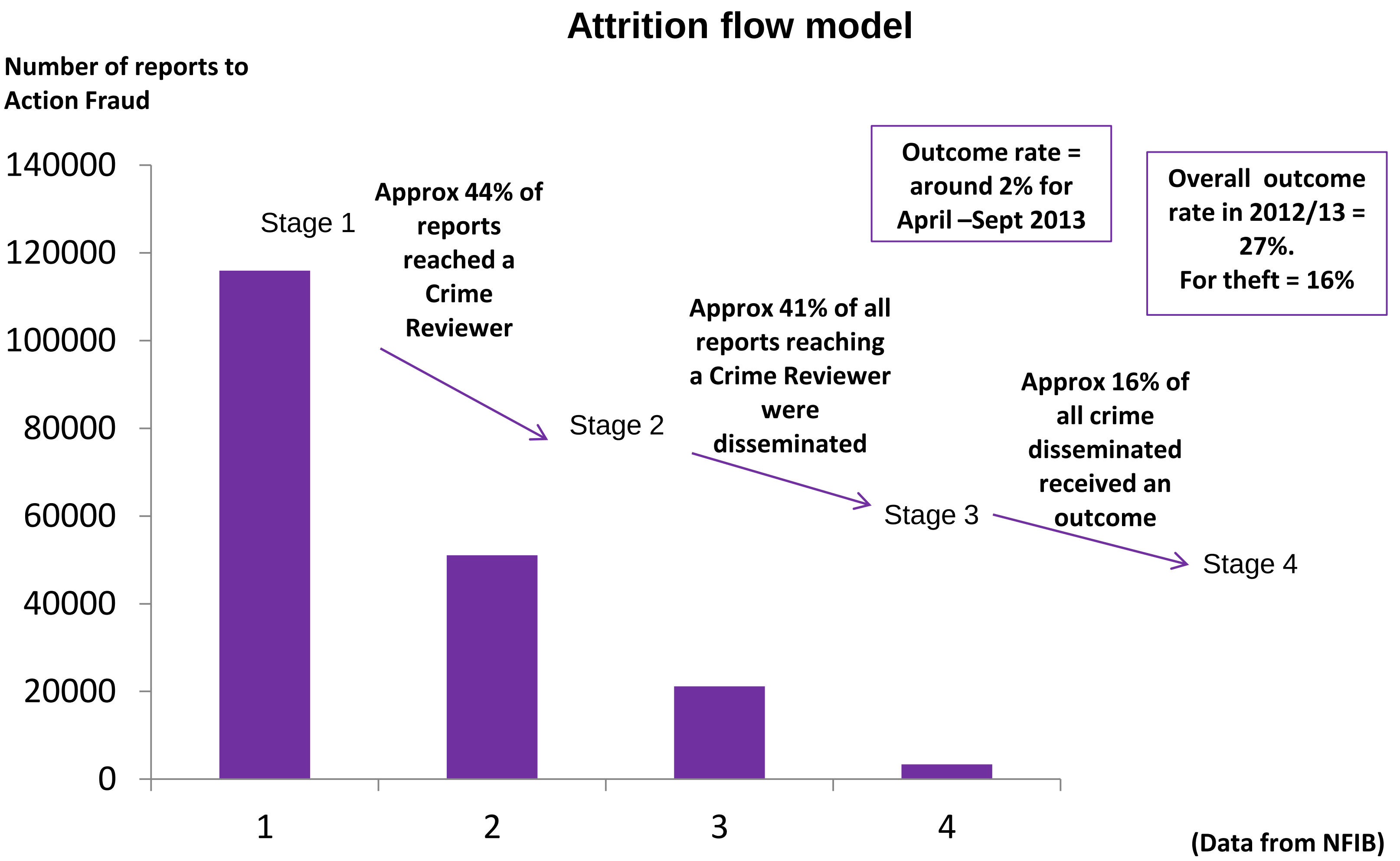
increased to around 5% (again based on the old 9-outcome framework).[7] [8] [9] By January – March 2015, the processes around both the new outcomes framework and the transition to Action Fraud had bedded in better, meaning more complete outcomes data was provided by forces.

[7] In order to make meaningful comparisons between years, this outcome rate is calculated based on the number of reports recorded in this period by Action Fraud, and does not take into account the inclusion of reports from the FFA and CIFAS (which were added to the overall crime count in October 2015). If these offences are included, the outcome rate is nearly 2%.

[8] The 9 outcomes are charge / summons; adult caution; youth caution; Taken Into Consideration (TIC); Penalty notices for disorder (PND); the offender has died; cannabis warning (obviously not relevant to fraud); community resolution; prosecution not in the public interest (CPS).

[9] It should be noted that the outcome rates are not 'true' outcome rates, as they are calculated by comparing the number of outcomes in the period with the number of offences. To calculate a true rate, only those outcomes that relate to offences that took place in the same period should be included. Those that relate to offences from older periods should not. However, data are not yet available on this basis for fraud outcomes, and so all outcome rates here are calculated on the 'old' basis to allow fraud to be compared to other crime types in a fair way. While this is not a perfect measure of outcome rates, it does give a general picture of outcomes.

Figure 1: Attrition flow model (based on reports made to Action Fraud between April – September 2013)



Approx 44% of reports reached a Crime Reviewer

Approx 41% of all reports reaching a Crime Reviewer were disseminated

Approx 16% of all crime disseminated received an outcome

Outcome rate = around 2% for April –Sept 2013

Overall outcome rate in 2012/13 = 27%.
For theft = 16%

(Data from NFIB)

2. Scope of the project

In July 2013 the National Fraud Authority (NFA) and the National Fraud Intelligence Bureau (NFIB) submitted an improvement plan to the Home Office Cyber Crime Board[10] for the reporting and management of cases received by Action Fraud and the NFIB. This stemmed from concern expressed by the Board regarding very low outcome rates for fraud and cyber-dependent crimes. For example, between April and September 2013 there was an outcome rate of around 2% for all crimes reported to Action Fraud and dealt with by the NFIB (although this is recognised as being artificially low due to the new processes bedding in). Part of this plan involved a requirement that the NFA / NFIB undertake further exploration of attrition levels in comparison to other crime types, with the assistance of the Home Office Science Cyber Crime Research Team. The full findings from that project are presented here.

The attrition project focused solely on reports to Action Fraud classified as crimes in accordance with the Home Office Counting Rules (HOCR).[11] However, it should be noted that this does exclude early parts of the recording process (before the decision is made that a report constitutes a crime), and the police investigation stages. Both of these aspects were outside the scope of the report.

Action Fraud receive a large number of initial contacts (approximately 379,000 in the six months to September 2013), many of which will not meet the threshold for a crime under the HOCR. Around 30% of contacts are crime reports, whilst others are information reports (around 20%), and nearly 50% are ‘signposted’ elsewhere (e.g. the informant will be given advice and information, advised to report to their local police force, as appropriate). Information reports and signposted contacts were outside of the scope of this project. Some (internal) work had already been undertaken by the NFIB to better understand the type of contacts that do not result in a crime or information report and how to minimise receipt of inappropriate or time-consuming contacts. A potential avenue for future research could be further

[10] Chaired in 2013 by James Brokenshire, then the Minister for Security; from 2014 onwards by Karen Bradley, Minister for Modern Slavery and Organised Crime, and from 2015 onwards by John Hayes, Minister for Security.

[11] Police recording of crimes is governed by the National Crime Recording Standard (NCRS) and the Home Office Counting Rules (HOCR). These set out the principles under which reports received from victims are recorded, and the broad classification groups into which those offences are managed for statistical purposes (see https://www.gov.uk/government/publications/counting-rules-for-recorded-crime for more information).

work to explore these earlier stages of ‘attrition’, to give a more complete picture.

Also out of scope for this project were the data the NFIB receive on ‘industry recorded frauds’, i.e. those reports which are passed to NFIB from CIFAS,[12] a UK-wide fraud prevention service, and Financial Fraud Action UK (FFA)[13], a body which collates information from the card payments industry in the UK. At the time this project was conducted, these offences were not included in the overall fraud count, for example due to the risk of double-counting, were a bank to report a crime to both CIFAS and the police. However in October 2015 the Office for National Statistics (ONS) included these offences in the overall crime count for the first time.[14] However, this is another important avenue for attrition, given that in the six months ending September 2013 there were around 138,000 industry recorded frauds.[15] Another potential avenue for future research would be exploring with industry partners how the value and use of their reports could be improved in future.

Also outside of the scope of the project are unreported frauds. In some attrition studies (e.g. those looking at rape) it is possible to estimate how many unreported offences there may be, for example by looking at alternative sources to Police Recorded Crime such as the Crime Survey for England and Wales (CSEW). However, at the point this project was carried out, this was not possible for fraud and cyber-dependent crimes due to the way the CSEW gathers data on these offence types. [16] Nevertheless, it is important to note that under-reporting is an issue for fraud and cyber-dependent crimes, albeit that it is outside of the scope of this project. This would be a potential avenue for future research.

[12] CIFAS is a cross-sector, not-for-profit membership association, which facilitates fraud data sharing between around 300 organisations, from both the public and private sectors. Membership covers all the major banks and around 90% of plastic card fraud providers. They collate data on various frauds, including banking and credit industry fraud, insurance-related fraud, charity fraud. However, they do not currently collect data on ‘card not present’ fraud, lost or stolen cards, or ATM fraud.

[13] FFA UK works in partnership with the UK Cards Association, and is the name under which the financial services industry coordinates its fraud prevention activity. FFA UK represents members of the UK Cards Association on credit and debit card fraud, and retail banks on non-card fraud matters, such as payment fraud using online banking or telephone channels. These crimes are only reported for intelligence purposes.

[14] See http://www.ons.gov.uk/ons/dcp171778_419450.pdf.

[15] In the year to December 2015 there were approximately 390,000 industry recorded frauds, see: http://www.ons.gov.uk/ons/dcp171778_419450.pdf.

[16] Since this research was conducted, the ONS concluded their work to develop questions to cover fraud and cyber-dependent crimes in the CSEW (see http://www.ons.gov.uk/ons/guide-method/method-quality/specific/crime-statistics-methodology/methodological-note--work-to-extend-the-crime-survey-for-england-and-wales-to-include-fraud-and-cyber-crime.pdf for more information) and published the results of the first field trials in October 2015. These questions cover fraud and elements of cyber crime experienced by households. However, it should be noted that the new CSEW questions will capture incidents which may not meet the threshold of a crime under the Home Office Counting Rules (HOCR). For example, if a victim of fraud has their loss reimbursed by their bank or card provider, they would not be considered the victim (the bank becomes the victim), and so the crime would only be recorded by police if reported by the financial institute. However, these were included by the ONS on the basis that these crimes had occurred and, as the CSEW would not pick up offences against businesses, they felt it important to capture them.

3. Project Aims

The aims of the project were as follows:

1. To work with Action Fraud / NFIB to establish overall outcome rates and levels of attrition for the fraud and cyber-dependent crimes they deal with (see Section 1. Background for more detail).

2. To understand where attrition is occurring in the recording and investigations process and the key factors driving attrition.

3. To draw comparisons between the outcome rates of offences reported to Action Fraud / NFIB, and of 'traditional' crimes.

4. To help identify possible methods to reduce attrition where necessary.

Using quantitative and qualitative analysis (see Section 4. Methodology) the project looked at factors affecting:

a) whether or not a crime reported to Action Fraud was disseminated by the NFIB to the police; and

b) whether or not the police achieved an outcome against the crime received.

Another important aspect of the project was to consider what a 'reasonable' outcome rate for fraud and cyber-dependent crimes might look like. By making comparisons with sanction detection or outcome rates for more 'comparable' crimes types (for example those relating to other acquisitive crimes, rather than violent crimes) and drawing upon the wider findings from this research, the intention was to develop a clearer understanding of what might be a realistic and appropriate outcome rate for crimes reported to Action Fraud and dealt with by the NFIB. However, it should be noted that fraud does differ from other offences in areas such as the 'investigative opportunities' – for example in contrast to burglary where there are likely to be additional forensic opportunities such as fingerprints and DNA evidence. In addition, it is often the case that victims take a considerable period of time to realise that they have been a victim of crime, if at all. All of these features combine to create additional challenges for law enforcement working in this area. (For further discussion of outcome rates, including on recent changes to the outcomes framework, see Annex B).

4. Methodology

A mixed-methods approach was taken. Quantitative data analysis was used to provide an evidence base to underpin factors linked to attrition, and to identify additional factors not previously considered. In addition, qualitative data (interviews and focus groups) were incorporated to give a deeper understanding of the challenges faced by those involved at various stages of the process.

There were three phases to the analysis:

First, quantitative analysis of 3,140 cases reported to Action Fraud between April and September 2013 was undertaken. Logistic regression analysis was used to identify factors that could be associated with crimes being sent to local police forces for enforcement, having reached an NFIB Crime Reviewer. This sample was drawn using a stratified random sample, from the total 115,991 cases reported to Action Fraud in the same period. It was not feasible to use the whole dataset largely due to constraints on timing. This meant that first, it was too difficult to transfer the data between NFIB and Home Office systems within the time allowed. Second, the data required a considerable amount of cleaning before it was ready for use, and it was not possible to do this for the whole dataset within the time available. Therefore a sample was taken. The sample was stratified according to the type of offence, with the strata being:

- Online frauds (or cyber-enabled frauds, defined as all frauds recorded as ‘Online Shopping and Auction frauds’, and all frauds where the report stated an online enabler[17] was involved);
- Offline frauds (all frauds that did not meet the definition for ‘online fraud’);
- Cyber-dependent crimes (all crimes that are recorded under the Computer Misuse Act, such as hacking).

[17] One of the questions on the Action Fraud reporting tool asks whether any of the following online enablers were involved: hacking, email, online sales, or online social media.

The definition of online frauds and offline frauds was based on advice from Action Fraud and NFIB.

The total sample was split according to the proportions in which each of the online frauds, offline frauds, and cyber-dependent crimes were seen in the total population of crimes reported to Action Fraud (see Table 1). In addition, due to the low number and proportion of cyber-dependent crimes in the population dataset, a 'booster' sample was taken, to increase the number of those cases in the sample so it would be sufficient for statistical analysis.[18] Approximately 2% of the population was sampled.

Table 1: Numbers of cases in sample, according to strata

	% cases in strata	# cases in sample
Offline frauds	49%	1,225
Online frauds	40%	1,000
Cyber-dependent crimes	11%	880 (275 + 605 as a booster sample)

The second phase consisted of quantitative analysis of a second sample of 1,642 cases that were reported between April and September 2013, and disseminated to one of seven forces. As in phase 1, logistic regression analysis was used to look at factors predicting whether disseminated cases would achieve an outcome, or not. Although for this part a random sample may have been preferable (as in the first part), there were several reasons as to why this approach was not taken:

- Getting the list of unique crime reference numbers for which there had been a dissemination, from which to draw the sample, was very difficult due to the way that data was stored by NFIB;

- The third phase (see below) involved (the same) seven forces, and so using a comparable set of data was desirable. As it was possible to get a census of cases disseminated to these seven forces there was no need to take a sample;

- A similar approach has been taken in other projects looking at attrition (e.g. Feist et al, 2007).

[18] See Tabachnick, B. & Fidell, L. (2013). Using Multivariate Statistics. 6th edn. Allyn and Bacon: Boston.

The seven forces were selected with the input of NFIB, on the basis of their monthly outcome rates and the number of crimes disseminated to them by NFIB (to ensure there would be sufficient cases for the statistical analysis), at the time of the research (April – September 2013). Selection of forces was not random. Two forces with lower outcome rates, two with average outcome rates, and two with higher outcome rates were chosen. A seventh force, which was a large metropolitan force, was also included, as the other six forces were smaller and in some cases, more rural.

