Developing questions on fraud and cybercrime for the CSEW

Final report

Authors: Debbie Collins, Jane Kerr, Shannon Harvey, Sophie Green, Carol McNaughton Nicholls
Date: 18/12/14
At NatCen Social Research we believe that social research has the power to make life better. By really understanding the complexity of people’s lives and what they think about the issues that affect them, we give the public a powerful and influential role in shaping decisions and services that can make a difference to everyone. And as an independent, not for profit organisation we’re able to put all our time and energy into delivering social research that works for society.
Contents

Acknowledgements ..................................................................................... 1
Executive summary ..................................................................................... 2
1 Background .............................................................................................. 5
  1.1 The Crime Survey for England and Wales .............................................. 6
  1.2 Aims of this research ........................................................................... 7
2 Measuring fraud and cybercrime ............................................................. 9
  2.1 Question development ......................................................................... 9
    2.1.1 Development of new screener questions ....................................... 9
    2.1.2 Defining incidents ......................................................................... 12
    2.1.3 Victimisation module ..................................................................... 12
    2.1.4 Other online and cybercrimes considered as part of the desk review ........................................................................ 12
  2.2 Challenges in measuring fraud and cybercrime ..................................... 13
3 Success in meeting the challenges .......................................................... 19
4 Recommendations for question wording .............................................. 28
  4.1 Recommendations for screener questions .......................................... 28
  4.2 Including a screener question to identify online harassment ................. 33
  4.3 On-line threats of violence and sexual offences ................................. 33
  4.4 Recommendations for victimisation questions .................................... 33
  4.5 Content of the victimisation module for the new screener questions ... 38
    4.5.1 Confidence fraud vs consumer detriment ..................................... 39
5 Recommendations for further testing ................................................... 41
  5.1 Further cognitive testing ...................................................................... 41
  5.2 Large scale field testing ..................................................................... 41
    5.2.1 Assessing the impact of change on the time series ....................... 43
    5.2.2 Assessing data quality ................................................................... 43
    5.2.3 Respondent debriefing questions ................................................ 46
  5.3 Developing rules .................................................................................. 46
  5.4 Offence coding .................................................................................... 47
  5.5 Development time .............................................................................. 47
Appendix A. Findings from the desk review ........................................... 51
  A1 Scope of crimes considered by the review ........................................ 51
    A1.1 Methods ......................................................................................... 52
A2 Considerations for the screener questions .............................................. 53
  A2.1 Categorising frauds, cyber and other online crimes .......................... 54
  A2.1.2 Other forms of cyber and online crime with individual victims .......... 59
  A2.2 Reference group discussion points for the screener questions .......... 60
A3 Measuring volume for fraud, cyber and online crime ............................ 61
  A3.1 Definitions – incidents, series and victimisation .............................. 61
  A3.2 Application of the current series questions .................................. 63
  A3.3 Implications of victimisation in the past-12 months ......................... 64
  A3.4 Reference group discussion points for the screener and series questions 65
A4 Including fraud, cyber and other online crime in the Victimisation Module 65
  A4.1 Considerations for the Victimisation Module .................................. 66
  A4.2 Reference group discussion points for the Victimisation Module ........ 66
A5 Online crime in the Self-Completion and Domestic Violence and Assault module .................................................. 73
Appendix B. Cognitive interview findings ............................................. 76
  B.1 Aims of stage 2 and study design ................................................ 76
B2 Screening questions findings ............................................................. 77
  B2.1 Confidence fraud ........................................................................ 78
  B2.1.1 Types of crime considered .......................................................... 78
  B2.1.2 Understanding of the different versions of the question .................. 79
  B2.1.3 Understanding of ‘goods’ ............................................................. 80
  B2.2 Non confidence fraud .................................................................. 81
  B2.2.1 Types of crime considered .......................................................... 81
  B2.2.2 Understanding of key terms ......................................................... 82
  B2.3 Interference with internet and computer access, and theft of personal data .......................................................... 82
  B2.3.1 Types of information considered ............................................... 84
  B2.3.2 Understanding of the different versions of the question ................ 85
  B2.3.3 Understanding of key terms ......................................................... 86
  B2.4 Interference with internet and computer access ................................ 86
  B2.4.1 Types of crime considered .......................................................... 87
  B2.4.2 Understanding of key terms ......................................................... 87
  B2.5 Number of incidents .................................................................... 87
  B2.6 Sorting out the series ...................................................................... 96
  B2.7 Crimes missed by the screening questions ...................................... 97
  B2.8 Willingness to answer .................................................................... 98
  B2.9 Potential double counting ............................................................. 99
B3 Victim form findings ............................................................................. 104
  B3.1 Date of incident ........................................................................... 104
  B3.2 Description of incident ................................................................. 107
  B3.3 Why the incident happened ............................................................ 110
  B3.4 Whether the devices involved were solely for personal use .......... 111
  B3.5 Location of incident ................................................................. 111
  B3.6 Method of entry ........................................................................... 112
  B3.7 Cost of incident (money and time) ............................................... 112
B3.8 Impact of incident ........................................................................................................115
B3.9 Other issues ..................................................................................................................117

Appendix C. Test materials ................................................................. 118
Appendix D. Cognitive testing methodology .............. 181

Figures and tables

Figure 2:1 Mapping of fraud methods................................................................. 10
Figure 2:2 Illustration of sample sizes needed to detect differences in survey
estimates.............................................................................................................. 11
Figure 2:3 Measurement challenges and strategies to tackle them.............. 13
Figure 3:1 Evidence of success of approaches to overcome problems........ 20
Figure 4:1 Content of the current victimisation module.......................................38
Figure 4:2 Current incident checklist questions.....................................................38
Figure 5:1 Summary of questions requiring further cognitive testing .............. 41
Figure 5:2 Illustration of effective sample sizes needed to detect differences in
survey estimates .................................................................................................. 43
Figure 5:3 Proposed data quality measures............................................................44
Figure 5:4 List of possible respondent debriefing questions .............................46
Figure B2.1 Number of incidents recorded ..........................................................91
Figure B2.2 Circumstances in which ‘double counting arose’............................102
Figure B3.1 Summary of rationale for answers to VICTAREA & WHEREHAP..111
Table A.1 Survey Questions by fraud type............................................................57
Table D.1 Participants characteristics...............................................................186
Acknowledgements

The authors are grateful to the following people, who contributed to this research:

- Sue Archer, Danai Chambati-Wood, Karen Joyce and Ann Roberts, who along with Sophie Green carried out the cognitive interviews;

- Meghan Elkin, John Flatley and Joe Traynor at the Office for National Statistics for their advice and help during the course of this project; and

- members of the expert advisory group:
  - Samantha Dowling and Angela Scholes, Cyber Crime Research, Home Office
  - DI Chris Felton, National Fraud Intelligence Bureau
  - DS Terry Wilson, ACPO lead for cyber crime
  - Professor Michael Levi, Cardiff University
  - Gareth Rees and Hilary Clarkson, National Crime Agency
  - Stephanie Gledhill and Catherine Crowe, Serious and Organised Crime, Home Office
  - Professor David Wall, Durham University
  - Irina Mineva, Crime and policing knowledge hub, Home Office; and
  - Laura Williams and Chris McKee, Crime Statistics, Home Office

- the members of the public who participated in the cognitive interviews.
Executive summary

The Crime Survey for England and Wales (CSEW) was designed back in the early 1980s to provide estimates of victimisation among adults aged 16 and over living in households in England and Wales that would be broadly comparable to police recorded crime figures. More recently the survey has also captured information on victimisation among children and young people aged 10-15 years. The way in which crimes are identified has remained largely the same since the survey started and involves participants being asked a series of screener questions that identify whether or not they or members of their household have experienced incidents of particular types that appear to amount to criminal incidents in the past 12 months. All those identified through the screener questions as possible victims of crime are asked more detailed questions about the incident in the Victimisation Module. The information collected in this module is then used to code the incident using a set of rules that approximate the way in which the police should record the same incident. These rules follow, as far as possible, the Home Office Counting Rules for recorded crime.

However, the ways in which crimes are committed have changed since the survey started, in particular in recent years with the rise in the use of the internet. The internet provides not only new means of committing established crimes (known as cyber-enabled), it also provides opportunities to undertake new types of crime (known as cyber-dependent). Fraud is a long-established crime but the internet has provided a new modus operandi for fraudsters and has spawned new (cyber) crimes such as theft of personal data and interference with internet and computer access. When the survey began, high volume crimes such as burglary and car crime were the main focus and fraud and cybercrimes were not a major concern but this has changed in recent years. While fraud and cybercrime offences are asked about in existing modules of the CSEW, they are not currently identified in the screener and victimisation modules of the questionnaire. This means that these offences are not currently included in the estimates of the volume of offences that occur in England and Wales, which are derived from data collected in the victimisation module. This gap in crime statistics was recognised by the National Statistician’s independent review of crime statistics in 2011.