In addition, for both these quantitative phases, many of the findings were based simply on an examination of the data – looking at where data was missing, and using it to understand potential issues in reporting.

The third phase of the project took a qualitative approach, using interviews with police forces and stakeholders, and focus groups with Action Fraud Call Handlers and NFIB Crime Reviewers. The purpose of this phase was to develop a deeper understanding of the overall process from recording to local law enforcement action, and the challenges posed by this process. Two focus groups were conducted with Action Fraud call handlers, and two with NFIB Crime Reviewers. Focus groups were used with Action Fraud and NFIB staff to enable capture of a range of views, and to encourage interaction and discussion amongst staff about their experiences. The focus groups were designed to understand more about staff backgrounds / experience, what their role entails, how they make decisions, challenges in their role, and what improvements would be beneficial. Each focus group lasted approximately two hours, and all had the same two facilitators. Interviews were conducted with seven call handlers across three forces, NFIB Specific Points of Contact (SPOCs) in five forces, and the person responsible for outcomes in six forces. In addition, interviews were conducted with individuals from the National Cyber Crime Unit, National Trading Standards Board, a Regional Organised Crime Unit, and the Metropolitan Police Service (specifically Project Falcon) (see Table 2). Interviews were structured similarly, to understand the process by which the force manages NFIB disseminations, from receipt to return of outcomes, along with their views on the overall model, the challenges / difficulties they experience, and the improvements they felt would be beneficial. All interviews were carried out by the same interviewer, and each lasted approximately one hour. Focus group and interview schedules are included in Annex C.

Table 2: Focus groups and interviews conducted for Phase 3

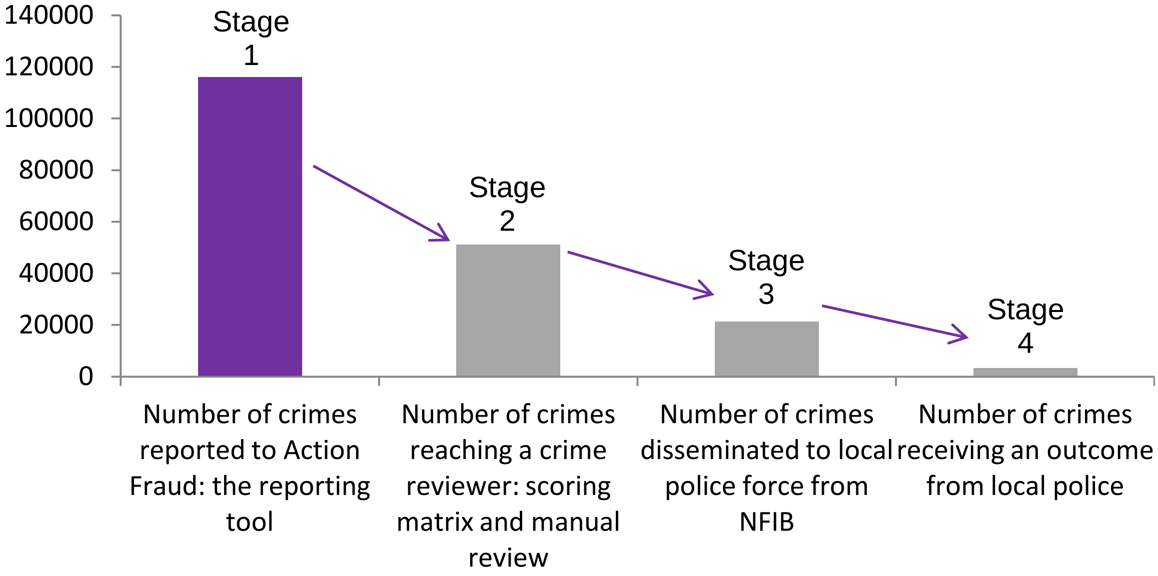
Role	Approach
Action Fraud call handlers	2x focus groups (12 participants in total)
NFIB Crime Reviewers	2x focus groups (13 participants in total)
Police force call handlers	7 interviews (across three forces)
NFIB Specific Points of Contact (in police forces)	5 interviews (across five forces)
Police force staff with responsibility for outcomes	6 interviews (across six forces)
National Cyber Crime Unit	1 interview (2 participants)
National Trading Standards Board	3 interviews
Regional Organised Crime Unit	1 interview
Metropolitan Police Service (Project Falcon)	1 interview

Findings from each phase were drawn together, to identify areas of attrition and opportunities for improvement across the four main stages of the Action Fraud / NFIB process (see Sections 5-10).

5. Key Findings: Attrition Stage 1 – Reporting to Action Fraud

At the first stage, findings show that improving functionality of the reporting tool, and user understanding of how best to complete reports, could help to reduce attrition by increasing the volume of cases that reach a Crime Reviewer, and improve the quality of these cases.

Figure 2: Attrition flow model – Stage 1 (based on all crime reports received by Action Fraud, April – September 2013)



Interviews with Action Fraud and force call handlers suggested that the staff interviewed have varying levels of knowledge about the Action Fraud / NFIB / local force process for dealing with fraud and cyber-dependent crimes. Improving knowledge of both the process, and crime prevention advice, will give a better victim service.

Call handlers interviewed, in Action Fraud and local police forces, reported varying levels of knowledge about how the whole process works, their understanding of what NFIB do / don't do, and what victims should expect.

They are one of the main points of contact for victims, but those interviewed suggested that they sometimes feel they don’t have enough knowledge to fully explain things to victims. For example, a police force call handler who was interviewed believed that the current system allows multi-session reporting, which is not the case. Telling victims this would have obvious impacts on the quality of reports and therefore the service victims would get.

In interviews wider stakeholders suggested that call handlers should have training specific to cyber-dependent crimes. Although the reporting tool is tailored to the crime type (e.g. for cyber-dependent crimes, the tool will ask specific questions about how the malware was introduced, which obviously wouldn’t be included for fraud offences), interviewees suggested that equipping call handlers to give certain advice would be beneficial. For example, in interview the National Cyber Crime Unit (NCCU) explained that it is generally recommended that devices / computers are not turned off, as this may prompt the virus / malware etc to uninstall itself. This type of advice could improve opportunities for investigation, and also give victims valuable advice on how to prevent becoming a victim again.

Recommendations:

NFIB should produce refreshed guidance for Action Fraud and force call handlers, showing an overview of the process (with detail on what NFIB do), and what victims can / cannot expect once they have made a report.

Forces should ensure that this guidance is distributed to relevant staff, to help their understanding of the whole process, as well as the parts they are directly involved in.

Action Fraud / NFIB should consult with wider stakeholders (e.g. the NCCU, cyber teams in the ROCUs) to establish what additional advice could be given to victims of cyber-dependent crime, both to improve investigative opportunities and equip victims with crime prevention advice.

Examination of quantitative data showed that information was not always correctly recorded in reports. In interviews, call handlers in Action Fraud and forces identified a number of areas where they would appreciate additional guidance on how best to complete the tool. Improving guidance should in turn improve the quality of data that goes into the system, which is key to reducing attrition.

Examination of NFIB data illustrated the importance of entering information in the appropriate place on the reporting tool, as good quality reports are essential for ensuring crimes progress through the scoring systems. In approximately 5% of the Phase 1 sample information critical to the scoring matrix (e.g. bank account numbers, phone numbers) was given in the free text box, but not entered into the appropriate tick / data box. As a result cases achieved a lower score on the SM than they might have otherwise, meaning potentially viable crimes were not reaching Crime Reviewers.[19]

Call handlers in forces and Action Fraud stated that they sometimes found it difficult to know how best to complete the reporting tool. For example, when there are multiple offenders, or when completing the free text field (Action Fraud call handlers in particular were keen to get feedback on what NFIB Crime Reviewers would find most helpful).

Simply looking at the Action Fraud data suggests that members of the public may also find this useful, particularly around the free text – some of the free text boxes contained incredibly long detailed descriptions which were difficult to follow. Others had such small amounts of information that it was difficult to understand what had happened.

Recommendations:

Action Fraud / NFIB should consider amending the tool to include better signposting to victims, to ensure reports contain the right information in the right places. This could incorporate features such as pop-up boxes, flagging when particular boxes have not been completed to ensure victims do not miss out important information. The tool could also make clearer where information is of particular importance, for example total money loss experienced, details of offenders, etc.

Action Fraud / NFIB should provide guidance on both of these aspects of the reporting tool to Action Fraud call handlers, and staff in local forces. Improving guidance should also improve the quality of data that goes into the system, which is key to reducing attrition. This advice could also be added to the online reporting tool, to assist victims who do not report via the call centre.

NFIB should work with Crime Reviewers to understand what is helpful in the free text. This should then be added to the reporting tool to guide those making reports. If possible checks should be made to see whether this a) improves the overall quality of reports, or b) reduces the number of poor quality reports.

[19] Because of the complexity of the Scoring Matrix, and issues with the data, it was not possible to calculate the number of crimes for which this would be the case.

In local forces, call for service (CFS[20]) cases are not always reported to Action Fraud immediately (as per guidance), but instead are sometimes held back and reported at different stages of an investigation. When they are reported, the process can be very time consuming, which has a knock-on effect of force staff phoning Action Fraud, taking up time that call handlers could be spending dealing directly with victims. As well as affecting victim perception of the service, it could also reduce the number of reports going into the process, causing attrition at the very start of the process.

In interviews with police staff and officers, participants suggested that when a force receives a CFS, the report is not always double-keyed[21] to Action Fraud as soon as possible. Staff and officers in forces reported that the double-keying is sometimes delayed until an investigation has begun or is completed.

Interviewees report that double-keying can take a considerable amount of time; around 20 minutes for simple crimes, and an hour or longer for more complex frauds. Responsibility for double-keying varies between forces, and interviewees suggested that when double-keying is not centralised the problems are exacerbated – less experienced staff are slower, have less understanding of how the Action Fraud system works, etc.

Police staff reported that it is frustrating having to enter their own details as an informant, when they are simply putting a report on the system on behalf of a victim / officer; some interviewees reported having to input their own details up to three times. Force staff stated that it would be helpful to be able to simply tick a box stating that the crime is a CFS, and then carry on entering victim details / details about the crime itself.

Again, looking at the Action Fraud data appears to support this. In the Phase 2 data it was necessary to identify what cases were reported as CFS, and at what stage in the investigation they were reported (e.g. as soon as officers took the report, or at some point further on in an investigation). However, it transpired that multiple variables had to be used to identify CFS cases (rather than there being just one variable that captured the information), and it was difficult to tell what point the investigation had reached before it was reported to Action Fraud.

It is possible that this also causes issues for Action Fraud. Police are expected to report via the online tool, but Action Fraud still receives a large

[20] Police will record fraud offences where there is a ‘call for service’, i.e. where: the offender(s) are arrested by police; there is a call for service to Police and the offender “is committing” or has recently committed at the time of the call for service for all fraud types; or there is a local suspect (i.e. where, through viable investigative leads, police can or could locate a suspect with the details provided, or police have sufficient details to apprehend an offender).

[21] “Double-keying” is the process by which information is entered onto a force system, and then also has to be entered onto the Action Fraud system (or vice versa).

number of calls from police every day. These calls, which are typically because the person doing the double-keying is not confident with the tool, block up the phone lines and divert resource from dealing with victims who are trying to report directly.

Recommendations:

NFIB should produce further guidance to forces to emphasise the importance of double-keying CFS cases as soon as possible.

NFIB should ensure that the reporting tool easily captures what stage the investigation has reached at the point it is reported to Action Fraud, and that staff in Action Fraud and local forces are aware of the importance of completing this (this will reduce the risk of Crime Reviewers disseminating a crime to another force when an investigation is already underway elsewhere).

NFIB should ensure that there is one clear (compulsory) tick box on the reporting tool so that crimes can be identified as CFS. If this is already the case, NFIB should further investigate the complaints about police (staff) having to repeatedly enter their own details, to better understand the problem, and whether it may be something such as police (staff) using the wrong reporting channel, or a misunderstanding about how the reports should be completed.

Where possible, NFIB should simplify the reporting tool used by police (as per recommendations above), to reduce the amount of time taken to double-key reports.

Forces should consider the benefits of having a centralised approach to double-keying, for example so that call handlers / the crime management unit are responsible for double-keying all CFS cases. This would enable expertise to develop, which would hopefully speed up the process (although it would require officers to notify staff of the need to double-key crimes).

Discussions with NFIB suggested that under-reporting from forces may be an issue. There is some evidence that (particularly in the early period of Action Fraud) forces did not always double-key reports of fraud and cyber-dependent crimes. These may or may not have outcomes attached. This impacts on the ability to understand the nature and scale of fraud and cyber-dependent crimes, of outcome rates, and of the attrition rate.

As well as the issues relating to using the reporting tool, there is some evidence that police forces are not always passing fraud and cyber-dependent crime reports onto Action Fraud for recording. For example, the NFIB found that one large force had recorded around 2,500 fraud and cyber-dependent crimes (with around 600 linked outcomes) on their systems that had not been double-keyed to Action Fraud. The impact of this is that both crimes and their outcomes may therefore be under-reported, potentially resulting in an inaccurate picture of how well law enforcement are tackling these types of crimes. It is also impossible to tell whether these police reports are 'different' in some way to those reports that are sent on to Action Fraud (e.g. they are more 'solvable' / likely to result in an outcome than Action Fraud crimes). The extent of this issue across all forces is unclear, as is how and where these reports are being recorded.

Recommendations:

Police should reiterate the importance of accurate record keeping, to minimise the risk that frauds and cyber-dependent crimes reported to them are not passed on to Action Fraud. In addition, forces should investigate the possibility of audits to identify 'missing crimes'. Based on interviews this simply may not be possible, due to the nature of the systems that record these NFIB offences. However, consideration should be given to approaches such as key word searches to identify NFIB cases that have outcomes that haven't been flagged properly, audits of cases disseminated by NFIB where no outcome has been returned, etc.

Throughout the project, interviews, focus groups and informal discussions with Action Fraud and NFIB staff have identified weaknesses in the reporting tool used by members of the public and Action Fraud / police staff. Key issues centred around the system not allowing (meaningful) updates, and problems with the questions the tool asks to determine what category a crime is under the Home Office Counting Rules.

At present, it is not possible to update reports made in any meaningful way. Information can be added at a later date, but only in a free text box; scoring matrix and other fields cannot be updated. This puts Action Fraud call handlers in a difficult position – if a victim makes a report but does not have all their information to hand, the call handler is required to take that report, even though it may be largely 'empty' of detail, and therefore extremely unlikely to go anywhere. If they suggest that the victim calls back at a later date, when they have all the necessary information available, they risk 'failing' the call in audit.

Police staff reported concerns around the way that cases are 'triaged' by the reporting tool, where the victim / informant is asked questions to determine what type of fraud they are reporting. Force staff felt that this is overly long and complicated. Staff said that they were sometimes confused by it, and were concerned that it could be even more confusing for victims with very little experience.

This was echoed by NFIB Crime Reviewers, who reported that the NFIB90 code (i.e. any other fraud) often contains inappropriate cases (i.e. that should be classified as other fraud types), seemingly because victims cannot decide how else to classify their fraud.

Both issues contribute to the overall attrition rate – if victims are not able to update their reports there is a risk that ‘empty’ reports are recorded (meaning little for the scoring systems or Crime Reviewers to work with). If reports are categorised incorrectly it is possible that cases meeting manual review criteria (i.e. specific crimes types) are therefore not identified, and will not be reviewed for dissemination.

Recommendations:

Although the new Action Fraud / NFIB system will allow multi-session reporting, in advance of its introduction it may still be worthwhile NFIB looking into how many reports are made with minimal information, and whether additional information is provided in the later ‘update’ box. This would provide an insight into the extent of the issue, and help to determine whether it is something that needs resolving before the new system is introduced.

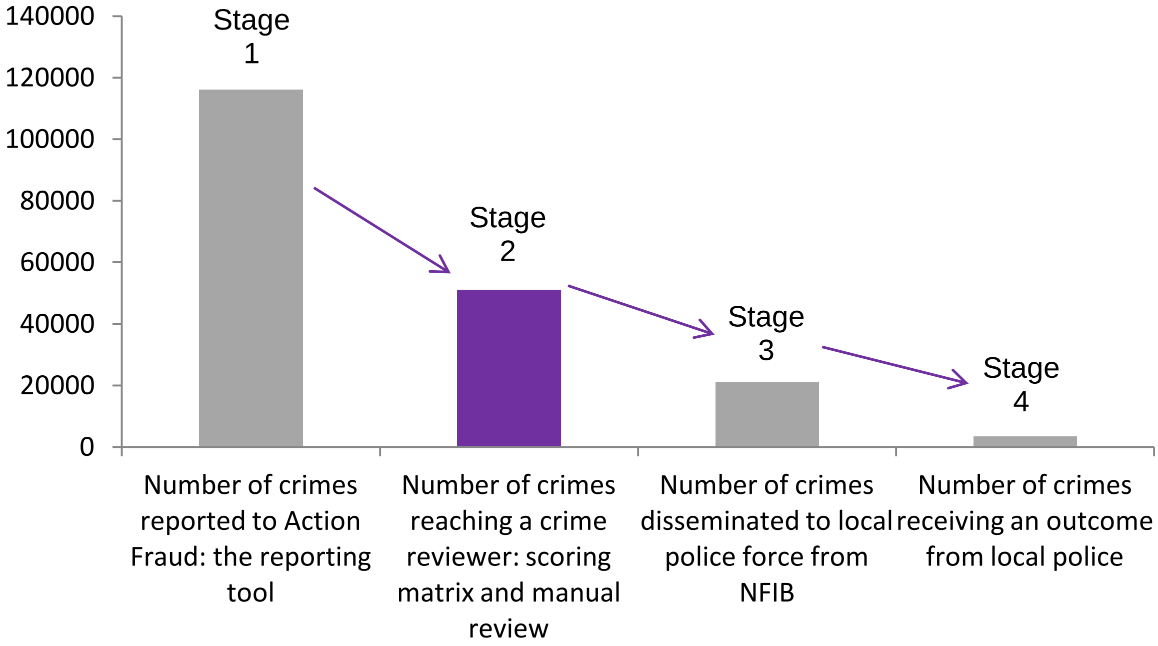
NFIB should consider options for simplifying the approach by which the fraud type is identified, if possible. If not possible, NFIB could consider implementing proactive web chat to assist those reporting online, if the amount of time spent on the relevant page indicates that they are struggling to make a choice.

In addition, NFIB should look into the types of crime that are in NFIB90, to understand whether the same types of crime repeatedly appear (indicating those crimes are harder to identify when reporting), or whether there may be new crime types present.

6. Key Findings: Attrition Stage 2 – The Scoring Matrix and Manual Review criteria

This stage presents findings centred on the volume and nature of crimes reaching a Crime Reviewer. Crimes reach a reviewer either because they meet the threshold of the Scoring Matrix, or they meet one (or more) of the manual review criteria. Improving the Scoring Matrix and manual review systems will help ensure that only the crimes that have the most potential for dissemination for enforcement (i.e. the most 'viable' crimes) reach Crime Reviewers for consideration.

Figure 3: Attrition flow model – Stage 2 (based on all crime reports received by Action Fraud, April – September 2013)



Examination of the data showed that the Scoring Matrix (SM) was not working as well as intended. Put simply, the purpose of the SM is to identify crimes that are most likely to be viable for enforcement, so that

NFIB Crime Reviewers’ time is put to best use (rather than looking at crimes which are unlikely to be viable). However, the findings demonstrated that a smaller proportion of the crimes reaching a Crime Reviewer were from the SM, than were from the Manual Review criteria (25% versus 60%, with it not being possible to match the remaining cases to either route).

It would not be possible for NFIB Crime Reviewers to review every crime reported to Action Fraud, as there are not enough Crime Reviewers to deal with the volume of reports. In addition, not all reports will contain viable leads for investigation. Instead two automated approaches are used to identify the cases that (in theory) are most likely to have viable lines for enquiry and therefore should be disseminated for enforcement.[22] The first is a scoring matrix, which is used to assign a score to all crimes that Action Fraud receive, based on the presence or absence of certain pieces of information. For example, if the suspect’s bank account details, telephone number, or vehicle registration are given then crimes will score higher than if they are not. All crimes go through this automated scoring matrix, and based on the score the system will flag them and place them in a ‘queue’ for further consideration by a Crime Reviewer. In addition to the scoring matrix, there are manual review criteria. Again, the system automatically looks at all crimes to identify any that meet one or more of these criteria. Crimes that do meet the criteria are also flagged and placed into a queue for review by a Crime Reviewer (regardless of score on the scoring matrix). For example, all reports with a loss of £100,000 [23] or over are reviewed because of the potential severity of impact on the victim, and certain crime types (e.g. pension liberation fraud) are reviewed to develop the intelligence picture, and support collaborative activity. In order to maximise outcomes, and if the SM were working properly, it would be expected that the majority of cases Crime Reviewers assess arrived with them via the SM. However, examination of data showed that this was not the case – in fact a higher proportion of cases reached Crime Reviewers because they met the Manual Review criteria (60%) than because they passed the SM (25%).

This finding was supported by focus groups with the Crime Reviewers. Overall, the Crime Reviewers had mixed views on the SM. They felt that the crimes / networks the SM does identify are the right ones (i.e. they do offer viable lines of enquiry), and the scores attributed give a fair guide of whether a crime / network is likely to be viable or not. However, they also voiced concerns that amongst the crimes that are deemed ‘not viable’ by the SM (i.e. that do not meet the scoring threshold), there are in fact ‘good’ crimes that a

[22] Reports that don’t get through the scoring matrix / manual review may be progressed if they are found (by the Know Fraud system) to have commonalities with crimes that do get through the scoring matrix / manual review. In such circumstances, they may become part of a network of crimes, and be disseminated as part of a network.

[23] £500 for computer misuse crimes.

Crime Reviewer could develop and disseminate to a local force. Thus from their perspective, there is a risk that potentially viable crimes are missed, increasing attrition.

To mitigate this risk one desk reported that they had made the decision to review all crimes / networks that score zero or above. As a result, on that desk there was a considerable backlog of crimes waiting for review. Crime Reviewers also reported concern around delays in reviewing / disseminating crimes impacting on the ability to recover funds etc.

Recommendations:

NFIB should consider alternative options for the SM, taking into account Crime Reviewers' views (and any others as appropriate) on what makes a crime viable for investigation, and what they perceive the SM is not picking up. Crime Reviewers tend to be the experts in what can be used to build a package for dissemination, so their expertise and knowledge should be utilised. In addition, machine learning could be a beneficial option, to automatically flag cases that do not meet the SM threshold, but that share similar traits to cases that have been referred to a Crime Reviewer via Manual Review in the past.

NFIB should work to ensure that they can manage / reduce any backlog in crimes waiting for review in the interim period.

The 'Manual Review' (MR) criteria could also be improved. These were introduced to mitigate some of the weaknesses of the scoring matrix. However analysis showed that while Crime Reviewers examined a lot of 'MR' cases, very few are sent for enforcement, or achieve an outcome (approximately 5% of cases identified via MR were disseminated for enforcement). In fact, the majority of those sent for enforcement come via the SM (approximately 56% of cases identified via SM were sent for enforcement). This indirectly increases attrition – if Crime Reviewers spend their time on these non-viable crimes, there is less time to spend on reviewing and disseminating viable crimes.

The effectiveness of the manual review criteria was also considered. As above, 60% of the crimes reviewed reached Crime Reviewers because they met MR criteria, rather than the SM threshold. However, the data showed that many of these cases were not suitable for dissemination for enforcement. In fact, of those crimes that reached a Crime Reviewer via the MR criteria, only 5% were disseminated. In comparison, 56% of those that reached a Crime Reviewer via the SM were disseminated. This could be partly because some of the MR criteria were designed to identify high harm / loss cases, which are not necessarily more likely to be suitable for dissemination. Similarly, certain crime types are selected for manual review (i.e. cyber-dependent crimes). This is because the SM was designed to identify viable fraud offences, rather than viable cyber-dependent crimes. Therefore cyber-dependent crimes were added to the MR criteria, to compensate for the weakness of the SM. However, these also do not tend to be viable, and so Crime Reviewer time is used examining cases that are known to be unlikely to be viable, rather than focusing on those assessed as more likely to be viable. For example of the 780 cyber-dependent crimes manually reviewed in the Phase 1 sample, less than 1% resulted in a dissemination.

Recommendations:

NFIB could consider making some specific changes to the MR criteria, ahead of the introduction of the new system, to understand how to make best use of the Crime Reviewers' time. For example:

- *Reducing the manual review threshold. For example, if the threshold were reduced to £5,000, this would mean an additional 3% of the sample could have progressed to review. Financial impact is subjective, and the amount lost is not directly proportionate to harm – some people could lose £1,000 and be relatively unaffected, while for others that sum could be their life savings.*

- *Review how MR criteria are chosen. For example, the inclusion of cyber-dependent crime codes does not appear to be the best use of time and resource.*

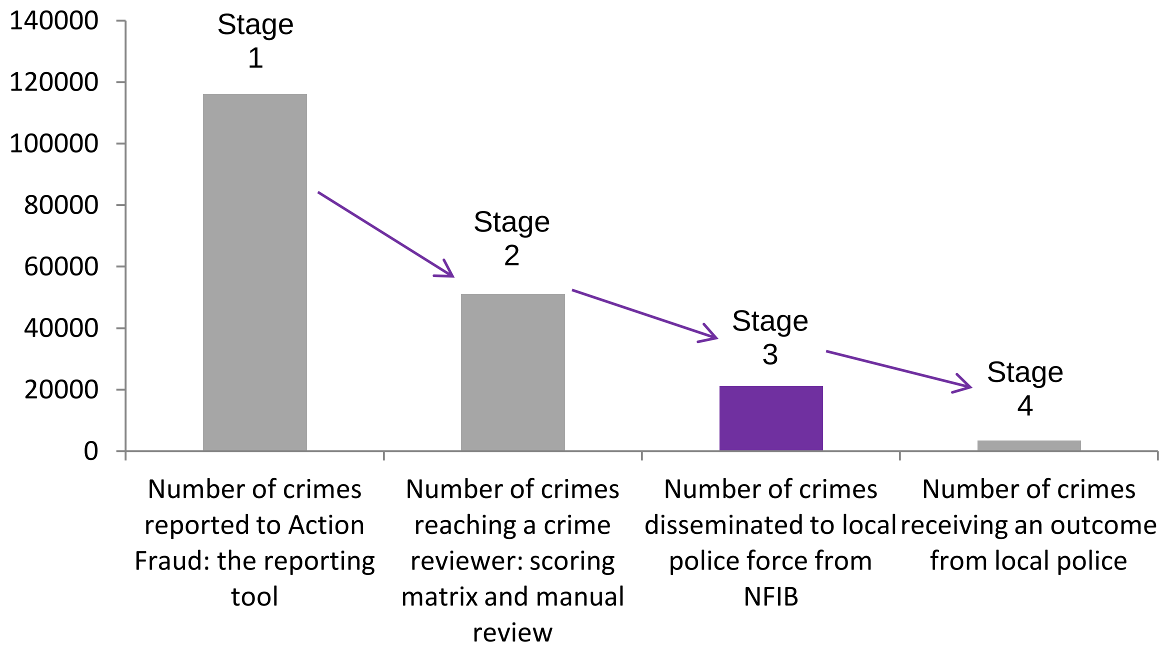
- *Consider including alternative MR criteria. For example, identifying cases where the victim knows the offender personally (which would require a corresponding amendment to the reporting tool, to gather this information), or cases where the victim has stated that the crime has had a severe impact on them (in this sample an additional 4% of cases could have progressed to review).*

In addition, it is worth NFIB looking at how they can record alternative, non-CJS / police outcomes for these crimes, to show the benefit of reviewing them and achieve recognition for their efforts. For example, if a case is disseminated for victim care / safeguarding as a result of the review process, this should be recorded.

7. Key Findings: Attrition Stage 3 – Dissemination of crimes to local police forces (and others) for enforcement

The third stage of the project considered the point at which crimes are disseminated to local police forces (and others) for investigation and enforcement. By improving the quality of information provided to Crime Reviewers through stages 1 and 2, it should be possible to increase the number of cases that are viable for dissemination. However, given NFIB's resource constraints it is likely that there is a limit on the number of additional cases reviewers could actually deal with.

Figure 4: Attrition flow model – Stage 3 (based on all crime reports received by Action Fraud, April – September 2013)



There were some residual issues around force responsibility for fraud and cyber-dependent crimes. When Action Fraud was rolled-out, some staff were led to believe that NFIB would send out 'arrest packages'

(which identified a candidate for arrest) rather than 'investigation packages' (which required further work by police).

In conversations with NFIB, and focus groups with Crime Reviewers, it became clear that some forces had an expectation that disseminations would contain sufficient information for forces to go straight out and arrest the suspect. This was echoed in interviews with some forces; staff / officers' perspective was that they had been told that with the roll-out of Action Fraud / NFIB they no longer had to investigate fraud. However, NFIB have never produced 'arrest packages', but rather packages containing viable leads for investigation. It should be made clear to all involved that NFIB do not provide arrest packages, and that forces are still required to investigate fraud.[24] It is essential for the success of the whole process that forces have a clear understanding of what they can expect from NFIB, and what they are expected to do.

Recommendations:

NFIB should refresh forces' guidance to show what they can expect from NFIB, and what their own roles / responsibilities are.

Police should also work to re-iterate responsibilities amongst forces, highlighting what they can expect from NFIB, but also what NFIB expect from them.

Forces reported that they sometimes receive packages with varying levels of detail, out-of-date information, and unclear networks. It is essential that NFIB consistently produce good quality packages, with monitoring to ensure standards are met. This will help to reduce attrition, as forces have better quality packages to take forward to investigation.

Interviews with forces found mixed feelings on the quality of the packages disseminated. Some participants felt that the quality was fine; others felt that the packages could be improved, while others still felt that the quality varied. In addition, some felt that NFIB's busier periods result in less detailed packages, and quieter periods result in more detailed packages. Thus it is important that NFIB are clear about their responsibility to consistently provide good quality packages, and monitor disseminations to ensure they meet minimum standards.

[24] In force interviews, participants reported that although they were clear that they still 'do' fraud, some officers are nevertheless under the impression that fraud is no longer the responsibility of local forces.

In interviews with forces there were some specific comments about packages containing out-of-date information, such as suspect addresses. This was despite the force being able to find current / correct data on the Police National Computer (PNC) (and therefore feeling that NFIB should be able to do this, given they have access to the PNC).

Another issue raised in interviews relates to the way that NFIB build networks of crimes. In general, forces and stakeholders appreciated and acknowledged the benefits of the networking capabilities of the NFIB. They reported that these aid understanding of the scale and nature of the threat in their area, and also offer better opportunities to tackle offenders in their area. However, forces reported that it is sometimes hard to understand why particular crimes have been networked. One example was a network in which all crimes were committed on EBay, and this was perceived by forces to be the only reason given in the dissemination email for linking the offences. For the force, this was both unhelpful from an investigative perspective, but also undermined their confidence in NFIB.