This project, undertaken by NatCen Social Research on behalf of the Office for National Statistics, was concerned with improving the measurement of fraud and cybercrime on the CSEW through the development of new screening and victimisation module questions for these crimes. The research involved three stages: a desk review; development and testing of new questions; and final recommendations. The desk review identified and reviewed existing survey questions across a range of surveys of the general population carried out in Europe, North America and Australia. The research team also drew on the expertise of a specially convened ‘expert reference group’. Drawing on evidence from stage 1, stage 2 involved the development and testing of proposed new screening questions and a subset of questions from the victimisation module. Testing involved 37 members of the public, who took part in face-to-face cognitive interviews. Cognitive interviewing is a qualitative method that is used to assess the validity of answers to survey questions. The aims of this testing were to assess participants’

- initial reaction to the new screening questions; and
- understanding of the test questions.

In addition, the testing explored any difficulties participants had in being able to answer the questions, such as recall of the event, and whether the new screener questions were picking up the types of crimes they are designed to identify.
As part of the testing, different forms of the new screener question wording were compared using a split ballot design, whereby participants were asked one or other version of the question and responses compared.

At Stage 3 recommendations were made on both the wording of questions and on the further testing required to assess the robustness of the data from these new questions and the impact of their inclusion on the time series data. This report discusses the challenges involved in development of new CSEW questions concerned with fraud and cybercrime, the strategies taken to tackle these, and their success. Evidence from the cognitive testing is used to judge success. The report makes recommendations on the wording of questions that should be taken forward and proposes further testing to assess data quality and the impact of questionnaire changes on the time series.

New questions (chapter 2)

A number of new screener questions were developed to capture incidents of victimisation of fraud and cybercrime. The types of incidents captured reflected those defined in the Government’s Serious and Organised Crime Strategy (Home Office, 2013) and covered fraud, theft of personal information, and interference with internet and computer access. The desk review identified the intrinsic characteristics of the different ways in which fraud is committed. Two main types of fraud were identified – confidence and non-confidence fraud and a screener question was developed about each type. A screener question about theft of personal data was included to capture this type of incident where no fraud had (yet) taken place. A screener question on interference with internet and computer access was designed to pick up incidents such as the spreading of viruses or malicious software and botnets, hacking and distributed denial of service (DDoS) attacks. Viruses and other interference captured by anti-virus software, before any harm was caused to the intended victim, were out of scope.

In addition, information collected in the current victimisation module was considered. Specifically, the current questions on when and where the incident occurred, and the impact of the incident on the victim were reviewed and tested so as to ensure their appropriateness for fraud and cybercrime.

In developing the new screener and victimisation module questions a number of issues were considered, including the following.

- Definitions of the new incidents being covered, the inclusion of attempts as well as actual incidents, and what should be in and out of scope, for example crimes against businesses and consumer detriment.
- What information victims will be able and willing to provide about these crimes, for example the number of incidents and where they took place?
- Ways to minimise the impact of including new questions on interview length, response rates and data quality.
- How to ‘future proof’ questions so as to avoid the need for regular updates which may interfere with the time-series data.
Success of the approach (chapters 3 and 4)

Results from the cognitive testing indicated that it is possible to capture incidents of fraud and cybercrime through the inclusion of a few additional questions. Victims are able to report information about these incidents once they become aware of them. Some double-counting of incidents was observed, particularly where theft of personal data was reported as well as the non-confidence fraud that took place as a result. For example, credit card details being stolen (reported at the theft of personal data question) and then used to purchase goods online (reported at the non-confidence fraud question). A number of check questions are proposed that would identify and address this problem. The wording of the screener question on interference with internet and computer access was problematic and required refinement.

Recommendations and next steps (chapter 5)

Further cognitive testing is recommended to test suggested refinements to some of the new questions, such as the screener question on interference with internet and computer access and check questions proposed. In addition, further thought should be given to the development of a screener question capturing online harassment, as this was not considered as part of this study.

It is recommended that a new victimisation module be considered for fraud and cybercrime. This would minimise the risks of accidental errors occurring as a result of modifying the current victimisation module and reduce the possible impact of changes to the existing time series.

Larger scale testing is recommended to test the new questions in the context of the CSEW survey as a whole. Ideally, this testing should be large enough to detect statistically significant differences in survey estimates, response rates and interview length between the current and new questionnaires and an indication of effective sample sizes needed are provided. The quality of data obtained from the new questions should be assessed. Recommendations are made on the kinds of metrics that could be used to assess the quality of these data.

While progress has been made in developing new questions on fraud and cybercrime that can be included in the CSEW there is still further work to do. Beyond the further testing recommended there is the development and testing of the computer-assisted questionnaire script for the new questions and of the procedures for coding these new incidents in line with the latest Home Office Counting Rules. Time will be needed to thoroughly test the software and coding procedures to ensure that the survey can collect data accurately on these incidents so that they can be reported on with confidence.
1 Background

The impetus for this research is the changing landscape in which crime is committed and the need to improve its measurement. The ways in which crimes are committed have changed during the past 25 years reflecting the rise in the use of the internet among the general public to carry out transactions and share information. For example, the offence of fraud (false representation for personal gain) is a long established crime, which in recent times has seen the incorporation of the internet into the modus operandi of the fraudster. However, the internet not only provides a new means for committing established crimes, it also provides opportunities to undertake new types of crime. “Just as the offence of phone tapping could not have existed before the creation of the telephone, computer hacking could not have taken place before the rise of the internet” (ONS, 2014a).

A useful typology has been developed that distinguishes between these two types of crime, known as ‘cyber-enabled’ and ‘cyber-dependent’ crimes (McGuire and Dowling, 2013). Cyber-enable crimes make use of the internet to facilitated new ways for existing crimes to be perpetrated. The McGuire and Dowling review included:

- fraud (including mass-marketing frauds, ‘phishing’ e-mails and other scams; online banking and e-commerce frauds);
- theft (including theft of personal information and identification-related data); and
- sexual offending against children (including grooming and the possession, creation and/or distribution of sexual imagery) in this category.

Cyber-dependent crimes are offences that can only be committed by using the internet and internet-enabled devices. These crimes include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks, i.e. the flooding of internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud (McGuire and Dowling, 2013).

These cyber-enabled and cyber-dependent crimes were included in the Government Serious and Organised Crime Strategy, which sets out a framework and direction for those working on the prevention of serious and organised crimes in England and Wales. Improving the measurement and recording of fraud and cybercrime is seen as critical to understanding how it is evolving over time, so that the right resources can be allocated to the appropriate prevention issues (McGuire and Dowling 2013).

The use of the internet to facilitate or commit crime and the extent to which criminality has been displaced from traditional crimes into these new types of criminality is an increasingly important question. However current crime statistics, while providing relatively robust measures of traditional crimes do less well in measuring new types of crime. For example, the Crime Survey for England and Wales (CSEW) provides estimates of the volume and prevalence of victimisation among adults (aged 16 years and over) and children (aged 10-15) living in households in England and Wales. Whilst the survey captures some information on these new forms of crime it does not currently provide volume estimates of these crimes. This gap in crime statistics and the need for improved measurement of these crimes was recognised by the National Statistician’s independent review of crime statistics (2011). If there has been a significant switch

---

1 The CSEW excludes businesses and people living in intuitions, such as hospitals, care homes and prisons.
from traditional to new methods of crime, then there is a risk that the statistics could be presenting a misleading picture. In the absence of reliable quantitative data it is difficult to prove or disprove the claim that crime has simply been displaced into these new forms of crime. Developing new questions that capture these new forms of crime, which could be included as part of the Crime Survey, would provide such data.

1.1 The Crime Survey for England and Wales

The CSEW is a large, random probability survey providing nationally representative data. Since 1981, the survey has run at approximately two year intervals before becoming a continuous survey in 2001. The survey provides estimates of victimisation among adults (aged 16 years and over) and children (aged 10-15) living in households in England and Wales. Survey participants are asked about their experiences of crimes against the household (for example, burglary) and personal crimes (for example, theft from a person) which they themselves have experienced in the past-12 months, irrespective of whether or not they reported these incidents to the police. This information is collected as part of a face-to-face, computer assisted personal interview (CAPI) which takes place in the participant’s home.

The questionnaire contains a set of ‘screener’ questions that determine whether the participant or other members of his or her household, have experienced particular types of crime or incidents that may amount to a crime during the past-12 months. For personal crimes (for example, assaults and personal thefts) participants are asked only about their own experience. For household crimes (for example, burglary and car crime) they are also asked about the experiences of others in their household as well as themselves. The screener questions are designed to ensure that participants do not mention the same incident more than once. At the end of the screener questions, the interviewer checks with the participant that all incidents have been recorded and nothing has been counted twice. Any amendments to the coding of the screener questions are made at this point.