As above, these kinds of issues reduce the resource available to investigate frauds disseminated to local forces, contributing (albeit indirectly) to attrition.

Recommendations:

NFIB should implement methods to monitor the quality of the disseminations, for example via the NFIB's National User Group (NFIB's group of Specific Points of Contact in local forces), or (more extensive) auditing of disseminations. NFIB should also establish a system to audit the quality of packages that are disseminated, and also a system to gather feedback from forces on the quality of the packages (for example via the National User Group meetings).

Depending on the findings of (ongoing, regular) audits, NFIB should ensure that quality is consistently achieved. There is of course a balance to be achieved between ensuring cases are disseminated in a timely manner, and ensuring they are of sufficient quality.

NFIB should ensure that all Crime Reviewers give explicit reasons for networking crimes, for example highlighting the common entities. This could also form part of the quality-audit.

Interviews with forces also highlighted some concerns around the size of networks. Forces have found it difficult to manage very large networks, both practically (because of limitations of record management systems) and in investigation terms – e.g. having to update 100 victims is time consuming.

Very large networks can be difficult to manage, both in practical terms (some force IT systems are limited to 99 victims per crime, others accept more but this requires that staff are available to enter all those crimes onto the system), but also in terms of staff confidence (large networks can seem daunting, requiring 10s / 100s of statements to be taken from victims, updates to be given to victims, etc). In addition, large networks can have an impact on outcomes, and therefore attrition. One force highlighted the problem that with large networks, outcomes will not always be achieved for the whole network (the decision may be made to charge a suspect with 10 out of the 100 crimes). Thus despite working on a 100-case network, the officer ends up only being able to outcome 10 crimes, leaving 90 crimes which seemingly have no outcome, despite vast effort. However, with the introduction of the new outcomes framework (see Annex B), this issue should be resolved, as there is an alternative outcome that can be used to reflect the work for the 90 crimes which did not result in a charge.

Recommendations:

These large networks appear to reflect changes in the nature of crime, and may even become more common as the number of reports of fraud increases (as there are more opportunities for links to be drawn). Forces should therefore consider how best to manage these large networks going forward, in terms of their own record management systems, resourcing the investigations, and ensuring all appropriate outcomes can be recorded and returned to NFIB.

It would be helpful for NFIB to look into the issues with outcomes – to what extent do portions of networks receive outcomes, and is there scope within the new outcomes framework to take this into account, to reflect the fact that a suspect has been identified, even when no charges are brought.

Interviewees also raised concerns around the speed of disseminations. For cyber-dependent crimes in particular, the feeling is that ‘speed is of the essence’ to maximise the chances of apprehending an offender. However, this is not considered within the current system.

The timeliness of packages was raised in interviews with forces and other stakeholders, with some reporting that ‘time is of the essence’, particularly for cyber-dependent offences. In interviews stakeholders who work with cyber-dependent crime said that such crimes are often still in progress when they are reported, so getting those packages / crimes through the system and out for investigation speedily is key to success. In addition, there is a risk that further offences will be committed; if dissemination is done quickly, there may be opportunities to prevent further offences / offending / victimisation. This was less of a concern for individuals dealing with fraud.

Recommendations:

As part of their new system, NFIB should look to work with key stakeholders (e.g. ROCUs, NCCU, relevant staff within local forces) to develop guidance on where it is important to disseminate packages quickly, and then put in place processes so that these cases can be swiftly identified, and then 'fast-tracked' through the system.

Throughout the project, NFIB were keen to highlight the beneficial work they do that does not result in a law enforcement outcome. This includes work such as disruptions, and disseminations for safeguarding of victims. However, to understand the scale of this work, and therefore the true scale of attrition, such information needs to be recorded transparently and consistently.

This finding was supported by looking at the data sampled for Phase 1 of the project, which showed that while disseminations for enforcement were recorded on Sharepoint, other actions such as safeguarding disseminations were more difficult to identify. It is important that for every crime / network reviewed there is a record of the type of dissemination, and the reason for dissemination. If there is no dissemination, the reason for that decision should also be recorded.

Forces may receive packages that, upon dissemination appear to meet the threshold of a crime, but following further investigation do not. The force can 'no crime' these cases on their own system, but some interviewees were concerned that even once this is done, and NFIB are informed, that crime(s) will not be removed from the dissemination 'numbers', therefore it will still affect their outcome rate (i.e. if they receive 100 outcomes one month, no crime 30 of them, and achieve a 'positive' outcome for 50, their 'positive' outcome rate will still be 50%, rather than just over 70%).

Recommendations:

NFIB should ensure that Sharepoint can record non-law enforcement disseminations (and the reasons for those).

NFIB should refresh guidance for Crime Reviewers, to highlight the importance of accurate data recording. Guidance should include instructions to ensure that the outcome of any review is recorded (whether there is a dissemination or not).

NFIB should conduct an audit of Sharepoint records, both to ensure that guidance is being followed, and to identify potential areas for improvement.

NFIB should consider, with forces, whether or not cases that are no crimed by a force (following further investigation that shows no crime has occurred) should be removed from the dissemination numbers. Either way, outcome rates should reflect the number of cases that are crimes, rather than potentially being based on disseminations that are not crimes.

As in Stage 1, double-keying is also an issue in Stage 3, where forces have to record crimes / networks disseminated to them on their own record management systems. This can be an onerous, time-consuming task. If a force gives this responsibility to only one person, there is a risk that double-keying will not happen if they are absent from work for any reason. This can delay investigation / enforcement, thus impacting on the likelihood of achieving an outcome, and contributing to attrition.

As mentioned in the Stage 1 findings, “double-keying” describes the process by which local forces have to record information on their own system, in addition to it being recorded on the Action Fraud / NFIB systems. This issue was raised throughout the project, particularly in interviews with police forces, but also in conversations with NFIB. Forces have to double-key all disseminations they receive onto their own system, so that crimes can be allocated to teams / officers, resources managed, etc. This is pure duplication of work, and can take considerable time. For example in one large force there were three full-time members of staff who entered all disseminations onto the force system (and it was anticipated that this would increase).

Further to this issue, there is also the issue of who is responsible for doing the double-keying (which relates to the previous point). In some interviews, forces mentioned that one or two people are responsible for the double-keying, which works well (as they are experienced, therefore quicker) until one or both are on leave / absent for some reason. Disseminations then simply sit in the forces’ email inbox until they return, which delays potential investigations.

Recommendation:

As part of the new system NFIB should look for ways to reduce the burden on forces caused by double-keying of disseminated cases, for example by providing access to their system so that forces can download the relevant information, rather than the current process of disseminations, which are in PDF format.
Forces should ensure that there is sufficient capability / back up staffing to ensure that disseminations are acted on promptly.

There is scope to improve the ways that forces work together. For example, when transferring crimes between forces interviewees reported that there are issues around transferring 'ownership' of the victim, and relevant information, and delays while allocation decisions are made. Interviewees also stated that there can be difficulties around force collaboration (e.g. to take statements) when victims / witnesses are in different force areas to the suspect (where the crime will typically be allocated).

From the perspective of NFIB, transferring crimes between forces should be a simple process. If a force has been sent a package, and they believe it is better placed elsewhere (e.g. because there is evidence that the suspect resides in another force area), they should contact their force's transfer SPOC, who will make the request to NFIB, who will then send the package to an alternative force (if they agree that it does belong elsewhere). The second force is then responsible for requesting any additional information from the first force.

However, from the perspective of interviewees in forces, there do appear to be some problems around this process.[25] In interviews, it became clear that the additional stage of having to go via NFIB is causing some issues. For example:

- There are delays because the first force has to wait while the NFIB decide where it should be allocated, and then whether or not the second force has accepted it.

- Some forces will amend the case(s) on their system, once it has been sent to the NFIB, to reflect that they are no longer dealing with it (as far as they are concerned it is no longer their responsibility). However, the victim may then contact that force to get an update, as they have received a letter from the NFIB stating that that force has been allocated their crime. The victim can then

[25] It should be noted that there are also issues around transferring 'regular' crimes, e.g. when forces won't accept a transfer

be told the force is not dealing with the crime (by someone who did not deal with the case themselves, and therefore can only give limited explanation to the victim), which is obviously a poor service for the victim.

- In interviews, some forces stated that they had concerns that they were not getting all of the information available when they accept a transfer, as they simply received the original dissemination package from NFIB. This can then lead to duplication of effort, as the second force repeat the same work to gather the same information.

Because of the nature of the crimes that NFIB deal with, forces may receive packages for investigation where victims and / or witnesses are spread across different force areas. There are two main ways that forces can get statements from those individuals:

1. Contact the individual themselves, via email or telephone, to take the statement ('remotely').

2. Put a request in to the force in which the individual lives, for an officer / PCSO to visit the victim / witness, and take a statement.

In interviews, some people were happy to take statements 'remotely', provided the victim did not appear to be vulnerable / require a face to face visit for some other reason. However, others felt that this was not appropriate, and that victims should be visited in person. Therefore, they would request that the relevant force would do said visit, and take the statement. However, there is no formal requirement that forces cooperate on this, so getting the statement taken is often down to the goodwill of the force. Interviewees reported that they have had difficulty persuading forces to make such visits on their behalf. This appears to be because of a combination of differences of opinion (some forces feel remote statements are fine, others do not, and if the force being asked is comfortable with remote statements, they may be reluctant to allocate resource to take a statement when (in their view) this is not necessary), some forces making many more requests for assistance than they receive (particularly for larger forces who receive more of the disseminations), and forces who take the statements feeling that they do a good proportion of the work with little recognition for it.

These issues are likely to have a direct, negative impact on the victim's experience, and can also affect attrition, if investigations are adversely affected by delays etc.

Recommendations:

To resolve these issues NFIB should re-iterate guidance on transferring crimes to forces, and forces should ensure that this is disseminated to the relevant staff / officers.

Forces should ensure that transfer requests go through their force transfer SPOC as a matter of routine.
Forces and NFIB should also work together to ensure that victims have a clear point of contact, even when their crime is transferred. This could be achieved by, for example, requiring that victims are contacted before the force 'no crimes' / transfers the offence, or similar.

Police should develop guidance on what forces can (and should) expect of one another in such circumstances. It is understandable that some individuals prefer not to take statements remotely, and that forces may find it difficult to provide resource to assist with other forces' investigations, especially when this effort is not reflected in their own outcomes data, but issues such as these have a negative impact on the investigation, and the victim experience. They can also generate more work for officers in the longer term, as agreements need to be reached each time such a situation arises.

Logistic regression identified a number of features of reports that affect the odds of a crime being disseminated. However, due to complexities of the system and issues with data quality these should only be used as guidance, rather than having a concrete association with dissemination, or not.

The quantitative data was also used to conduct a form of analysis called logistic regression, which was used to look at those features of a crime that 'predict' whether or not a crime was disseminated for enforcement. However, a number of data quality issues mean that these features should not be considered as any more than a guide to what may contribute to a crime being disseminated:

- As discussed previously, difficulties people experience when using the Action Fraud reporting tool can impact on the quality of the data. This meant that the dataset used for this analysis had a combination of missing and poor-quality data.
    - Due to the way the questions are asked, it is not possible to tell whether 'blank' cells were not completed by the reporter even though they had something to add, or whether they are blank because the reporter genuinely had nothing to add.
    - We know from looking at the data that sometimes information provided in the free text was not put in the correct 'tick' boxes. For example a reporter would write in the free text box that they had lost money, but

would not tick the corresponding box. Therefore that information could not be captured in the logistic regression (and there was not the resource available to go through all the free text boxes to identify such errors).

  - Data that was put in the correct fields sometimes appeared to be incorrect, e.g. numeric strings that were entered in phone number fields that did not correspond to a typical phone number structure.

- In addition to the problematic Action Fraud data, the dataset also contained data from NFIB’s Sharepoint system, where Crime Reviewers record what actions they have taken. However, this is not always completed consistently or accurately. For example, 56% of the cases that reached a Crime Reviewer had no Sharepoint data available. As this project used Sharepoint data to determine disseminations and outcomes (amongst other things) it is possible that in reality there are more disseminations and outcomes than were recorded on Sharepoint, and therefore that we knew about (see Section 10 for more information).

Due to these issues with the quality of the data, no statistics will be presented alongside the logistic regression models. Although the models generated are interesting in terms of what factors are included, we do not have sufficient confidence in the quality of the data to say that any one factor has more influence than another.

Two logistic regression models are presented here. The first examines factors that go into NFIB’s Scoring Matrix, to try and understand whether there is any associate between these factors, and a crime being disseminated to police for enforcement. However, due to the issues with data in general discussed above, and the complex algorithms that make up the Scoring Matrix, it was not possible to conduct a true ‘test’ of the Scoring Matrix. Instead, a simplified approach was taken, using the presence or absence of Scoring Matrix factors to identify any association with dissemination. The logistic regression analysis suggests that factors which increase the odds of dissemination are:

- Presence of vehicle registration information;
- Presence of a suspect’s sort code;
- The presence of a suspect phone number.

The model also showed that crimes that are cyber-dependent have lower odds of dissemination than frauds.[26] It is perhaps not surprising that cyber-dependent crimes are less likely to be disseminated than frauds; because of the nature of these offences, reports tend to include less useful information (e.g. cryptolocker or ransomware cases contain very little to go on). Looking at

[26] This finding may be influenced by the data quality issues discussed above.

what makes a crime more likely to be disseminated, it is possible that phone numbers, vehicle information or sort codes offer routes to identifying suspects, and therefore are considered viable by Crime Reviewers. Of course, this does not mean that other aspects of the report do not contribute to the Crime Reviewers decision to send for enforcement, but this is an area in which NFIB should do more work.

A second regression model was used to look at what factors, other than those in the Scoring Matrix, might be associated with dissemination. This could give insight into what could be considered in future scoring approaches. Factors related to features of the crime, and victim characteristics, were used in the analysis. Those found to increase the odds of a dissemination are:

- A payment having been made, versus no payment being made;
- The victim being a business rather than a member of the public;
- A victim stating that they have evidence in the form of call recordings;
- A victim stating they have emails as evidence.

As outlined previously, due to concerns around the quality of the data, these factors should be treated as a guide, rather than clear statements of what information will predict a dissemination. The fact that certain types of evidence, or a payment being made, increase the odds of a dissemination seems intuitive. It is interesting that reports made by business victims are more likely to be disseminated by a member of the public; perhaps this is related to the amount of money lost, or businesses giving better quality reports. It is also possible that businesses are more often the victims of certain types of fraud (for example Counterfeit Cashiers cheques, Mandate fraud, Application fraud) which may in turn have a higher likelihood of dissemination.

Certain features were found to reduce the odds of a dissemination: the victim listing themselves as ‘other’ rather than being a member of the public, and a victim reporting via the contact centre rather than the online reporting tool (see Annex D for full details). This finding in particular is worthy of further consideration – it is unlikely that the contact centre in itself is making cases less likely to be disseminated; instead it seems likely that this is reflecting something about the crimes themselves, possibly that the contact centre takes more complex crimes or those that tend to have less information. Another possibility is that the contact centre tend to be used by users with increased ‘need’ of some kind, or that those who report via the contact centre tend to make poorer witnesses. However, these are only suggestions and further research is required to confirm these.

Recommendations:

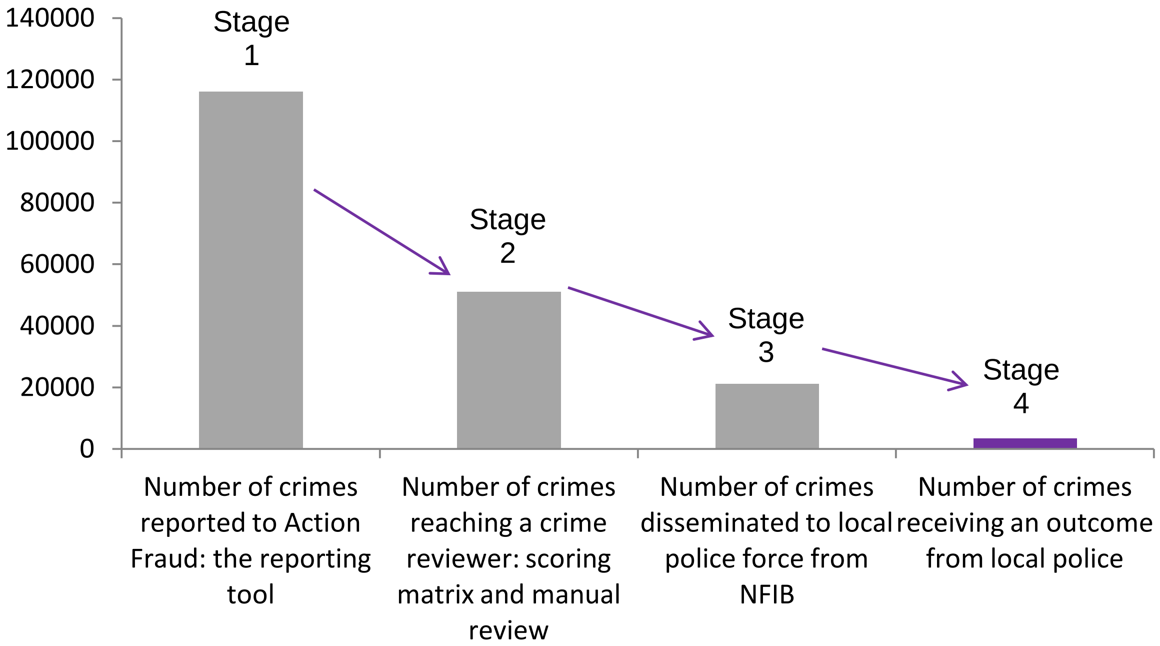
NFIB should consider how the findings on which aspects of the scoring matrix contribute to likelihood of a dissemination could be used in work on new approaches to scoring. For example NFIB should consider whether the findings around crime and victim characteristics could contribute to new scoring approaches – for example, taking into account the presence of evidence.

NFIB may want to look in more depth at why cases reported via the contact centre have lower odds of dissemination than reports made online, to get a better understanding of what it is about these cases that cause this – e.g. are they different fraud types, different quality reports, etc.

8. Key Findings: Attrition Stage 4 – Crimes being investigated by, and receiving an outcome from, local police forces

The final stage of the project considered the point at which crimes achieved an outcome (or not) by local police forces (and others), and that outcome information is returned to NFIB. Improving the number of outcomes returned to NFIB would reduce attrition, and also improve understanding of how many frauds and cyber-dependent crimes are achieving some kind of CJS outcome.

Figure 5: Attrition flow model – Stage 4 (based on all crime reports received by Action Fraud, April – September 2013)



At the time of this project, a considerable number of forces were still not consistently making monthly returns, and so the known outcome rate is likely to be an underestimate.

This is likely to be one of the key reasons for the low outcome rate for NFIB offences. At the end of this piece of research, around 20 forces were consistently making monthly returns, meaning around half of all forces were still not consistently providing outcomes information to NFIB. It is not possible to say what the effect would be on the outcome rate if the remaining forces were to begin making consistent returns, but it is probable that outcome rates would improve. Thus this is likely to be a key part of the attrition in these crimes.

Recommendation:

NFIB should continue to work with forces where outcomes are not consistently returned on a monthly basis to ensure that returns do become consistent.

In addition to sending packages to local police forces, NFIB also send packages for enforcement to other organisations, such as Trading Standards, and the Insolvency Service. However, these organisations do not use the same outcomes framework as the police, and (at the time of writing) do not return outcomes information to the NFIB.

Despite sending packages for enforcement to non-police organisations, there is no framework by which they can inform NFIB of any outcomes achieved. In the six months to September 2013, over 2,000 cases were sent to such organisations, but there were zero outcomes returns. This is in part because these organisations do not use the same outcomes framework as the police. But also because there is simply no formal process / arrangement by which these organisations are required to send returns. Exacerbating this is the fact that if these organisations were to take on an investigation and achieve an outcome, this would then go into Police Recorded Crime figures. Thus there are concerns that the work / achievement of the non-police organisation is not recognised / acknowledged.

This is a key point for attrition – it is possible that the outcome rate would be higher if these organisations could provide data on outcomes.

Recommendations:

NFIB should work with these organisations to understand how such outcomes could be captured – for example to establish whether there is scope for a ‘positive outcome achieved by other party’ option. This would give credit where it is due, and would be a more accurate reflection of performance.

In addition, NFIB should work with the organisations to highlight the importance of getting feedback when packages are disseminated. It may be that NFIB need to be more proactive with these cases than those sent to police, given there is no requirement / mechanism for such organisations to return information.

Double-keying causes problems at this stage as well. The process by which outcomes are returned requires forces to double-key outcomes information from their own record management systems onto a spreadsheet provided by NFIB. Approaches vary across forces, but this can be time consuming, and is heavily reliant on there being well-designed processes to capture necessary information.

Interviews with forces showed that the ‘double-keying’ issue arises again at this final stage. In order to return outcomes data to NFIB, forces have to identify and extract the data on their own systems, and then add it to a spreadsheet provided by NFIB, which asks for information such as suspect details, outcome, NFRC number, etc. The spreadsheet should be returned to NFIB on a monthly basis. The amount of work this requires varies considerably, depending on the approach taken. There appear to be two main ways for forces to gather outcomes data:[27]

1. Manual: Forces look up the relevant data on their systems (case-by-case) and type (or copy) that information into the NFIB spreadsheet. In these cases they are typically reliant on officers informing them that an outcome has been achieved for a crime.

2. Automatic: Some forces have designed automatic processes which can run a query on their system to identify any crimes with a fraud / NFIB marker that have an outcome. The necessary information is entered into the NFIB spreadsheet. This process is reliant on the marker being applied correctly.

In interviews, forces doing manual returns reported that they spend a considerable amount of time doing this, e.g. a few days a month, or an hour or so every day, depending on how the work is broken up. They felt that this was a considerable amount of work. Some interviewees felt that it would be helpful if they could record outcome information directly onto the NFIB system, rather than the spreadsheet approach. In forces where the system is automated the process is obviously faster, but they did highlight the considerable time spent in designing and testing the automation process.

Additionally, there are issues in both approaches that may be cause for concern. In general, identifying cases for which there is an outcome relies on a marker being attached to a crime, or the officer notifying the person collating outcomes data that an outcome has been achieved. With both there is a risk that outcomes may be missed. It was not possible to gauge how likely this is to be a problem, or the likely scale of the problem; understandably staff were

[27] It should be remembered that the interviews on which these findings / recommendations are based only captured views from seven forces. It is entirely possible that other approaches are used by the remaining 36 forces, and that these pose different challenges.

reluctant / unable to put a figure on it. However, anecdotal evidence from conversations with NFIB suggest that one large force could have 2,500 crimes that have not been reported to Action Fraud, of which 600 have outcomes attached.

Recommendations:

NFIB should investigate options in the commission of their new system to simplify / speed up the outcomes returns process.

Given that some forces have managed to automate the returns process, forces should share knowledge / expertise with each other on how this can be done. Although forces run their own IT systems, as some use the same providers (e.g. Athena, Niche) it should be possible to share learning.

Police should reiterate the importance of accurate record keeping, to minimise the risk of 'missing' crimes that have outcomes attached.

Forces should investigate the possibility of audits to identify 'missing' crimes. While some systems may not allow for this, consideration should be given to alternative approaches to identify NFIB cases that have outcomes that have not been flagged properly, such as key word searches, or audits of cases disseminated by NFIB where no outcome has been returned, etc.

Interviews showed that in some areas responsibility for providing outcomes information to NFIB rests with one person. This is typically because of the complexity of the process, and can increase efficiency. However, if that person is absent from work, the returns may not be completed. This can cause (temporary) falls in outcome rates, followed by an (artificial) increase when the person returns to work.

Interviews highlighted that as well as issues around the administrative burden of the outcomes returns, there are also issues caused by way that this work is allocated. In some forces one person tends to be responsible for collating and returning outcomes data. If they are absent (e.g. because they are on leave, or they retire) it is likely that the outcomes return will simply not be done. There are various reasons for this, e.g. other staff not realising that the task needs to be done, nervousness / reluctance of other staff because tasks related to the NFIB are perceived to be difficult, or other staff not knowing how to do the return. This means that outcome rates could be artificially skewed; negatively when people are not at work, and positively when they then return, and send outcomes to NFIB for multiple months at once.

Recommendations:

Forces should ensure that there is more than one person who is capable of making the monthly returns, and must ensure that where the main member of staff is not available, a second person will step in, to maintain consistency.

As at Stage 3, logistic regression was again used at this stage, this time to look at what features may be associated with whether or not a crime has achieved an outcome. Again, factors identified should be seen as guidance, due to data quality.

Logistic regression was used again to look at what aspects of the Scoring Matrix may be associated with an outcome being achieved. As before, this was to try and understand the efficacy of the Scoring Matrix, given its purpose is to identify 'viable' crimes. However, as discussed previously due to issues with the quality of the data the findings presented here are merely indicative of factors that may affect whether or not a crime achieves an outcome. Again, there is not sufficient confidence in the data to indicate which factors may be more important than others.

A second logistic regression was run to understood what other features of the crime, or victim characteristics, might be associated with achieving an outcome.

The analysis looking at the presence / absence of scoring matrix factors (see Annex E for full details) identified two factors that gave higher odds of a crime having an outcome:

- Presence of a suspect mobile phone number;
- Presence of a suspect sort code.

There were three factors that gave lower odds of an outcome:

- Presence of a (suspect) organisation phone number;
- Presence of a suspect email address;
- Presence of a suspect payee name.

It seems possible that these are reflective of the crime rather than inherently affecting whether or not there is an outcome. For example, having a suspect mobile phone number and the presence of a sort code may be reflective of a payment being made (which also increases the odds of an outcome, see below).

As before, another analysis was done using other features looking more broadly at the crime and the victim. In this analysis four features were found to increase odds of an outcome (see Annex E for full details):

- Evidence in the form of call recordings / texts;
- A payment having been made (versus no payment);
- The offence being an online fraud, rather than an offline fraud;
- Dissemination within 14 days of a report.

It is likely that some of these are likely to reflect wider aspects of a crime. The crime being disseminated within 14 days of the report being made is likely to a proxy for other factors, such as:

- That some types of crime are disseminated quickly, for example simpler frauds, with more information that are therefore ‘easier’ to disseminate and investigate.

- It may also reflect police attitudes; they may see a case as more ‘solvable’ if it is a more recent dissemination / report.

It is very unlikely that it is the speed of dissemination which inherently affects whether an outcome is achieved or not. Thus this should not be interpreted as suggesting that simply increasing the speed of dissemination will automatically boost outcome rates – there is no point sending packages out quickly, if they are of poor quality. However, if good quality packages can be disseminated quickly then it may impact officer perception and therefore encourage better outcomes. Similarly, online frauds are probably not inherently more likely to get an outcome, but could reflect better networking capabilities. There are also factors that appear to reduce the odds of crimes achieving an outcome:

- The presence of evidence in the form of emails or online transcripts.
- The victim being female (rather than male);
- The presence of evidence in the form of contracts or other legal documents;

Similarly it is likely that these kinds of evidence are more common with other fraud types, such as land scams or investment frauds, which are simply more complicated and therefore less likely to achieve an outcome.

9. Other notable findings: Vulnerable victims

Vulnerable victims are not consistently identified using one clear definition of ‘vulnerability’, and there are different processes for identifying vulnerable victims based on whether they report via the call centre, or the online tool.

Discussions with NFIB raised a number of issues relating to how vulnerable victims are defined and identified.

During this project, there are two ways by which Action Fraud / NFIB could identify ‘vulnerable’ victims – **firstly**, the call centre could identify callers as vulnerable, using ACPO guidance.[28] In these circumstances, victims would be referred to their local force, for the force to deal with as they see fit (e.g. a PCSO may visit to offer reassurance / advice on how to avoid becoming a victim of fraud again).

If a report was made using the online reporting tool, unless a case happened to reach a Crime Reviewer (because it met the scoring threshold, or one of the ‘manual review’ criteria), it was not possible to routinely or purposefully identify individuals who fell under the ACPO guidance.

The **second way** that people could be identified as ‘vulnerable’ was if they ticked one of three boxes on the reporting tool – saying that they felt vulnerable because they were at risk of losing money, because they were a repeat victim, or because they were a regular target (‘vulnerability boxes’). It should be noted that these are not necessarily accepted views of ‘vulnerability’, but the questions did ask victims if they felt vulnerable. These reports are not selected for automatic / manual review, and are not automatically referred to local police for a service.

Thus, if a vulnerable victim makes an online report, at present they will not be identified as vulnerable by Action Fraud. However, NFIB review approximately 50% of all crimes reported to them. Therefore, a good proportion of those who tick the boxes, or mention some vulnerability in the free text box, will be

[28] Determined by adult safeguarding guidelines, which define a vulnerable adult as anyone over 18, who is / may be at risk of abuse because of mental or other disability, age, or illness, who is / may be unable to take care of themselves, or to protect themselves against significant harm or exploitation.

reviewed, by virtue of the fact that they meet the scoring threshold, or one of the manual / automatic review criteria, such as crime type. Therefore, some vulnerable victims who report online will end up being disseminated to forces for enforcement, although this is by chance, rather than by selection due to their 'vulnerable victim' status.

In addition, an NFIB Crime Reviewer could decide that a victim is vulnerable - this decision is made in accordance with the ACPO guidelines, but also using their own opinion, and not using a standardised Action Fraud / NFIB definition. In this instance, the Crime Reviewer can send that case to the victim's force for the police to deal with (if that is not already happening). This means that some of those who are 'ACPO vulnerable' and who report online, will still be identified and still receive a service from the police. However, this can be difficult as the Crime Reviewers are simply relying on what was written in the report.

However, the varying definitions and routes to be identified as 'vulnerable' may mean that some individuals who require a service are not receiving one. This project identified some risk for a small group of people who:

- had ticked the vulnerability boxes;
- had not been reviewed or disseminated; and
- had not been reported separately by the police.

Within this group, some individuals may have met the definition of vulnerability in accordance with ACPO guidelines. Another group potentially at risk is those where third parties (e.g. a relative or carer) report on behalf of a vulnerable victim. In many (but not all) cases no referral is made under these circumstances, as Action Fraud / NFIB consider that the victim is already cared for, and therefore does not require an additional service from the police. However there is no standard guidance on the third-party reporting process.

It should be noted that from the evidence available, this risk may be present for those reporting online and those who report via the contact centre, but it could be assumed that online reporting is particularly problematic for identifying vulnerability, because the informant / victim does not get to speak to a call handler.