All those identified through the screener questions as possible victims of crime are asked detailed questions about the incident in the Victimisation Module. The Victimisation Module questions establish when and where the incident took place as well as what happened. Answers to these questions establish whether the crime is in scope (i.e. it happened in the last 12 months; took place in England or Wales; is not a crime against a business; and is classified as ‘a crime’ according to the Home Office counting rules (Home Office, 2014)), and form the basis of the classification of offences. The Victimisation Module also provides information on the characteristics of offences – such as, extent of losses, level of injury, time, place and location.

The CAPI questionnaire program selects the incidents identified in the screener questions to be followed up in more detail in the Victimisation Module. Each incident is eligible to be followed up, but incidents defined as forming part of a ‘series’ are only covered by one Victimisation Module (with detailed questions being asked only about the most recent incident in the series). Up to six Victimisation Modules can be completed, though the last three that could potentially be completed contain fewer questions (primarily those required for offence coding using the Home Office Counting Rules). This cap on the number of victim forms that can be completed in one interview is a means of reducing respondent burden and interview length. In practice, very few participants are asked more than three victim forms. Some 96.6% of all victims were asked up to three victim forms, with almost three quarters of victims (73.8%) being asked just one (2012-13 CSEW Technical Report). The selection of incidents to follow

---

2 A series is defined as "the same thing, done under the same circumstances and probably by the same people". CSEW Technical Report 2012-13.
up and collect further information on in the Victimisation Module has been done the same way in each survey, with some types of offence taking priority over others. In practice this means that rarer incidents are asked about first to ensure good coverage of lower-volume crimes.

The use of the Home Office Counting Rules by the CSEW to classify crimes reflects an aim of the survey to benchmark trends in crime and facilitate comparison between the police figures and those from the CSEW.

1.2 Aims of this research

In January 2014, the Office for National Statistics (ONS), in consultation with the independent Crime Statistics Advisory Committee (CSAC), published a discussion paper on the coverage of crime statistics³. This paper presented an overview of the existing survey coverage, challenges in measuring cyber-crime, and outlined the steps being taken to improve measurement of cyber-crime.

This research, commissioned by the ONS is concerned with the development of new questions which would allow these estimates to be produced.

The research involved three stages: a desk review; development and testing of new questions; and final recommendations. The first stage aimed to:

- understand how members of the public, including victims, describe and understand fraud and cybercrime;
- evaluate the range of methodologies and survey questions used on other national surveys to measure the prevalence of victimisation from fraud and cybercrime; and
- inform the development of new questions and amendments to existing ones.

To meet these aims an evidence review was carried out, which identified and reviewed existing survey questions across a range of surveys of the general population carried out in Europe, North America and Australia. The research team also drew on the expertise of a specially convened ‘expert’ reference group.

The crimes covered by the stage one review include fraud and cybercrimes, as defined by the Serious and Organised Crime Strategy (Home Office, 2013). This includes cyber-enabled crimes that are traditional crimes which have increased in their reach because of the internet (for example, mass-marketing frauds), and cyber-dependent crimes which are offences that can only be committed by using a computer, computer networks, or other forms of information and communications technology (for example, the spread of viruses). In addition, other types of online crime against the person which may already be identified by the CSEW were also included, such as online abuse and harassment. The findings from this stage are summarised in Chapter 2, with Appendix A containing further details.

Stage two involved the development and testing of proposed new screening questions and of a subset of questions from the victimisation module, which included those questions used in the coding of offences. The testing involved a purposive sample of

37 members of the public who were recruited to take part in a face-to-face cognitive interview. Cognitive interviewing methods explore participants’ thought processes as they attempt to go about answering survey questions. These methods assessed participants’:

- initial reaction to the new screening questions; and
- understanding of the test questions.

In addition, the testing explored any difficulties participants had in being able to answer the questions, such as recall of the event and whether the new screener questions are picking up the types of crimes they are designed to identify.

As part of the testing, different forms of the new screener question wording were compared using a split ballot design, whereby participants were asked one or other version of the question and responses compared. The questions were tested over two rounds. Findings from round one were used to revise the questions, which were tested at round two. A summary of these findings is contained in chapter 3 with chapter 4 presenting recommendations on the question wording to be taken forward. Appendix B contains more detailed findings from the cognitive testing for each test question. Appendix C contains the details of the test questions and cognitive interviewing protocols used. Appendix D contains further information on the stage two cognitive testing methodology.

Stage three involved making recommendations on further development and testing that may be needed before the questions can be included as part of the CSEW time series. These recommendations are presented in Chapter 5.
2 Measuring fraud and cybercrime

The stage one review identified a number of challenges in measuring fraud and cybercrime as well as the strategies used on a range of international, general population surveys to overcome these. These were evaluated to determine those strategies that might be most appropriate for the CSEW. This chapter summarises the approach taken to developing the new questions that were tested using cognitive interviewing methods. We also discuss the challenges and strategies developed to tackle them.

2.1 Question development

Stage one of this research identified and examined existing evidence reviews that had been conducted over the past five years and covered a range of issues, including McGuire & Dowling, 2013; Kerr et al, 2013; Button et al, 2009. Other literature on fraud, cyber and online crime were also considered (see References at the end of this report). In addition questions on fraud and cybercrime from ten national surveys, see Appendix A for a list, were reviewed to identify the range of questions and methodologies being used. Questions asked by Action Fraud – the national fraud and cybercrime reporting service - were also reviewed. This evidence was used to develop the new screener questions and revisions to existing victimisation questions that were subsequently tested.

2.1.1 Development of new screener questions

Fraud

The review identified five broad, potentially overlapping categories of fraud, comprising of eight ‘types’, shown in Figure 2.1. In the vast majority of cases, these frauds can be perpetrated entirely offline, supported by online activity, or be perpetrated entirely online. For this reason, the screener questions developed on fraud were kept broad, focusing on the intrinsic characteristics of the different ways of committing fraud. This focus was also consistent with the aim of ‘future-proofing’, as far as possible, the new screener questions. This aim was concerned with minimising the need for changes to question wording to reflect changes in technology or the modus operandi of fraudsters. Two main categories were identified - confidence and non-confidence frauds - which cover the five sub-categories shown in Figure 2.1. Figure 2.2 shows how the five categories map onto the confidence-non-confidence classification.

The questions developed and tested as part of this research were based on these two broad categories of fraud.

---

4 More details on Action Fraud are available at http://www.actionfraud.police.uk/
<table>
<thead>
<tr>
<th>Identity theft</th>
<th>Identity theft: Theft of personal information, including identification-related data and financial information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraudulent use of information</td>
<td>Banking frauds: card-not-present fraud; plastic card fraud</td>
</tr>
<tr>
<td></td>
<td>Application frauds: Submitting an application using another person’s personal details for example, loans and mortgages; transferring ownership of property; using another person’s details for other forms of gain for example, electoral fraud.</td>
</tr>
<tr>
<td>Advance fee frauds</td>
<td>Inheritance fraud: request to send money to help someone in trouble; requesting a ‘bond’ to sell victim’s shares; lottery, sweepstake or competition frauds; other requests for fee to claim a financial benefit.</td>
</tr>
<tr>
<td>Fraudulent sales</td>
<td>(E-)Commerce frauds: Money or personal information taken for goods or services that do not arrive or prove to be counterfeit for example, tickets, weight loss products, psychics, holiday clubs, rental flats, loans, career opportunities, charity collections.</td>
</tr>
<tr>
<td></td>
<td>Investment frauds: Ponzi schemes; market abuse; selling of investments that don’t exist (for example, IPOs, foreign exchange); land banking; investments where resale is unlikely for example, emissions trading certificates, gold, rare metals, coloured diamonds and wine; high risk investments.</td>
</tr>
<tr>
<td></td>
<td>Money-making frauds: Pyramid schemes, working from home frauds.</td>
</tr>
<tr>
<td>Romance frauds</td>
<td>Request for money to cover an activity or crisis; extortion through recording of intimate acts. This would include the long-term building of relationships and shorter periods of contact between the perpetrator and the victim.</td>
</tr>
</tbody>
</table>
Figure 2:2 Categories of fraud

**Non-confidence frauds**

- **Banking frauds, Application frauds**
  - Fraudulent use of personal information for gain
  - Fraudulent use of financial information for gain

- **(E-)commerce frauds, investment frauds, money-making frauds**
  - Fraudulent sale of a product, service or opportunity, where the product exists but not as sold

**Identity theft**
- Theft of non-financial personal information
- Theft of financial personal information

**Confidence frauds**

- **Advance fee frauds**
  - Request for up-front payment in order to receive a benefit of some kind

- **(E-)commerce frauds, investment frauds, money-making frauds**
  - Fraudulent sale of a product, opportunity or service, where the product does not exist

- **Fraudulent relationships**
  - Romance frauds
  - Making someone believe they are in a relationship, for financial gain
Theft of personal information

The evidence mapping identified further forms of online crime, which include individual rather than organisational victims. One of these forms of crime was theft of personal information or data held digitally, where no fraud has (yet) taken place and it was decided to include a separate screener question on this crime. Two alternative questions on theft of personal data were developed and tested: one focusing on the theft of personal information or data held digitally; the other covering theft of personal information or data held in any form.