Recommendations:

Determine what is meant by 'vulnerable':

- *For example, does this include people with learning difficulties, mental health problems, physical health problems, particularly old or young victims, those who are repeatedly victimised, those who have lost large amounts of money, the recently bereaved, etc.*
- *Specifically, if a third party reports on behalf of the victim, consider whether this person should be treated as 'vulnerable' if they meet other criteria, or whether the presence of a third party removes the requirement to offer some safeguarding service.*

- *Consider whether there are different criteria that make people vulnerable to fraud and / or cyber-dependent crime, compared to other crime types.*

NFIB should think about the purpose of identifying vulnerable victims and how that relates to defining vulnerability. For example, if it is to stop people being repeatedly victimised, then it is important that repeat victimisation is a part of the criteria for identifying vulnerability. NFIB should think about who should be involved in creating the definition of 'vulnerable victim', and how it will be used. It seems sensible for Action Fraud and NFIB to have a consistent definition, but consideration should be given to whether forces should also use this definition, or simply be made aware of it. In addition, NFIB may wish to consider how forces define vulnerability.

Once a definition of vulnerability is established, NFIB should begin work on how these victims can be identified, with particular focus on the online reporting tool. It is essential that this is a part of the new system, and that questions are extensively tested to ensure that they work in identifying people appropriately.

When the questions are in place, NFIB should consider tailoring the scoring system to identify vulnerable victims whose cases should be reviewed, or indeed to automatically alert forces to the presence of any vulnerable victims in their force area.

10. Other notable findings: Auditing ability

There appear to be some issues around the ability of NFIB to audit their own data / systems, because of weaknesses in those systems. For example, it is not possible to audit how 'well' the SM is working, or whether the MR criteria are making best use of resources, etc.

NFIB use two main systems, Know Fraud and a Sharepoint system. Sharepoint was introduced to compensate for weaknesses of Know Fraud, and is largely used to record information about what has happened to crimes post-report, i.e. what decisions Crime Reviewers have taken. For this project, data from both Know Fraud and Sharepoint was required. In requesting this data, a number of issues came to light. For example:

- Accurate documentation for the SM was not held by NFIB. NFIB provided the research team with a copy of the SM from their contractor / supplier. However, it then transpired that the matrix had changed since its introduction, and the changes were not reflected in the documentation. Again, NFIB had to go to their contractor to clarify how the matrix was working in practice, with the contractor having to get that information direct from the system (rather than either party holding accurate master copies of important documents).

- There were similar issues with the manual review criteria, with delays because of difficulties establishing the financial thresholds for manual review. This again highlights the importance of NFIB ensuring they have accurate and up-to-date records, and that any changes to reviewing criteria are documented (along with dates for such changes).

- During this project, NFIB did not know 'where' their data was stored, i.e. what fields in their database correspond to what questions on the reporting tool. This made it difficult to get access to the necessary data, and resulted in delays in the project, due to the 'trial and error' approach used to identify data. If not resolved, as NFIB become more established and begin to do more work with other organisations (e.g. academics, local forces), this may continue to be problematic. It is also important that this is considered with the introduction of the new system.

- Some of the Know Fraud data was not easily accessible by NFIB, with them having to pay the contractor to get that data. Again, this caused delays to the project, and meant costs were incurred, both financial and in terms of staffing. The fact that some data is only accessible by contractors limits the auditing that NFIB can do. They can look at scores individually, and amend thresholds themselves, but getting information, for example on all crimes with a specific score, is more difficult.

- Data held on Sharepoint can be patchy. Staff do not always complete this consistently or accurately. As a result of incorrect data, some of the analysis for this project had to be repeated / re-done. In addition, because of the patchy nature of the data the analysis that it was possible to do was limited. In the 'real world', this means that when questions are asked about specific cases NFIB may not be able to immediately find information about what decisions were made about a crime, but instead have to go back to the crime to try and 'guess' why e.g. it was not disseminated.

These issues were problematic for this project, causing delays and limiting what analysis could be done. However, they are likely to reach beyond just this project; as mentioned above other organisations are beginning to make data requests to NFIB and it is possible the same issues will be encountered repeatedly. With the introduction of the new system, there is an opportunity to eliminate these issues and build in auditing abilities. Better ability to 'audit' the system will mean better understanding – of how well scoring approaches are working, how well staff / resources are targeted, and what has happened with crimes / networks, all of which will strengthen NFIB in their work.

Recommendations:

As with the SM, it is important that in the future NFIB hold accurate documentation on all such systems, and that if any changes are made, the documentation held by both parties is suitably updated.

NFIB should ensure staff a) record the data, and b) record the right data, and that auditing arrangements are put in place to ensure this.

In the period before the new system is introduced, NFIB should work with Crime Reviewers to emphasise the importance of recording the correct data in the correct places.

NFIB should reduce the need for duplication in the new system – all these facilities should be part of one system / database, which can be viewed in multiple ways.

11. Discussion / conclusions

This is the first project of its kind to look at attrition in reported fraud and cyber-dependent crimes. The purpose was to identify where attrition happens, from the point of a victim (or their representative) making a report to Action Fraud, through to the point at which an outcome is achieved (or not) by the police. In addition, the project was designed to understand more about why attrition happens, and how it could be reduced.

The aims of the project were as follows:

1. To work with Action Fraud / NFIB to establish overall outcome rates and levels of attrition for the fraud and cyber-dependent crimes they deal with.

2. To understand where attrition is occurring in the recording and investigations process and the key factors driving attrition.

3. To draw comparisons between the outcome rates of offences reported to Action Fraud / NFIB, and of 'traditional' crimes.

4. To help identify possible methods to reduce attrition where necessary.

To work with Action Fraud / NFIB to establish overall outcome rates and levels of attrition for the fraud and cyber-dependent crimes they deal with.

Throughout the project we worked with NFIB to establish what the outcome rates are for the crimes they record, and to determine levels of attrition. At the start of the project, the outcome rate was 2% (for the period April – September 2013). Since then, the outcome rate has gradually increased, with the most recent data for 2014/15 showing that the outcome rate was around 5% (using the old 9-outcome framework).[29] [30] [31]

[29] In order to make meaningful comparisons between years, this outcome rate is calculated based on the number of reports recorded in this period by Action Fraud, and does not take into account the inclusion of reports from the FFA and CIFAS (which were added to the overall crime count in October 2015). If these offences are included, the outcome rate is nearly 2%.

[30] As mentioned previously, there are caveats to this increase: First, the later time period means that there are simply more crimes for the police to attach an outcome to, compared to the earlier period in

What is important in the future is to look in more detail at what is captured in the ‘outcome rate’ – as discussed previously, the outcomes framework now captures a whole variety of different types of outcome, including those where no offender has been identified. It is important that it is possible to distinguish between ‘positive’ outcomes (i.e. where an offender has been identified and some sanction applied), and ‘negative’ outcomes (i.e. where no offender has been identified, or if they have been, no action has been taken). In addition, it may be beneficial to add a ‘time stamp’ to outcomes. This would serve two purposes. First, it would enable Home Office Statistics to monitor how quickly outcomes are applied. This would give more information around whether any delays are due to (for example) staffing issues, or because cases genuinely take longer to investigate and resolve. Second, it would allow calculation of a ‘true’ outcome rate – at present the outcome rate is calculated by looking at how many offences are sent to Force X in one month, and how many returns are made in that same month. This gives an ‘aggregate’ outcome rate. However, with a time stamp it should be possible to calculate the ‘true’ rate, reducing the distortion of outcome rates that is caused by the time lag between dissemination and outcome.

To understand where attrition is occurring in the recording and investigations process and the key factors driving attrition.

The project has identified attrition at all four stages – at the point of recording, during the scoring process, when crimes are disseminated to forces (and other organisations) for enforcement, and when outcomes are returned (or not to the NFIB). These results of the analysis at all four stages can be distilled into three themes:

1. *Accurate and timely recording of information*

At all stages of the process, there were problems with information being accurately recorded in a timely manner. At the first stage, issues were identified with understanding of how to complete the tool, and the functionality of the tool (e.g. that reports cannot be updated at a later date). At the next stage, the ability of the Scoring Matrix to identify crimes that should be

which there were no ‘historic’ crimes against which outcomes could be given. Second, in the later period the process was much more ‘bedded in’, therefore processes would have improved, again ensuring outcome rates were higher.

The 9 outcomes are charge / summons; caution – adult; caution - youth; Taken Into Consideration (TIC); Penalty notices for disorder (PND); the offender has died; cannabis warning (obviously not relevant to fraud); community resolution; prosecution not in the public interest (CPS).

[31] It should be noted that the outcome rates are not ‘true’ outcome rates, as they are calculated by comparing the number of outcomes in the period with the number of offences. To calculate a true rate, only those outcomes that relate to offences that took place in the same period should be included. Those that relate to offences from older periods should not. However, data are not yet available on this basis for fraud outcomes, and so all outcome rates here are calculated on the ‘old’ basis to allow fraud to be compared to other crime types in a fair way. While this is not a perfect measure of outcome rates, it does give a general picture of outcomes.

considered by Crime Reviewers is hampered by poor information at the first stage. At the third stage, the point at which disseminations are made, there are various problems with the recording of information. For example, NFIB Crime Reviewers use a Sharepoint system to record decisions made about crimes they review. However, looking at this data shows that decisions are not always recorded here. In forces, double-keying these crimes onto force systems put a considerable burden on staff in police forces, before investigations can actually begin. Finally, at the last stage when outcomes are returned to NFIB, issues were identified around forces and other agencies being able to consistently, regularly provide that data to NFIB. The accurate and timely recording of information throughout the process is critical to an accurate understanding of the scale of reported fraud and cyber-dependent crimes, and associated outcome rates.

2. *Understanding roles and responsibilities*

The second theme that presented in the project was about understanding roles and responsibilities. Again, this theme was present across the whole process, with the project demonstrating the importance of everyone involved understanding what their role is, and what they can expect from others. At the first stage, qualitative work showed that call handlers in police and Action Fraud have a limited understanding of the rest of the process, impacting on the advice they can give to victims of crime. This then impacts on the second stage: if those at the beginning do not understand their role, and what they should be doing, the number of cases with potential to pass through scoring reduces. At the third stage, it is essential that NFIB staff provide police with disseminations that meet their needs, and record what actions they have taken. Similarly, it is essential that forces understand that their role is to investigate crimes disseminated to them (subject to decisions / priorities at force level). At the last stage, it became apparent that in some forces there were delays in outcomes being returned because it was not clear who should be doing this, or how often it should be done. This has an obvious impact on attrition rates, as if outcome information is not returned to NFIB, there is no way to know the scale of 'true' attrition.

3. *Variation in approaches between forces*

The final theme reflects the differences in the approaches forces take to dealing with cases disseminated to them by NFIB, and can be seen in the third and fourth stage of the process, i.e. when crimes were disseminated to forces, and when outcomes were returned. Each force that participated in this project had a slightly different approach to dealing with fraud and cyber-dependent crimes. This was of course understandable, and reflected the particular needs / structures of those forces. However this also meant that there was limited sharing of best practice between forces. There was considerable scope for sharing 'best practice' between forces. For example, some forces have automated the process by which they identify outcomes on their own systems, and then collate this data for return to NFIB. This has reduced the time and resources required by this force to provide outcomes data to NFIB, and if there is scope for sharing expertise amongst forces, this could increase the number of crimes with outcomes that are returned to NFIB, and in turn reduce attrition.

Of course, some of the attrition is reasonable – some crimes simply will not have enough information to warrant review, while others will not have enough viable leads for investigation. However, a good deal of attrition is likely to be avoidable. For example, by making improvements to the reporting tool, better quality data will be gathered, increasing the chances of a case getting through later stages of the process. By amending the scoring system, more crimes should be reviewed, increasing their chances of being sent for enforcement. And by working with police to understand their processes, there is potential to increase the number of crimes that are investigated, and therefore the number of outcomes returned to NFIB.

To draw comparisons between the outcome rates of offences reported to Action Fraud / NFIB, and of 'traditional' crimes.

Due to the changes in the way that outcomes are recorded between the start of the project, and currently, it is more difficult than imagined to draw meaningful comparisons with comparable crime types. Nevertheless, it is possible to draw comparisons using the charge / summons rates for 'comparable' crime types, and this is useful to develop a clearer understanding of what might be a realistic, appropriate outcome rate for fraud and cyber-dependent crimes.

The most recent data (for the year to 2014/15) shows that the charge / summons rate (the proportion of recorded crimes for which there was a charge or summons) for all crime is 17%. Clearly it would be unfair to compare fraud to this overall rate, as some crimes are more likely to result in a charge / summons than others (for example, sex offences tend to have higher charge / summons rates due to the amount of investigative effort). Following advice from Crime Statistics colleagues, theft and criminal damage were selected as comparable crimes. Both are likely to leave little in the way of forensic evidence, and thus can be difficult for police to investigate. Compared to fraud's charge / summons rate of 4% [32] (2014/15), theft has a charge / summons rates of 11%, and criminal damage a rate of 9% (both 2014/15).

[32] In order to make meaningful comparisons between years, this charge/summons rate is calculated based on the number of reports recorded in this period by Action Fraud, and does not take into account the inclusion of reports from the FFA and CIFAS (which were added to the overall crime count in October 2015). If these offences are included, the charge/summons rate is 1.4%.

While the fraud rate is lower than that for theft or criminal damage, it is important to remember that fraud is considerably different from these kinds of acquisitive crime – not only because of the international nature of these kinds of offences, but also due to the level of deception that is inherent in fraud, and the absence of many of the forensic opportunities present in other crime types (e.g. fingerprints, DNA). These combine to create additional challenges for law enforcement.

To help identify possible methods to reduce attrition where necessary.

Throughout the project, areas for improvement have been identified, ranging from issues with the computer systems used by Action Fraud and NFIB, through to the processes followed by their, and policing, staff. These findings have regularly been fed back to NFIB, in order that changes could be made swiftly. A detailed list of recommendations has been provided to Action Fraud and NFIB, including recommended changes for both the current IT system, and the new system (due to be implemented December 2015), as well as suggestions for how to improve ways of working / training needs.

Recommendations have also been shared with policing, highlighting areas for improvement such as ensuring there are sufficient staff to provide outcomes returns to the NFIB, and refreshing training for public-facing staff to ensure they are giving out accurate information (e.g. call handlers in local forces).

In addition to methods to directly reduce attrition, the project identified wider issues around NFIB's data management and auditing capability. As discussed previously, there were some difficulties getting the necessary data, and understanding what had happened with reports once they were picked up by Crime Reviewers. In these areas there is therefore scope for improving NFIB's ability to understand what happens to reports, and therefore their ability to understand and assess attrition in the future. This is particularly important with the introduction of a new system, and a new approach to scoring, where it is important NFIB assess whether the new approach is identifying the 'right' crimes, and is not 'missing' any crimes that should be reviewed.

Similarly, the project highlighted some concerns around how vulnerable victims are identified, and then dealt with by NFIB and policing. Due to issues identifying vulnerability online, it is possible that such victims are not receiving the response that they should. However, work has begun to resolve this, looking at ways that vulnerability can be identified online.

Future work

There is still more work that could be done to build on these findings. Unlike much research into attrition in other crimes, it was not possible for this project to look at attrition in three other stages. The first is around the reports that are made to Action Fraud that are not recorded as crimes. These are dealt with via signposting etc, and it would be of interest to see whether there are any regularly occurring queries. This could raise the possibility of automated messages being used to re-direct people, increasing the amount of time call handlers can spend dealing with victims of crime, and minimising the amount of inappropriate or time-consuming contacts. The second stage which was not covered by this project was the investigation stage, when attrition can occur as a result of decisions made by police. The final stage was attrition post-police outcome, i.e. when offences are taken forward for prosecution by the CPS, and then what the outcomes of those prosecutions are. At each of these points attrition could also be occurring, and there may be value in exploring these stages in future work. Work could also examine the CIFAS / FFA UK cases, to understand more about those, what kinds of reports they are, how they progress through the system, and what attrition ‘looks’ like for them.