Interference with internet and computer access

Another form of online crime identified by the evidence review was interference with internet and computer access. This includes crimes such as spreading viruses or malicious software and creating botnets, hacking, or DDoS attacks. It includes crimes that may or may not be targeted at an individual victim, but where individuals are victimised (for example, their computer being damaged by a virus) and could occur across a range of digital devices.

A screening question on this type of crime was developed and tested.

2.1.2 Defining incidents

The stage one review looked at how incidents of fraud, cyber and online crime should be defined and counted, see Appendix A, and the findings informed the approach tested at stage two. In Section 2.2 the challenges of defining and counting incidents are summarised.

2.1.3 Victimisation module

The review also looked at the victimisation module questions concerned with:

- when the incident(s) took place;
- what happened; and
- other contextual information, such as where it took place, why it occurred and contact with the police.

At stage two a subset of victimisation module questions were tested, including when and where the incident occurred, what happened and the impact of the incident on the victim, both financially and emotionally. Details of the questions tested and the findings are provided in Appendix B.

2.1.4 Other online and cybercrimes considered as part of the desk review

The desk review highlighted that existing screener questions, such as those on violence, threatening violence and sexual violence could be carried out online. These questions may require some revision to reflect this – see Appendix A.
2.2 Challenges in measuring fraud and cybercrime

It is recognised that the measurement of fraud and cybercrime victimisation is challenging, see for example the ONS discussion paper on the coverage of crime statistics (ONS, 2014). In developing new questions a number of challenges were identified to which solutions were sought. Figure 2.3 sets out these challenges.

It is worth noting that in some cases, i.e. number of incidents and location, while a challenge was identified a solution was not proposed ahead of testing. Instead the current CSEW approach was tested so as to gain further understanding of the issues and identify potential remedies. A discussion of remedies is provided in Chapter 3.

Figure 2.3 Measurement challenges and strategies to tackle them

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practical</td>
<td>Minimise, as far as possible, the impact of including new screening and victim form questions into the survey on interview length, response rates, data quality and time series data.</td>
</tr>
<tr>
<td></td>
<td>Introduce a small number of new screening questions. The format of these new questions should follow that of the existing ones where possible to ensure consistency.</td>
</tr>
<tr>
<td></td>
<td>New questions should be positioned towards the end of the screener, in the personal crimes section after the question on domestic violence.</td>
</tr>
<tr>
<td></td>
<td>The victim form questions should be tailored to reflect the new crimes being included and the requirements of the 2014 Home Office counting rules for these (see section 4.4).</td>
</tr>
<tr>
<td>Definitions</td>
<td>Fraud – there is a wide range of ways in which offences are committed. There is a lack of agreed definitions of different types of fraud (Button, 2009)</td>
</tr>
<tr>
<td></td>
<td>Include new screening questions on fraud.</td>
</tr>
<tr>
<td></td>
<td>Define fraud in terms of its intrinsic features rather than modus operandi, distinguishing between confidence and non-confidence frauds (see section 2.1.1).</td>
</tr>
<tr>
<td></td>
<td>Exclude frauds committed against businesses and against survey participants who were living outside England and Wales at the time the offence occurred.</td>
</tr>
<tr>
<td>Challenge</td>
<td>Strategies</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Other forms of cyber-enabled crime</strong> are very broad</td>
<td>Many of these crimes are not targeted at individuals so would not be included in the CSEW. Other crimes are already potentially covered by existing screening questions, such as threatening violence. The exception is online harassment see section 4.2. Include a new screening question on theft of personal data from the individual, as this may be a precursor to a fraud taking place.</td>
</tr>
<tr>
<td><strong>Cyber-dependent crimes</strong> include interference with internet and computer access, for example, by viruses.</td>
<td>Include a new screening question on interference with internet and computer access as a result of, for example viruses and DDoS attacks on ‘internet enabled devices’ used by participants for personal use. Exclude attacks made on devices used solely for business purposes.</td>
</tr>
<tr>
<td><strong>Number of incidents</strong></td>
<td>The current CSEW questions were tested. Victims may not know this information or have sufficient knowledge to be able to provide an accurate answer.</td>
</tr>
<tr>
<td><strong>Reference periods</strong></td>
<td>The survey can only collect data on incidents that participants are aware of. Victims of some cyber enabled and dependent crimes may not be aware they have been victimised until sometime after the incident took place. Victims may not know, for example, when their personal details were first obtained or when money was first taken from their account until the matter is brought to their attention by the authorities.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Collect information on where the participant was living when the incident occurred. Only include incidents where participants</td>
</tr>
<tr>
<td>Challenge</td>
<td>Strategies</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>place anywhere in the world.</td>
<td>were living in England and Wales at the time the incident occurred.</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>The diverse and continually evolving ways in which fraud and cybercrime can occur mean it can be described and understood by members of the public in a multitude of ways.</td>
</tr>
<tr>
<td></td>
<td>Use non-technical language where possible, which is consistently understood as intended.</td>
</tr>
<tr>
<td><strong>Attempts and actual victimisation</strong></td>
<td>Participants may not be aware that an attempt has occurred or how an attempt might be linked to a completed crime.</td>
</tr>
<tr>
<td></td>
<td>For confidence fraud, theft of personal data and interference with internet and computer access, attempts should not be captured. Participants may be less likely to know that there has been an attempt, an individual may not have been specifically targeted and the Home Office counting rules do not include such attempts.</td>
</tr>
<tr>
<td></td>
<td>However, for non-confidence fraud attempts and actual victimisation should be counted, in line with Home Office counting rules.</td>
</tr>
<tr>
<td><strong>Series</strong></td>
<td>Victims may not know whether the same person or group of people was behind each incident. This applies to all crimes, not just fraud and cybercrime.</td>
</tr>
<tr>
<td></td>
<td>Ask the current ‘series’ questions in the knowledge that some participants will not know whether the incidents were carried out by the same people or not.</td>
</tr>
<tr>
<td><strong>In-scope incidents</strong></td>
<td>The CSEW is concerned only with the victimisation of individuals and their households not businesses. This distinction may pose difficulties for certain groups, such as the self-employed and could lead to errors such as over-reporting. This problem is not specific to fraud and cybercrime: other crimes covered by the CSEW may also be affected.</td>
</tr>
<tr>
<td></td>
<td>Screener question wording should make explicit that the survey is only interested in personal fraud i.e. that targeted against participants for non-confidence fraud, their households.</td>
</tr>
<tr>
<td></td>
<td>Although non-confidence fraud and interference with internet and computer access can be seen as crimes against a business (for example, a bank)</td>
</tr>
</tbody>
</table>
In developing these proposed strategies a number of pragmatic decisions were made. These are set out in the rest of this chapter.

**Placement of the new screener questions**

As described in section 1.1 the Crime Survey’s approach to measuring the prevalence and volume of victimisation has hardly changed in over 30 years. As such it allows researchers to look at changes over time on a consistent basis. Adding new screening questions will mean more incidents of victimisation are likely to be captured. This impact on the time series is unavoidable. The inclusion of new screening questions might also affect the way in which existing questions are interpreted by participants. This change might also disrupt the time series. To mitigate this risk a small number of new screener questions were developed, which were placed at the end of the current screening questions. In adopting this approach it is recognised that some forms of fraud and interference with internet and computer access may not be directed at the individual. Some incidents may be directed at the household, for example a joint bank account may have been compromised, a shared computer infected with a virus.
Location

The CSEW only captures information on crimes committed in England and Wales. However, as McGuire and Dowling (2013) note cyber-crime is a global phenomenon that is not constrained by national boundaries. Asking only about fraud and cyber offences that have taken place in England and Wales is likely to be problematic because participants may not know where the offence took place. An alternative approach is required. Initially the approach adopted was that taken by the Scottish Crime and Justice Survey whereby participants are asked where the incident happened, with a code for ‘on the internet/online’. However, findings from the first round of cognitive interviews suggested this approach was problematic because, as mentioned, some participants did not know where the crime occurred or answered in terms of where they were when they found out about it (for example, ‘home’) rather than where the crime was committed (for example, another part of England and Wales, see Figure B.3). Based on this evidence an alternative approach was developed, whereby participants were asked where they were living when they found out they had been victimised. The success of this revised approach is discussed in chapter 3. It is acknowledged that this approach could inflate the estimates of victimisation for these incidents compared with just asking about crimes that took place only in England and Wales.

Of course the issue of participants not knowing where the offence took place is not specific to fraud and cyber-crime. For example, a participant may not know where their wallet was stolen. However, the problem is likely to be more acute for fraud and cybercrime. It is recognised that by adopting two different approaches the survey will measure different types of incident in different ways.

Number of incidents

The counting of incidents should follow the Home Office counting rules for police recorded crime. The following extract illustrates how the rules would be applied to an incident of non-confidence fraud.

Generally this will equate to one crime per credit card, cloned card, cheque book or online account.

**Example 4:** Five cheques from a previously reported stolen cheque book are used to obtain goods from the same store. They are reported to the police at different times.

*One crime - cheque and credit card fraud (class NFIB5A). They are all from the same account.*

Example 1: A stolen credit card or cheque book has been used to obtain goods from two shops which reported the incidents separately. During police enquiries 57 other crimes, involving identifiable and different victims, are discovered using the same credit card or cheque book account.

*One crime (class NFIB5A). They are all from the same account plus original theft of card or cheque book (class 49).*

*Home Office Counting Rules; 2014*
Dealing with crimes against businesses

The CSEW excludes crimes against businesses; focusing solely on crimes against individuals and other household members. A self-employed electrician could, for example, have left their tools in their car and had them stolen. This incident would not be included in the survey estimates. However the offence coding becomes more complex if the tools and or vehicle are not solely used for work. This ‘grey area’ becomes more problematic for fraud and cybercrime where increasingly internet-enabled devices are used for personal as well as work use. The approach proposed excludes devices and accounts used solely for business use, but includes devices used for both work and personal use.
3 Success in meeting the challenges

The cognitive interviews conducted as part of this study provide qualitative evidence on the performance of the test questions against their measurement objectives. This evidence can be used to assess the success of the question-design approach in overcoming the challenges discussed in chapter 2. However, for some challenges the cognitive testing was not able to provide any evidence due to the limitations of the method and small sample size. In this chapter we summarise the evidence from the cognitive testing in relation to the challenges and identify where further evidence is required. A summary is provided in Figure 3.1. The recommended wording of the screening questions and victimisation module questions is provided in sections 3.1 and 3.2.
<table>
<thead>
<tr>
<th>Challenge</th>
<th>Approach(es)</th>
<th>Success of approaches – CI evidence</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practical</td>
<td>Minimise, as far as possible, the impact of including new screening and victim form questions into the survey on interview length, response rates, data quality and time series data.</td>
<td>Cognitive Interviewing (CI) evidence suggests the four screener-question approach (asking about confidence fraud, non-confidence fraud, theft of personal data and interference with internet and computer access) was successful in identifying fraud and cybercrime. However, potential double counting was identified as a problem. This particularly affected non-confidence fraud and theft of personal data, although confidence and non-confidence fraud were also affected.</td>
<td>Larger-scale, quantitative testing is required to assess the impact of including these new questions and amendments to the victimisation module on interview length, response rates, and the time series data (refer to chapter 5). To tackle the problem of double-counting an introduction to the new screener questions, the use of a show card showing the four new types of crime and a check question to ascertain if responses to more than one of the new screening questions are valid are proposed. In addition a number of check questions are proposed to establish whether incidents are linked (i.e. part of the same incident) or are separate, see chapter 4. These recommendations</td>
</tr>
</tbody>
</table>
### Evidence of success of approaches to overcome problems

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Approach(es)</th>
<th>Success of approaches – Cl evidence</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definitions</td>
<td><strong>Fraud</strong> – there is a wide range of ways in which offences are committed. There is a lack of agreed definitions of different types of fraud (Button, 2009)</td>
<td>Include new screening questions on fraud. Define fraud in terms of its intrinsic features rather than modus operandi, distinguishing between confidence and non-confidence frauds (see section 2.1.1). Exclude frauds committed against businesses and against survey participants who were living outside England and Wales at the time the offence was committed</td>
<td>The Cl evidence indicates that the two fraud questions – on confidence and non-confidence fraud - were understood as intended. However, there was some evidence of double-counting, with some participants answering ‘yes’ to both questions about the same incident. This appears to be related to question order.</td>
</tr>
<tr>
<td>Other forms of cyber-enabled crime are very broad</td>
<td>Many of these crimes are not targeted at individuals so would not be included in the</td>
<td>CI participants understood the question on theft of personal data as intended. However evidence of double-counting</td>
<td>A check question is proposed, see section 4.1, to ascertain whether the theft of personal data was in fact a precursor to</td>
</tr>
</tbody>
</table>
### Figure 3:1  Evidence of success of approaches to overcome problems

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Approach(es)</th>
<th>Success of approaches – CI evidence</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSEW.</td>
<td>Other crimes are already potentially covered by existing screening questions, such as threatening violence. The exception is online harassment see section 4.2. Include a new screening question on theft of personal data from the individual, as this may be a precursor to a fraud taking place.</td>
<td>was identified, with participants answering ‘yes’ to both the theft of personal data and non-confidence fraud screener questions.</td>
<td>the non-confidence fraud reported or whether it was a separate, stand-alone incident. Further larger scale, quantitative testing is recommended to further assess data quality, see chapter 5.</td>
</tr>
<tr>
<td><strong>Cyber-dependent crimes</strong> include interference with internet and computer access, for example, by viruses.</td>
<td>Include a new screening question on interference with internet and computer access as a result of, for example viruses and DDoS attacks on ‘internet enabled devices’ used by participants for personal use. Exclude attacks made on devices used solely for business purposes.</td>
<td>Evidence from the CI suggests that participants can provide information on interference with internet and computer access but the current wording of the new question is problematic</td>
<td>A revised version of the screener question is proposed, see section 4.1 and tested through further cognitive interviewing prior to field testing, see chapter 5.</td>
</tr>
<tr>
<td>Number of Victims may not know this</td>
<td>The current CSEW questions</td>
<td>Some inconsistencies were</td>
<td>The question should contain</td>
</tr>
<tr>
<td>Figure 3:1 Evidence of success of approaches to overcome problems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Challenge</strong></td>
<td><strong>Approach(es)</strong></td>
<td><strong>Success of approaches – CI evidence</strong></td>
<td><strong>Recommendations</strong></td>
</tr>
<tr>
<td>incidents</td>
<td>information or have sufficient knowledge to be able to provide an accurate answer.</td>
<td>were tested.</td>
<td>identified. In some cases of non-confidence fraud participants answered in relation to the theft of details (answering one), whilst in other cases they reported the number of times their bank card was used/ a transaction was made.</td>
</tr>
<tr>
<td>Reference periods</td>
<td>Victims of some cyber enabled and dependent crimes may not be aware they have been victimised until sometime after the incident took place. Victims may not know, for example, when their personal details were first obtained or when money was first taken from their account until the matter is brought to their attention by the authorities.</td>
<td>The survey can only collect data on incidents that participants are aware of.</td>
<td>The CI evidence indicates that without clear guidance participants will vary in terms of the date they provide (for example, some will provide the date the incident occurred and others the date they found out about it).</td>
</tr>
<tr>
<td>Location</td>
<td>The CSEW collects information on the volume and prevalence of crime in England and Wales. However fraud and cyber-crime can take place anywhere in the</td>
<td>Collect information on where the participant was living when the incident occurred. Only include incidents where participants were living in England and Wales at the time</td>
<td>Generally participants were able to answer the question ‘where were you living when this [incident] occurred?’ However, there were cases where participants found it</td>
</tr>
</tbody>
</table>
## Figure 3:1 Evidence of success of approaches to overcome problems