Annex A – The Action Fraud / NFIB process

Figure 1 (see Section 1. Background) gives a broad overview of the main stages of the Action Fraud / NFIB process, but more detail is given here.

All reports of fraud and cyber-dependent crime are taken by Action Fraud, via their online reporting tool, or their contact centre.[33] As in Section 1, a number of these will not meet the threshold for recording as a crime, and so the victim will be signposted to more appropriate agencies, or an information report will be taken.

All data collected at this stage is ingested into NFIB's database, called Know Fraud. This database builds networks of crimes (and information reports), based on common entities in the reports (such as suspect bank account numbers). It then automatically scores all of the networks using a Scoring Matrix, attributing scores according to presence of information such as bank account number, vehicle registration information, etc. If a crime is part of a network that meets the scoring threshold (5 for cyber-dependent crimes, or 15 for frauds), that network will be placed in a queue for a Crime Reviewer to pick up. Crimes in networks that do not meet this threshold will not be reviewed, unless they meet one of the Manual Review criteria,[34] in which case the system will also automatically identify that, and add that network to a queue for a Crime Reviewer to pick up. The Know Fraud system continually re-

[33] The only exception is crimes that meet the criteria for 'Call For Service', in which case local police will take a report if: the offender(s) are arrested by police; there is a call for service to Police and the offender "is committing" or has recently committed a crime at the time of the call for service for all fraud types; or there is a local suspect (i.e. where, through viable investigative leads, police can or could locate a suspect with the details provided, or police have sufficient details to apprehend an offender).

[34] There are five categories of MR criteria: 1) The category itself will almost always be viable, but the quality of report made by the victim may mean the score is not reached. Examples are corporate employee fraud, or fraud by abuse of position. With these crimes the offender is almost certainly known and traceable; 2) Horizon scanning. Following reports of suicides as a result of cyber bullying / blackmail daily searches of reported crimes were commenced to identify reports and action; 3) Loss threshold. All reports with a loss over £100,000 (fraud) or £500 (cyber-dependent crimes) are reviewed because of the potential severity of impact on the victim; 4) As a result of tasking – such as pension liberation fraud where as a result of ECC tasking all reports were reviewed to develop the intelligence picture and support collaborative activity; 5) Vulnerability of the victim when it meets the ACPO definition. When this is identified at the contact centre from speaking to the victim the report is taken and the details provided to the local force to provide a service. All of these report numbers are passed through to the NFIB and these crimes are always reviewed and disseminated to forces.

scores crimes, so crimes that do not meet the threshold initially may network to other crimes (at a later date), meet the threshold, and then be added to the queue.

Crime Reviewers work on different ‘desks’[35], focusing on different types of crime. Crime Reviewers work through the networks in ‘their’ queue, and examine the content of the network to assess whether or not it may be viable for dissemination to a local police force (or other organisation) for enforcement.[36] As part of this they may ‘build’ packages by requesting information from banks under the Data Protection Act, looking for information on suspect names / addresses on databases they have access to, etc. These packages (containing developed networks) are then sent out to local forces, for investigation, and that is recorded on the Sharepoint system.

Local forces all receive packages for investigation that contain networks NFIB have identified as viable for further investigation. The response varies according to force, but in general forces record the packages they receive on their own record management systems, and then follow in-force processes for allocating crimes for investigation.[37] When an outcome is achieved, forces are required to notify NFIB via a monthly ‘return’, so that NFIB can return that information to the Home Office for crime counting purposes. If forces do not achieve an outcome, they do not tend to report this to NFIB.

[35] Cyber Crime Desk, Mass Marketing Desk, Investment Fraud Team, Volume Crime Desk, Banking and Corporate Desk. The desks were introduced in Summer 2014, prior to that (and for the period in which this study drew data) there were no desks; Crime Reviewers worked across all crime types.

[36] As well as sending packages for enforcement, NFIB can also disseminate intelligence packages to forces, and may also disseminate crimes to local forces if there is a safeguarding issue (e.g. a previously unidentified vulnerable victim).

[37] Not all forces investigate all crimes.

Annex B – The Outcomes framework

In April 2013, significant changes in the way that outcomes achieved by the police are recorded were implemented. Prior to April 2013 police focused on detections (i.e. crimes resolved via a sanction against the offender, such as a charge, summons or caution). The new outcomes framework that replaced the old detections framework was designed to increase transparency in how crimes recorded by the police (including Action Fraud / NFIB) are dealt with.

The outcomes framework introduced in April 2013 expanded on the detections framework, giving more detail on out of court disposals. In addition, collection of data on community resolutions became mandatory for all police forces (having previously been collected on a voluntary basis). In April 2014 the outcomes framework was expanded further, to include ten additional outcomes. These cover a range of outcomes where the crime would previously have been classified as 'undetected', or 'no further action taken', and so would never receive a formal outcome in the published data. The April 2014 framework gives additional transparency to police recorded crime, with the intention that every crime recorded by police will receive an outcome.[38]

It should be noted that at any one time, there will be a proportion of offences where an investigation is still ongoing and so there will be no outcomes for those crimes. In addition, crimes which are initially given an outcome such as "Investigation complete: no suspect identified" (Outcome 18) may have that outcome revised if further information comes to light, and the force is able to identify a suspect.

For the period in which this research took place, crimes would come under the April 2013 framework, with nine potential outcomes. The 'outcome rate' that is referred to throughout is calculated by looking at the number of crimes disseminated in a particular month / year / time period, divided by the number of crimes for which an outcome is returned to NFIB in the same period. Any crime that is said to have achieved an outcome will have one of nine outcomes, while as of April 2014, the expanded framework would be used, with 18 police outcomes. These are set out in Table 3:

[38] For more information, see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/331597/hosb0114.pdf.pdf.

Table 3 – Changes to the detections / outcomes framework

Detections framework – prior to April 2013 (Outcomes 1-6)	Outcomes framework – April 2013 to March 2014 (Outcomes 1-9)	Outcomes framework – April 2014 onwards (Outcomes 1-19)
1. Charge / summons	1. Charge / summons	1. Charge / summons
2. Caution	2. Caution – youths	2. Caution – youths
	3. Caution - adults	3. Caution - adults
3. Taken into consideration (TIC) – previously recorded	4. Taken into consideration (TIC)	4. Taken into consideration (TIC)
4. Taken into consideration (TIC) – not previously recorded		
5. Penalty Notices for Disorder	5. Penalty Notices for Disorder	5. Penalty Notices for Disorder
6. Other	6. The Offender has died (indictable only / sexual offences)	6. The Offender has died (all offences)
	7. Cannabis warning	7. Cannabis / Khat warning
	8. Community Resolution	8. Community Resolution
	9. Prosecution not in the public interest (CPS) (indictable only offences)	9. Prosecution not in the public interest (CPS) (all offences)
Data not collected by the Home Office	*Data not collected by the Home Office*	10. Formal action against the offender is not in the public interest (Police decision)
Data not collected by the Home Office	*Data not collected by the Home Office*	11. Prosecution prevented – Named suspect identified but is too ill (physical or mental health) to prosecute.
Data not collected by the Home Office	*Data not collected by the Home Office*	12. Prosecution prevented – Named suspect identified but is too ill (physical or mental health) to prosecute
Data not collected by the Home Office	*Data not collected by the Home Office*	13. Prosecution prevented – Named suspect identified but victim or key witness is dead or too ill to give evidence.
Data not collected by	*Data not collected by the Home Office*	14. Evidence Difficulties Victim Based – Named suspect not

the Home Office		identified: The crime is confirmed but the victim either declines / or is unable to support further police investigation to identify the offender
Data not collected by the Home Office	*Data not collected by the Home Office*	15. Named Suspect identified: the crime is confirmed and the victim supports police action but evidential difficulties prevent further action
Data not collected by the Home Office	*Data not collected by the Home Office*	16. Named Suspect identified: evidential difficulties prevent further action; victim does not support (or has withdrawn support from) police action
Data not collected by the Home Office	*Data not collected by the Home Office*	17. Prosecution time limit expired: Suspect identified but prosecution time limit has expired
Data not collected by the Home Office	*Data not collected by the Home Office*	18. Investigation Complete: No suspect identified. Crime investigated as far as reasonably possible – case closed pending further investigative opportunities becoming available
Data not collected by the Home Office	*Data not collected by the Home Office*	19. National Fraud Intelligence Bureau – filed (NFIB only) – A crime of fraud has been recorded but has not been allocated for investigation, because the assessment process at the NFIB has determined there are insufficient lines of enquiry to warrant such dissemination.

For the period April – September 2013, the overall outcome rate for all crimes reported to Action Fraud was 2%.[39]

However, as well as the overall outcome rate, it is informative to look at the charge / summons rate (the proportion of recorded frauds that result in a charge or summons). To do this, it is important to look back to the years before the Action Fraud roll out began. As Table 4 shows, there were two

[39] It should be noted that for the full year (2013/14) the outcome rate was around 6%. The outcome rate for this period should be seen in the context of two things: first, that at this time forces were using the 'old' outcomes framework (with only nine outcomes), and second, that forces had only just switched to sending outcomes data via NFIB, with the process far from established at this point. Thus a number of data quality issues affect the outcome data, and this should be taken into consideration in discussion of outcome rates.

years (2011/12 and 2012/13) of ‘transition’, in which some forces had switched to the Action Fraud process, and others had not. In this period, no outcomes data were provided for those crimes recorded by Action Fraud, and so it is necessary to look further back for comparable charge rates. The nearest year is 2010/11, when the charge / summons rate for fraud was 23%. After the roll out of Action Fraud, the charge / summons rate fell to approximately 4%. Much of this was likely because of the changes in the way outcomes data is collated and recorded (see page 7), and the delays many forces had in returning outcomes (see page 37). The most recent data available, for 2014/15 shows that the charge / summons rate is still around 4%. [40]

Table 4 – Recorded crime, dissemination rates, and charge rates, 2009/10-2014/15

	Forces only		Transition period		Action Fraud only	
	2009/10	**2010/11**	**2011/12**	**2012/13**	**2013/14**	**2014/15**
Fraud offences	73,259	72,441	119,426	179,891	211,229	230,630
Fraud disseminations	-	-	-	-	39,138	61,682
Dissemination rate	-	-	-	-	19%	27%
Fraud charges	15,191	16,350	14,488	13,324	7,956	9,054
Charge rate	21%	23%	12%	7%	4%	4%

The charge / summons rate is also a more appropriate comparator when looking at fraud against other types of crime. Although there are considerable differences between fraud and other crime types, it is nevertheless important to consider what outcomes are achieved for other crimes, to give context to the fraud data. The most recent data (2014/15) shows that the charge / summons rate for all crime is 17%. Clearly this is not an appropriate comparison, as some crimes are more likely to result in a charge / summons than others. Based on advice from the Home Office Crime Statistics team, theft and criminal damage were selected as suitable comparable crimes –

[40] In order to make meaningful comparisons between years, this outcome rate is calculated based on the number of reports recorded in this period by Action Fraud, and does not take into account the inclusion of reports from the FFA and CIFAS (which were added to the overall crime count in October 2015). If these offences are included, the outcome rate is nearly 2%.

both are likely to leave little in the way of forensic evidence, and are high volume offences. They therefore present challenges for police investigations. Compared to fraud's charge / summons rate of 4% in 2014/15, in 2014/15 theft had a charge / summons rate of 11%, and criminal damage a rate of 9%.[41]

However, it is important to remember that there are a number of caveats around these figures, and any comparison between crime types. In 2013/14, forces and NFIB were working with a new process following the transition to Action Fraud, and so the outcome and charge / summons rates were likely affected by that – as discussed in this paper, there were delays in returns of outcomes data from a number of forces (see Section 8: Key Findings: Attrition Stage 4). In addition, with the new outcomes framework introduced in 2014/15, some forces needed to make considerable changes to the administrative systems they use to provide outcomes data, impacting on recording processes. Both these changes meant that some forces sent little or no outcomes data for a short period of time, while they were making the transition. Looking at outcomes data for fraud more specifically, these offences do pose some unique challenges. For example, there tends to be a lack of forensic opportunities, for example fingerprints, and the strong international element to fraud, with many offenders based overseas. Fraud is also inherently deceptive. Thus there is likely to be a 'ceiling' to outcome rates, and the more specific charge / summons rate.

[41] As above, in order to make meaningful comparisons this charge/summons rate is calculated based on the number of reports recorded in this period by Action Fraud, and does not take into account the inclusion of reports from the FFA and CIFAS (which were added to the overall crime count in October 2015). If these offences are included, the charge/summons rate is 1.4%.

Annex C – Focus group and interview schedules

A selection of the focus group and interview schedules are included here:

- Action Fraud call handler focus groups
- NFIB Crime Reviewer focus groups
- Interviews with call handlers in local forces
- Questions for SPOCs / those who deal with dissemination / enforcement packages
- Questions for National Trading Standards Board
- Questions for Crime Registrars / those responsible for sending outcomes to NFIB

Not all were included due to space constraints, but all included very similar topics.

Questions for Action Fraud call handlers

1. Can we start by going around the room, and doing some introductions. Tell us your name, what your job is, and what your typical day entails.
    a. What's your background? Have you worked as a call handler/for the police before?
    b. What are the main challenges faced, on a day-to-day basis?
    c. What do you know about the whole process, from Action Fraud, through the National Fraud Intelligence Bureau, to local police forces?
    d. We understand that you are employed by BSS – do you see yourself as part of the 'Action Fraud team', or more as part of BSS?
2. Can you describe the 'process' of your job – when you get a call, talk us through what you do...
    a. Do you have a script to follow, or is the only guidance the tool?
    b. How easy is it to complete the form?
    c. How much do you feel that you rely on the free text box? What kind of information do you tend to put in there?
    d. Do you have targets to meet each day about the number of calls answered, or similar?
    e. And any targets to do with completing X% of the form?
    f. How busy are you, day-to-day?
    g. What type are the majority of calls you take – incidents, crimes, people just asking for advice/calling AF when they should call the police?
    h. Have you had many reports of cyber crime/computer misuse crime, such as hacking, ransomware, etc.
    i. How comfortable are you with these kinds of crimes – do you understand enough about them to do your job?
    j. How much knowledge do you have about different crime types, i.e. fraud & cyber?
    k. When you get a call, how do you decide if it is a crime, or an incident?
3. What kind of training have you had, about fraud and cyber crime in general, and how to deal with callers/informants/victims?
    a. What kind of training have you received?
    b. Do you know much about the Home Office Counting Rules?
    c. Is there ongoing training/refresher training?
    d. Are you happy with the training? Do you feel there are any 'gaps' or any training that you could use to help you in your job?
    e. Do you have all the information that you need to do your job? If not, what further information would help you?
    f. Do you know about the scoring matrix and/or manual review criteria?
    g. Do you know what fields are most important in terms of the scoring matrix or manual review?
    h. If you get a call that is upsetting, say from a particularly distressed person, what support do you have? Is there someone available for you to talk to?

4. When the caller is vulnerable, or the caller is calling on behalf of someone vulnerable, how do you deal with that?
    a. What guidance have you received about vulnerable victims?
    b. How do you identify vulnerable victims – do you ask specific questions?
    c. If someone calls on behalf of a vulnerable victim, e.g. a parent, carer, relative, what do you do?
    d. How do you find using the ‘vulnerable victim list’? How well does it work?
    e. What’s your experience of police forces, when you contact them to tell them about a vulnerable victim in their area?
    f. There are three questions on the tool about whether a victim is vulnerable – how useful are these? Do victims tend to give positive responses to these?
5. If you receive a call about a crime that you think falls under ‘call for service’ criteria, what do you say to the caller?
    a. What’s your understanding of the criteria under which a crime counts as a call for service?
    b. [What if the victim refuses to contact the police, or has already contacted the police and been refused service?]
    c. How often do you get cases that fall under the call for service criteria?
    d. Would you ever contact the police yourself about a call for service case? If so, what kind of response do you get from them?
6. How do you manage calls when victims (or informants) call wanting to know more about their crime report and what’s happened with it?
    a. Do you often get victims calling to ask for an update on their crime?
    b. What response do you give to these victims?
    c. Do you know that (in some cases) nothing will happen to a crime?
    d. What do you do if they want to know what’s happened – would you ever contact NFIB to find out?
    e. What are the challenges around this?
    f. Do you have many calls from people who have had a letter from NFIB, who have been told that their report has been no-crimed? What do you say in these circumstances?
7. Aside from everything else we’ve discussed today, are there any other comments you’d like to make, about the challenges you face or improvements that you think are necessary?

Questions for NFIB Crime Reviewers

1. To start with, could we go around the room, and have everyone introduce yourselves – what's your name, your role here, and a brief bit about your background – are you an ex-officer, previous police staff?
    a. What experience do you have of fraud or cyber crime?
    b. What training have you had, how do you know what police can/cannot investigate? How do you know what counts as 'viable'?
    c. What do you know about the whole process, from Action Fraud, through the National Fraud Intelligence Bureau, to local police forces?
    d. How well do you feel you understand the scoring matrix and/or manual review criteria?
    e. Do you know what fields are most important in terms of the scoring matrix or manual review?
2. And how does a typical day go – can you talk us through what you would usually do in a day?
    a. Do you have targets? What are they, and how do you feel about those?
    b. Are you busy, or just right? Too quiet?
    c. How much contact do you have with local police forces, either before or after you disseminate a crime to them, or just in general?
3. And how you deal with the tasks that you pick up – could you talk us through that, step-by-step?
    a. What do you understand about the overriding principles underlying dissemination [i.e. do they disseminate based on value, perceived likely response, viability, or some combination?]

       FACTORS IN DECIDING WHAT TO DO WITH A CRIME:
    b. What do you first look at when you open a task?
    c. How do you know if it's viable for enforcement? For intelligence?
    d. What do you look for when deciding what to do with it? Does this vary depending on the crime type?
    e. Do you ever disseminate packages to police forces for further intelligence gathering? (e.g. a forensic examination in the case of network intrusion may expose methods and techniques that may be valuable intelligence beyond the victims report)
    f. Do different crime types take different lengths of time to deal with? For example, are (some) computer misuse offences quicker to deal with than other crime types?
    g. What proportion of your disseminations are fraud based compared to computer misuse offences? Why do you think that is? [Subject to answer: What is it about the computer misuse reports that means that a lower proportion of them are progressed]

       FACTORS IN DECIDING WHETHER TO GET EXTRA INFORMATION:
    h. What kind of organisations can you request extra information from? Who do you typically make requests to?
    i. Do you ever re-contact victims for further information? If so, do you commonly ask for the same things (in which case should that be added to the initial report)?

j. How do you decide that it’s worthwhile asking for that information?
k. What’s the system for contacting other organisations? How do you know who to contact? Does this work well? What are the challenges?
l. What proportion of your disseminations are analysed packages which you feel you have added value to, as opposed to pushing reports straight out of the door?
VULNERABLE VICTIMS/LARGE LOSSES
m. How does this process change when you come across a crime targeted at, for instance, a vulnerable victim? Do you see many of these/are you aware of these?
n. Do you ever have to contact local police about these kind of cases?
o. And does it change when you come across people who have had large losses?
p. Do you look at what people answer for how the crime has impacted on them? Does this affect your decision making at all?

4. Thinking more generally about the types of crime that you review, what are your thoughts on them in terms of the quality of the report, and the types of report you see?
    a. What proportion of crimes that you pick up are good quality? In terms of the quality of the crime itself, and in terms of the quality of the report?
    b. Would you ever contact the call handler to query something?
    c. Do you feel you’re getting the ‘right’ types of crimes?
    d. What difference does the presence of ‘evidence’ (e.g. CCTV, documentation) make to your decision making?
    e. What information do you like to see in the free text? Is there any structure that’s particularly helpful, or particular pieces of information that are useful/not useful?
    f. How often do you get reports where there is ‘additional information’, i.e. the victim has called a second time to add more details, and the details are in a second text box?
    g. What would you put in the scoring matrix, or add as a manual review criteria?
    h. What provides a viable line of enquiry, that isn’t built into the system, that you would like to see? What information would you like to see added to the reporting tool, as well as anything you feel should be built into the scoring matrix or manual review processes?
5. Are there any challenges or difficulties with the IT systems you use, i.e. KnowFraud and Sharepoint?
    a. What information do you record on Sharepoint? Is this a simple process?
    b. Does this take up time that you’d rather spend doing other things?
    c. Do you feel like it’s important to leave an audit trail? Is that kind of thing part of your job?
    d. Do you ever get feedback from forces about the packages you send out for investigation? In terms of the usefulness or quality of them?
    e. Do you think that the email approach to sending out packages is a good one?
6. Having thought about everything we’ve talked about today, what would you say are the best bits about the process/system, and what still needs improving?

Questions for call handlers in local police forces

1. Could you explain to me what your role is, and what your job entails?
    a. Specifically in relation to NFIB and Action Fraud.
    b. Do you work as part of a team? If so, who else is in the team?
2. Were you in your current job when Action Fraud was rolled out, and responsibility passed to them for recording fraud and cyber?
    a. What's your understanding of the Action Fraud/NFIB process?
    b. What's your understanding of who is responsible for taking reports of fraud and computer misuse crime?
    c. Do you have any contact with Action Fraud or the NFIB? Do you have any SPOCs?
3. What kind of training do you receive
    a. Call handler specific?
    b. In relation to specific crime types?
    c. How happy are you with the level of knowledge you have about fraud, and cyber crime/computer misuse crime? And compared to other types of crime, such as burglary, assault, etc?
    d. What kind of training did you get about Action Fraud and the National Fraud Intelligence Bureau, when centralised reporting was introduced/when you started your job?
    e. Would you like any other training? What else might be useful?
4. What's your understanding of how fraud and computer misuse crime is dealt with in your force?
5. Do you often get victims of fraud or computer misuse crime (e.g. hacking) calling you to report a crime?
    a. Under what circumstances would you take a report from that victim?
    b. What do you know about call for service criteria?
    c. Are there any other instances in which you'd take a report of fraud, from an officer calling one in, or someone else?
    d. When you've taken the report, what do you do with it? Do you double-key it onto the Action Fraud system yourself or is that up to someone else? Is there any way to record whether it's been double keyed or not?
6. Do you often get victims of fraud or computer misuse crime calling to find out what progress has been made with their crime?
    a. What do you do under those circumstances? Can you look it up yourself (on your system) or do you pass it on to another team?
    b. Do you find that victims contact you, having received a letter from the NFIB, before the crime is on your system?
    c. Would you ever refer these victims back to Action Fraud?
7. Do you get police officers asking you about Action Fraud/NFIB? Or asking you for help with fraud/computer misuse crime, maybe how to make a report to AF?
    a. What kind of questions?

    b. What do you tell them/how do you help them?

8. Do you receive vulnerable victim referrals from Action Fraud? What happens in these circumstances?
    a. How do you record them on your system? Are they crimes or incidents?
    b. What is the force’s response to those victims – visit or phone call or other?
    c. How do you feel about this process – does it work well, or are there changes that need to be made?
9. Is there anything else you’d like to add, that we’ve not covered already? Any other challenges you face, improvements you’d like to see, or comments?

Questions for SPOCS/those who deal with dissemination/enforcement packages

1. Could you explain to me what your role is, and what your job entails? What does your day 'look like'?
    a. Specifically in relation to NFIB and Action Fraud
    b. Do you work as part of a team?
    c. If so, who else is in the team?
2. And what's your background? Do you have a fraud or cyber background?
    a. Have you had any fraud/financial investigation/cyber training?
    b. Was that useful/do you think that kind of training would be useful?
3. What do you know about the whole process, from Action Fraud, through the National Fraud Intelligence Bureau, to local police forces?
    a. Would you like to know more about this process?
    b. Would more knowledge help you understand your 'part' better?
4. Moving on to talk specifically about the packages you receive from NFIB, what are your thoughts on these?
    a. Are they good quality?
    b. Do they contain the information that you need?
    c. Are they timely? Do they get to you quickly enough, from the point that the victim makes the report, or are there delays that impact on what you (can) do with them?
    d. Is there anything else you would like to see in the packages?
    e. What do you do with the packages once you receive them – do you screen them? How do you decide who to allocate them to?
    f. Are there any force policies around what's investigated?
    g. Do you pass the whole package on to that person? Or just what you think is important?
    h. Are there any particular factors, such as financial loss, victim type, that would affect a decision to investigate a case?
    i. How often do you get cyber cases, such as hacking, PBX, DDoS? How well equipped are you to deal with these?
    j. Do you ever request assistance from, for example, regional teams, or digital investigations/forensics teams within your own force?

5. If you need more information or assistance with the investigation, would you or your team/officers contact the NFIB or Action Fraud?
    a. How do you know who to contact?
    b. What kind of information do you contact them for?
    c. Is there a better way to get this information, or are you happy with how it's working?

    d. Would you like direct access to the NFIB system so that you can see what's been done at that stage?

6. How do you record progress on a crime, both on your own systems and on NFIB systems?
    a. Does this work well? Is it time consuming?
    b. When you resolve a case, and get an outcome (e.g. arrest, charge), what are your next steps?
    c. How would you feel about having direct access to the NFIB system, and being able to update your progress and outcomes on there?
7. Will the new outcomes framework, that was introduced this year, have any impact on your work with NFIB crimes?
8. Are you also responsible for taking referrals from Action Fraud, when they identify vulnerable victims who need a 'welfare' check?
    a. What do you do in those situations?
    b. Do you have to investigate those cases, or just 'give them a hug'?
    c. Any thoughts on how well that process works?
9. Is there anything else, which we haven't covered, that you'd like to add, about how the system works, challenges you face, or improvements that could be made?

Questions for National Trading Standards Board

1. Could you explain to me what your role is, and what your job entails?
    a. Specifically in relation to NFIB and Action Fraud.
    b. Do you work as part of a team? If so, who else is in the team?
2. And what's your background? Do you have a fraud background?
    a. Have you had any fraud training?
    b. Was that useful/do you think that kind of training would be useful?
3. What do you know about the whole process, from Action Fraud, through the National Fraud Intelligence Bureau, to local police forces?
    a. Would you like to know more about this process?
    b. Would more knowledge help you understand your 'part' better?
4. I understand that Trading Standards receive reports via the Citizens Advice Consumer Service. How does that service work? Is it a national reporting centre, or is it localised?
    a. Any idea on the numbers of reports that they receive?
    b. Has this changed at all since the introduction of Action Fraud?
    c. What kind of overlaps are there, between reports taken by Action Fraud, and those taken by the Citizens Advice Consumer Service?
5. Moving on to talk specifically about referrals that Trading Standards receive from the NFIB, I understand that these go direct to local authorities?
    a. Do you feel that they are going to the appropriate place?
    b. Have you had any feedback from local authorities/local Trading Standards about the quality of packages, or the type of packages that they are getting?
    c. Do you feel that AF/the NFIB understand Trading Standards' remit?
    d. Are they good quality? Do they contain the information needed? Is there anything else you would like to see in the packages?
    e. Are they timely? Do they get to you quickly enough, from the point that the victim makes the report, or are there delays that impact on what you (can) do with them?
    f. Are there any particular factors, such as financial loss, victim type, that would affect a decision to investigate a case?
6. Is there anything else, which we haven't covered, that you'd like to add, about how the system works, challenges you face, or improvements that could be made?

Questions for Crime Registrars/those responsible for sending outcomes to NFIB

1. Could you explain to me what your role is, and what your job entails? What does your day 'look like'?
    a. Specifically in relation to NFIB and Action Fraud
2. And what's the process by which you provide outcomes (or other data) to NFIB?
    a. Would you ever do any kind of audit of the data you get from NFIB?
    b. For example, looking at how things are classified under Home Office Counting Rules, and whether it's been done correctly?
3. How much time would you say you spend on NFIB business, per week or per month?
    a. Is this more or less than you used to spend on fraud and computer misuse crime, before the introduction of Action Fraud/the NFIB?
    b. How does this compare to other work that you have to do?
    c. Given the level of work that's required for all this/the difficulties there are in getting al this done/finding it all on the system, how sure are you that you're sending everything back?
4. Do you feel the system works well?
5. What could work better?
6. Ideally, how would the system work?
7. Can I ask you a bit about 'double-keying' [where people have to enter crimes/information on the forces system, and then enter it all again on the Action Fraud system] – do you have to do any of this?
    a. Who would be responsible for it in your force?
    b. What do you do if you find an crime on your system, and you suspect that it's not been double keyed, whether that's in terms of reporting it, or an outcome has been added, or anything like that?
8. Will the new outcomes framework, that was introduced this year, have any impact on your work with NFIB crimes?
9. Do you have any experience of how police/other staff find the AF/NFIB system, in your force?
    a. Are there any particular challenges faced?
10. Is there anything else, which we haven't covered, that you'd like to add, about how the system works, challenges you face, or improvements that could be made?

Annex D – Logistic Regression output: dissemination of crimes to local police forces (and others) for enforcement

Table 5: Logistic Regression to see what aspects of the scoring process affect the odds of a crime being disseminated.[42]

	B	Exp(B)
Independent Variables		
Constant	-.95	.39
Suspect phone number	.49	1.64
Vehicle registration	1.48	4.4
Suspect sort code	1.09	2.97
Cyber-dependent crime	-2.68	.07

Table 6: Logistic Regression to see what aspects of the crime and / or victim affect the odds of a crime being disseminated.[43]

	B	Exp(B)
Independent Variables		
Constant	**-3.08**	**.05**
Business victim	**.99**	**2.70**
Payment made	**2.50**	**12.17**
Evidence - Call recordings / texts	**.68**	**1.98**
Evidence – Emails / other online transcripts	**.60**	**1.82**
‘Other’ victim	**-.94**	**.39**
Report via Contact Centre	**-.49**	**.62**

[42] Variables not included in the model: Suspect payee name; Suspect’s bank name; Organisation’s website; Account number; Information about transfer method used; Payment reference for any transfers; Suspect email address.

[43] Variables not included in the model: Victim said that the crime had a severe or significant impact on them; Victim sex; Evidence – Photos, recordings or minutes; Evidence – Letters or faxes; Evidence – contracts or other legal documents; Victim age – Over 65.

Annex E – Logistic Regression output: crimes being investigated by, and receiving an outcome from, local police forces

Table 7: Logistic Regression to see what aspects of the scoring process affect the odds of a crime achieving an outcome.

	B	Exp(B)
Independent Variables		
Constant	-2.49	.08
Suspect mobile phone number	1.10	3.00
Suspect sort code	.98	2.68
Suspect organisation phone number	-2.10	.12
Payee name	-.55	.58
Suspect email address	-1.51	.22

Table 8: Logistic Regression to see what aspects of the crime and / or victim affect the odds of a crime achieving an outcome.

	B	Exp(B)
Independent Variables		
Constant	-3.61	.03
Dissemination within 14 days	.44	1.56
Evidence – Call recordings / texts	1.45	4.26
Payment made	1.41	4.10
Online fraud	.69	1.99
Evidence – Contracts / legal docs	-1.13	.32
Evidence – Emails / other online transcripts	-.75	.47
Female victim	-.81	.45

ISBN: 978-1-78655-681-3

ISSN: 1756-3666