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Approach(es)</th>
<th>Success of approaches – Cl evidence</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>The diverse and continually evolving ways in which fraud and cybercrime can occur mean it can be described and understood by members of the public in a multitude of ways.</td>
<td>Use non-technical language where possible, which is consistently understood as intended.</td>
<td>Overall the language used in the new screener questions was well-understood. The exception was the wording of the question about viruses where the term ‘installed software’ caused confusion.</td>
</tr>
<tr>
<td>Attempts and actual victimisation</td>
<td>Participants may not be aware that an attempt has occurred or how an attempt might be linked to a completed crime. For certain types of fraud and cybercrime attempts are likely to be far more numerous than completed crimes and this could inflate the overall crime figures.</td>
<td>For confidence fraud, theft of personal data and interference with internet and computer access, attempts should not be captured. Participants may be less likely to know that there has been an attempt, an individual may not have been specifically targeted and the Home Office counting rules do not include such attempts.</td>
<td>Participants understood that they were only being asked to provide details of actual confidence frauds, theft of data and virus attacks.</td>
</tr>
<tr>
<td>Challenge</td>
<td>Approach(es)</td>
<td>Success of approaches – CI evidence</td>
<td>Recommendations</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Series</strong></td>
<td>However, for non-confidence fraud attempts and actual victimisation should be counted, in line with Home Office counting rules.</td>
<td>CI data were limited with only four participants being asked these questions. All correctly interpreted the question but their ability to answer it varied depending on what they knew about the circumstances in which offences took place.</td>
<td>Further larger-scale, quantitative testing is required to assess data quality.</td>
</tr>
<tr>
<td>In-scope incidents</td>
<td>Victims may not know whether the same person or group of people was behind each incident. This applies to all crimes, not just fraud and cybercrime.</td>
<td>CI evidence was limited with regards to whether the self-employed only reported crimes relating to them personally and not to their business. This was in part due to the small number of self-employed people included in the cognitive testing.</td>
<td>Further larger-scale, quantitative testing is required involving a larger group of self-employed people to assess the success of the proposed new questions. A new question in the victimisation module should establish whether the account was in the participant’s name</td>
</tr>
<tr>
<td></td>
<td>Ask the current ‘series’ questions in the knowledge that some participants will not know whether the incidents were carried out by the same people or not.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Screener question wording should make explicit that the survey is only interested in personal fraud i.e. that targeted against participants and, for non-confidence fraud, their households.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Although non-confidence fraud and interference with internet and computer access can be</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Challenge</td>
<td>Approach(es)</td>
<td>Success of approaches – CI evidence</td>
<td>Recommendations</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>Participants may be unwilling to disclose being victimised because of shame or self-blame.</td>
<td>CI evidence was limited, making it difficult to assess the extent of under-reporting that may occur. However the testing identified one case.</td>
<td>Further larger-scale testing is required to assess this. However, measurement of social desirability bias is not straightforward. Options are</td>
</tr>
</tbody>
</table>

seen as crimes against a business (for example, a bank) and not an individual, individuals can feel victimised and as such the survey should capture such incidents.

If participants use an internet-enabled device only for business this should not be included. However if it is used for both personal and business use it should be included on the basis that in practice it will not be possible to identify whether the individual or business were the target. It is recognised that this approach may mean some business crime is captured by the survey.

Figure 3:1 Evidence of success of approaches to overcome problems

Option 1

Evidence of success of approaches to overcome problems

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Approach(es)</th>
<th>Success of approaches – CI evidence</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitivity</td>
<td>Participants may be unwilling to disclose being victimised because of shame or self-blame.</td>
<td>CI evidence was limited, making it difficult to assess the extent of under-reporting that may occur. However the testing identified one case.</td>
<td>Further larger-scale testing is required to assess this. However, measurement of social desirability bias is not straightforward. Options are</td>
</tr>
</tbody>
</table>

seen as crimes against a business (for example, a bank) and not an individual, individuals can feel victimised and as such the survey should capture such incidents.

If participants use an internet-enabled device only for business this should not be included. However if it is used for both personal and business use it should be included on the basis that in practice it will not be possible to identify whether the individual or business were the target. It is recognised that this approach may mean some business crime is captured by the survey.
<table>
<thead>
<tr>
<th>Figure 3:1 Evidence of success of approaches to overcome problems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Challenge</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Future-proofing</td>
</tr>
</tbody>
</table>

where a participant was too embarrassed to initially report being the victim of a fraud, which suggests there is a risk. discussed in section 5.2.3.
4 Recommendations for question wording

4.1 Recommendations for screener questions

Screener questions wording

The proposed wording of new screener questions, set out below, is based on a review of evidence from the cognitive interviews carried out in stage two of this research and reference to the findings from the stage one desk review. Recommendations are made for question wording, answer options, routing and interviewer instructions.

CON

[Apart from anything you have already mentioned], in that time …have you been tricked or deceived out of money or goods, in person or online? YesNo

INTERVIEWER: IN PERSON INCLUDES TELEPHONE.

NCON [ASK IF CON=YES]

As far as you are aware, how many times has that happened? If you received multiple communications about the same scam please count as one incident.

NOTE: 97 = 97 OR MORE/TOO MANY TO REMEMBER. USING CODE 97 CAN CAUSE PROBLEMS IN SEPARATING SINGLE AND SERIES INCIDENTS, SO PROBE FOR BEST ESTIMATES WHERE POSSIBLE

ENTER NUMBER

97 More/too many to remember

VIRUS

Apart from anything you have already mentioned], in that time…has an internet-enabled device of yours been infected, for example by a virus? YesNo

INTERVIEWER: IF R MENTIONS RANSOMWARE, BOTNETS, DDoS ATTACKS, MALWARE THEN CODE YES.

IF VIRUS=YES

---

To keep the wording as short as possible we use the phrase ‘in person’ to cover face-to-face and telephone interactions. There was no evidence found in testing that confidence frauds involving telephone interactions were being missed. This should be assessed as part of the larger scale field testing.
ANTIVIR

Was it blocked by anti-virus software?

Yes – GO TO CMACT

No (INCLUDE does not have anti-virus software or anti-virus software out of date) – ASK NVIRUS

NVIRUS [ASK IF ANTIVIR=NO]

As far as you are aware, how many times has that happened?

NOTE: 97 = 97 OR MORE/TOO MANY TO REMEMBER. USING CODE 97 CAN CAUSE PROBLEMS IN SEPARATING SINGLE AND SERIES INCIDENTS, SO PROBE FOR BEST ESTIMATES WHERE POSSIBLE

ENTER NUMBER

97 More/too many to remember

CMACT

Apart from anything you have already mentioned], in that time has anyone accessed or obtained information or details about you without your permission? YesNo

NCMACT [ASK IF CMACT=YES]

As far as you are aware, how many times has that happened?

NOTE: 97 = 97 OR MORE/TOO MANY TO REMEMBER. USING CODE 97 CAN CAUSE PROBLEMS IN SEPARATING SINGLE AND SERIES INCIDENTS, SO PROBE FOR BEST ESTIMATES WHERE POSSIBLE

ENTER NUMBER

97 More/too many to remember

NONCON

Apart from anything you have already mentioned], in that time …has your personal information or account details been used or tried to be used to obtain money, or buy goods or services without your permission or knowledge? YesNo

NNONCON [ASK IF NONCON=YES]

As far as you are aware, how many times has that happened? Please tell me how many separate incidents there were.

INTERVIEWER: We want to record here the number of times this type of incident has occurred. We do not want to record how many times within each incident the participant’s information was used. For example, if the participant has had their bank card cloned on one occasion and the card was used 3 times, we would only want to record one occasion of the card being cloned (not the 3 times it was used).
NOTE: 97 = 97 OR MORE/TOO MANY TO REMEMBER. USING CODE 97 CAN CAUSE PROBLEMS IN SEPARATING SINGLE AND SERIES INCIDENTS, SO PROBE FOR BEST ESTIMATES WHERE POSSIBLE

ENTER NUMBER

97 More/too many to remember

In the case of interference with internet access significant amendments were made to the question wording as a result of an analysis of the round two cognitive interview data. It is therefore recommended that further cognitive testing of this question be carried out ahead of any field testing.

I am now going to ask you some more about the time since \^DATE.

**+SIMILAR_26 [ASK IF NCON > 1]**

You mentioned [WRITE IN NUMBER OF CON INCIDENTS FROM NCON] incidents of being tricked or deceived out of money or goods, either in person or online. As far as you are aware, were any of these very similar incidents, where the same sort of thing was done under the same circumstances and probably by the same people?

1. Yes
2. No

**+SIMILAR_28 [ASK IF NVIRUS > 1]**

You mentioned [WRITE IN NUMBER OF CMACT INCIDENTS FROM NVIRUS_____] incidents of having your internet-enabled device infected, for example by a virus that was not blocked by antivirus software. As far as you are aware, were any of these very similar incidents, where the same thing was done under the same circumstances and probably by the same people?

1. Yes
2. No

**+SIMILAR_27 [ASK IF NCMACT > 1]**

You mentioned [WRITE IN NUMBER OF CMACT INCIDENTS FROM NCMACT_____] incidents of someone accessing or obtaining information about you without your permission. As far as you are aware, were any of these very similar incidents, where the same thing was done under the same circumstances and probably by the same people?

1. Yes
2. No
You mentioned [WRITE IN NUMBER OF NONCON INCIDENTS FROM NNONCON____] incidents of your personal information or account details being used or tried to be used to buy goods or services without your permission or knowledge. As far as you are aware, were any of these very similar incidents, where the same sort of thing was done under the same circumstances and probably by the same people?

1. Yes
2. No

It is recommended that the current questions asked to sort out the series pattern are asked in relation to the new screener questions. These questions should be assessed as part of the larger scale quantitative testing, see chapter 5.

Additional issues to be considered

Analysis of the cognitive interviews identified a number of additions to the current screener module that should be considered. These are as follows.

- The inclusion of an introduction, to be read aloud by the interviewer ahead of asking the new screener questions on fraud and cybercrime. The introduction might look something like this:

  I am now going to ask you about your experience of some other types of crime that you might have experienced or become aware as having happened in the last 12 months. The types of crime I am going to ask about are shown on this card. I'll ask you about each one in turn.

SHOW CARD

- Being tricked or deceived out of money or goods, in person or online
- An internet-enabled device of yours being infected, for example, by a virus
- Your personal information or details being accessed or used without your permission
- Your personal information or account details being used or tried to be used to obtain money, or buy goods or services

It is recommended that this introduction and show card be tested using cognitive interviewing methods, prior to its inclusion in the larger-scale field test proposed in chapter 5.

- The cognitive testing highlighted that in some cases participants answered ‘yes’ to more than one screener question about the same incident. This problem was noted as particularly affecting theft of personal data (CMACT) and non-confidence fraud (NONCON) and reflects the fact that, as noted in section 2.1.1, non-confidence fraud may involve the theft of personal data. The screener question on theft of personal data is designed to identify incidents where no non-confidence fraud has actually occurred, as far as the victim is aware.
To address this problem additional check questions are proposed. These would identify any incidents that have been picked up by more than one screener question and provide the interviewer with priority coding rules so that only one screener question is coded positively. These new check questions would be included after the individual screener questions but before the questions checking whether incidents are part of a series. The check questions proposed are as follows.

**CMACHK1**
IF CMACT=YES AND NONCON=YES

You mentioned that someone had accessed or obtained information or details about you without your permission and that your personal information or account details been used or tried to be used to obtain money, buy goods or services without your permission. Can I just check, were these incidents linked? Yes, No, DKREF

[Interviewer: IF LINKED (CHECK Q=YES) CODE CMACT NO and NONCON YES]

**CMACHK2**
IF NONCON=No and any type of theft=Yes. Ask check for each type of theft.

You mentioned that someone had (TEXTFIL TYPE OF THEFT INCIDENT). Can I just check whether your personal information or account details were used or were tried to be used to obtain money or buy goods or services without your permission or knowledge as a result of this ^THEFT. Yes, No, DKREF

[Interviewer: IF LINKED (CHECK Q=YES) CODE NONCON=YES]

**CMACHK3**
If CMACT=Yes and NONCON=NO

You mentioned that someone had accessed or obtained information or details about you without your permission. As far as you are aware, was this information used or attempted to be used to obtain money or buy goods or services without your permission or knowledge? Yes, No

[Interviewer: IF YES THEN AMEND CODING. CMACT SHOULD BE CODED NO AND NONCON CODED YES].

The exact wording of these check questions requires some further consideration. If participants have experienced more than one incident of theft of personal data or non-confidence fraud then the wording of the check may need to change. The wording of these check questions should be cognitively tested before they are included in a larger scale field test.

---

66 This check would be asked if any of the following theft questions are answered ‘yes’: HOMETHEF, YRHOFTHEF, YRHOSTOL, PERSTHEF, TRYPERS, OTHTHEF.
4.2 Including a screener question to identify online harassment

This research did not cover the development of a new screener question on online harassment. However, the desk review identified that such incidents are included in the Government Serious and Organised Crime Strategy. Online harassment is thought to be on the increase and there is a case for including it in the CSEW screener module. If ONS wish to include online harassment then it is recommended that a new screener question is developed and tested.

4.3 On-line threats of violence and sexual offences

The desk review also highlighted that the current screener questions on threats of violence and sexual assault do not explicitly mention online incidents (see A2.1.2). It is currently unclear whether these types of incident are being captured. This research did not explore these issues further. It is suggested that ONS pay further consideration to whether these existing screener questions need amendment to ensure online incidents are captured.

4.4 Recommendations for victimisation questions

As mentioned in section 1.2, stage two focused primarily on the development of new screener question. Some existing victimisation module questions were tested alongside some new questions on the cost (both financial and time) for the victim of the incident. The following recommendations for their wording are made. These are based on an analysis of the cognitive interview data for these questions.

Date when incident occurred (revised, existing questions)

Currently the CSEW asks about when an incident happened. However, research evidence reviewed as part of this study suggests that victims of fraud and cybercrime do not always know when the incident took place. Findings from testing support this evidence. We propose that the approach used on the US National Crime Victimisation Survey be adopted whereby participants are asked when they discovered the incident. It is acknowledged that this may lead to some incidents being included within the reference period that actually took place outside it (i.e. more than 12 months ago) however our hypothesis is that this approach will lead to fewer missing answers (i.e. Don’t knows). We make some proposals for assessing the extent of this problem in section 5.2. The recommended questions are set out below.

DATESERA  [ASK IF SERIES OF SIMILAR INCIDENTS]
You mentioned a series of [ENTER NUMBER FROM CNUMSER_________] similar incidents of ^CRIME TYPE7^ since the first ^DATE^.

7 Textfill for ^CRIME TYPE
(CON) *being tricked or deceived out of money or goods
(VIRUS) *your internet-enabled device being infecting, for example with a virus
{FOR NEW SCREENER Qs ASK} When did you become aware these incidents happened?

**MTHRECIN**  [ASK IF MORE THAN ONE INCIDENT IN A QUARTER AT NQUART AND NEW SCREEENE]

{FOR NEW SCREENERS} When did you become aware that the most recent of these incident(s) had happened?

**MTHINC2**  [ASK IF SINGLE INCIDENT]

You said that, since the first of ^DATE^, you had an incident of ^CRIME TYPE^.

{FOR NEW SCREENER Qs ASK} In which month did you become aware that it had happened?

**QTRINCID**  [ASK IF MTHINC2=DK]

In what quarter (IF NEW SCREENER Qs) ^did you become aware the incident had happened? Was it ...

1. Before [the first of ^DATE^]
2. Between [^QUARTER^]
3. Between [^QUARTER^]
4. Between [^QUARTER^]
5. Between [^QUARTER^]
6. Between [the first of ^DATE^] and the present?

**CHKRECI2**

And can I just check, [TEXTFIL – IF EXISTING SCREENER Q} ^did the incident happen before or after the first ^DATE^?^?

Circumstances of incident (new questions)

Proposed questions on the circumstances of the incident are set out below.

**WHERLIVE**

And where were you living when you found out about this? Were you living …

READ OUT:
1. At this address
2. Somewhere else within 15 minutes of here
3. Somewhere else in England and Wales
4. Somewhere else (END VICTIM FORM)

{IF A CONFIDENCE OF NON-CONFIDENCE FRAUD}

(CMACT) ‘your personal information or account details being accessed’
(NONCON) ‘your personal information or account details being used or tried to be used to obtain money or buy goods and services’
HACK

Did they gain access to your account(s) by using your password, pin number or online security information?

1. Yes
2. No
3. Don’t know

IF NON-CONFIDENCE FRAUD

ACCOUNT

Was this/Were these account(s) in your name only or were they held jointly with someone else?

1. (All) in participant’s name only
2. (All) held jointly with someone else
3. Some held in participant’s name only, some held jointly

Costs of crime (new questions)

(IF A CONFIDENCE OF NON-CONFIDENCE FRAUD)
FRLOSS2

How much money, if any, did you personally lose? Please DON’T include any money that was subsequently refunded but DO include any additional charges or costs that you incurred as a result of the incident.

1. None OR all money was refunded
2. Less than £1
3. Up to £5
4. Up to £10
5. Up to £50
6. Up to £500
7. Up to £1,000
8. £1,000 or more
9. Not yet resolved
99. DK/REF

FRLOSS3 [ASK IF FRLOSS2 CODED 8– LOST £1000 OR MORE]

You said you lost more than £1000. How much did you personally lose?

ENTER AMOUNT TO NEAREST £1,000
{IF A THEFT OF PERSONAL DATA}
CMALOSS1
How much money, if any, did this incident personally cost you? Please DON’T include any money that was subsequently refunded but DO include any additional charges or costs that you incurred as a result of the incident.
1. None OR all money was refunded
2. Less than £50
3. £50 - £99
4. £100 - £249
5. £250 - £499
6. £500 - £999
7. £1,000 - £2,499
8. £2,500 - £4,999
9. £5,000 or more
10. Not yet resolved

{ASK ALL}
TRES
How long did it take to resolve this most recent incident?
1. Less than one week
2. Less than two weeks
3. Less than one month
4. One to less than three months
5. Three to less than six months
6. Six months or more
7. It is still on-going
8. Case has been closed but is unresolved

TRIGHT
How much time, overall, do you estimate you spent dealing with this incident to put things right? If it is still on-going or has been closed but is unresolved then please estimate how much time you have spent so far.
1. A couple of hours
2. A couple of days
3. Up to a week
4. More than a week
5. More than a month
Use of force (revised existing questions)

**WHENMOT**  **[ASK ALL]**
SHOW CARD
Which, if any, of these reactions did you PERSONALLY have?
CODE ALL THAT APPLY
1. Anger
2. Shock
3. Fear
4. Depression
5. Anxiety/panic attacks
6. Loss of confidence/feeling vulnerable
7. Difficulty sleeping
8. Crying/tears
9. Annoyance
10. Foolishness / embarrassment
11. Frustration
12. Other (SPECIFY)
13. None of these

**HOWAFF1**  **[ASK IF WHENMOT NOT EQUAL TO NONE OF THESE]**
Overall, how much were you affected? Were you affected ...READ OUT
1. Very much
2. Quite a lot
3. or just a little?

**IMPACT2**  **[ASK ALL]**
SHOW CARD
Looking at this card which, if any, of these things happened to you as a result of this incident? CODE ALL THAT APPLY
1. Financial loss
2. Time off work
3. Loss of employment
4. Relationship breakdown
5. Avoided social situations
6. Inconvenience
7. Moved house
8. Took additional security precautions (for example, installing a burglar alarm, installing a firewall or anti-virus software)
9. Loss of trust in other people/the public
10. Time off from school/college/university
11. Impact on health
12. Effect on personal confidence
13. Had to purchase new equipment
14. I no longer use the internet at all
15. I use the internet less
16. I no longer use certain internet sites or services / I am more cautious online
17. I no longer use the internet in public places
18. Other (SPECIFY)
19. No impact
4.5 Content of the victimisation module for the new screener questions

The current victimisation module is made up of 15 sections. These are shown in Figure 4.1. A review of the current victimisation module suggests that the current content and routing is not appropriate for the new screener questions on fraud, theft of personal data and computer interference.

The incident checklist questions, shown in Figure 4.2, along with the question WHERE1, which establishes whether the incident happened inside the victim’s home or garage, drive the routing through the victimisation module. The current incident checklist questions and WHERE1 are not appropriate to the new screener questions. New incident checklist questions are therefore required for fraud, theft of personal data and computer interference. The development of these new incident checklist questions fell outside the scope of this project. It is recommended that such questions are developed and tested.

The current victimisation module requires considerable amendment to accommodate the new types of crime to be included in the CSEW. Whilst this level of amendment
may be possible it would be time-consuming. Moreover the extent of amendments required could lead to errors being made, which could disrupt the time series data on existing crimes. To mitigate this risk a new victim form could be designed to cover incidents of fraud, theft of personal data and computer interference. The current victim form would remain unchanged, and continue to be used for existing crime incidence covered by the CSEW.

Questions in the existing modules on plastic card fraud, mass marketing fraud and internet security could be included in the victim form, where relevant, and dropped from the existing modules. The dropping of questions from these modules would make space for the new screener and victimisation module.

Content of the new module

The content of this new victimisation module would need to be developed. However it is recommended that as a starting point the Home Office counting rules for recorded crime should be consulted to inform the development of the incident check list questions for the new incidents included in the screener. This will ensure that the offence can be coded correctly.

The CSEW currently contains modules on online security, mass marketing and plastic card fraud and these modules should be reviewed to identify any questions that could be moved into the new victim form. A cursory review of these modules suggests the following questions could be included.

- Did the virus infect your computer as a direct result of opening an email or web link?
- What type of personal data was accessed?
- How was the money taken? (for example, stolen cards, access to online banking)
- How did you find out that money had been taken?
- How did you find out your personal information or data had been accessed?

The new victimisation module would also include questions on whether the incident was reported to for example, the police, Action Fraud or Trading Standards and victim’s satisfaction with how the incident was dealt with.

The current Online Security module has a longer list of questions on this topic compared to the existing victim form, and this may be a useful starting point.

4.5.1 Confidence fraud vs consumer detriment

The cognitive testing highlighted a grey area between confidence fraud and consumer detriment. Participants may feel they have been ‘conned’ or ‘deceived’ into purchasing something that was not what they thought it was. Participants will be answering the new question of confidence fraud in the context of a crime survey and so this might mean that the inclusion of consumer detriment incidents may be reduced. However, clear coding rules (and follow up questions in the victimisation) are needed that allow these two offences to be distinguished from one another and only confidence fraud
counted in the survey estimates. Consumer detriment falls outside the scope of the CSEW.

Such coding rules and follow up questions in the victimisation module need to be developed. A starting point would be to use the Action Fraud approach to establishing if the incident was a confidence fraud. [Confidence] fraud is defined as paying for a product or service which has not been delivered, is of poor quality, fake or counterfeit or turns out to be stolen. Other indicators of confidence fraud include the company or website no longer existing.

Possible check questions, which would be asked in the victimisation module could include:

- Did you buy/ get what you thought you were buying/ getting?
- Did you try to contact the seller to try to sort out the problem?
- Could you get in touch with them to put things right / to redress the situation?
- Is the seller/ business still trading?
- When you bought it did you think it was too good to be true?
- Have you complained/ raised the problem with the auction sire and asked them to arbitrate?
- If so, what was the response?
- Who do you think you should report it to/why did you not report it?
- Do you think that this is a crime?
- Did you report this to trading standards? Consumer Advice Line?

These questions require further development.
5 Recommendations for further testing

This chapter sets out recommendations for the wording and placement of new questions and for further testing and development work.

5.1 Further cognitive testing

Further testing of the revised and new screener and victimisation module questions is proposed to assess whether revised and or new questions are being consistently understood as intended. Figure 5.1 lists the questions that should be tested. Ideally this testing would take place prior to any larger-scale field testing. However, if this is not possible then cognitive interviewing could take place in parallel with field testing. In this scenario the cognitive data could be triangulated with the quality data, described in section 5.3, to assess question performance. This strategy is risky in the sense that new/modified questions would not have been cognitively tested prior to field testing. If the cognitive testing identified ‘serious problems’ then there would be little opportunity to revise the questions and field test them again.

<table>
<thead>
<tr>
<th>VIRUS</th>
<th>Test revised wording to assess whether Q is being understood as intended, consistently</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCINTRO</td>
<td>Test introduction &amp; show card to new screener Qs on fraud and cybercrime to assess understanding &amp; impact on answers to new screener Qs</td>
</tr>
<tr>
<td>New check Qs</td>
<td>Wording of new check Qs, establishing whether theft of personal data was linked to non-confidence fraud requires testing to establish if being understood as intended</td>
</tr>
<tr>
<td>Possible new Q on harassment</td>
<td>Test wording of new Q to establish whether being understood as intended</td>
</tr>
<tr>
<td>New victim form incident checklist Qs</td>
<td>Test wording of new incident checklist questions relating to fraud and cyber crime</td>
</tr>
<tr>
<td>Number of incidents of NONCON</td>
<td>Test whether instruction at NNONCON on what to count as an incident is being understood as intended</td>
</tr>
</tbody>
</table>

It is recommended that at least one further round of cognitive testing is undertaken, involving 15 interviews. All participants should be victims of non-confidence fraud, theft or personal data and or interference with internet of computer access.

5.2 Large scale field testing

A large-scale field test should be undertaken to assess the impact of the new screening questions and modifications to the victimisation module on the CSEW's:

- response rates;
• interview length; and
• data quality.

To assess each of these the field test needs to be of a sufficient size to ensure that there is adequate statistical power to make comparisons between estimates. In making this judgement the following factors need to be considered.

• The size of the change in the survey estimate one is concerned with detecting; for example a two percentage point change or a five percentage point change;

• The level of confidence one wishes to have that any change is 'real', for example 80 per cent confidence or 95 per cent confidence;

• The size of the population groups being compared – for example, is it general population estimates or estimates for sub-groups that are of interest; for example are the populations being compared in the 1000s or in the hundreds.

• The availability of time and money. Large-scale field testing can be expensive and take time. The Crime Survey is carried out face-to-face so field costs will be on the expensive side and this may limit the size of any field test.

Figure 5.2 shows the size of sample needed for both the control and treatment group to provide sufficient statistical power to detect a two and five percentage point difference in survey estimates. In these examples an existing CSEW sample estimate of 50% has been compared with a sample estimate derived from the questionnaire that includes the new screener questions. This produces a more conservative standard error around the sample size estimate than would be the case with an estimate of say 60% or 40% and as such a larger sample size is required. For example, to detect a 5 percentage point difference, with 95% confidence on an existing survey estimate of 60% sample sizes of 1,471 are required for each sample being compared. In comparison sample sizes of 1,565 are needed for each sample if the existing estimate being compared is 10%.
5.2.1 Assessing the impact of change on the time series

Making changes to an existing, long-established survey brings with it risks that the changes may affect the survey estimates. Any changes may be an artefact of revisions to the questionnaire rather than a measure of ‘actual’ change. There are two options. The first would be to attempt to assess the impact of the proposed changes to the CSEW screener and victimisation modules on measures of change over time in victimisation rates for existing incidents. This would involve the new questioning approach being run in parallel with the current approach over a period of one year or more. In parallel would involve selecting an additional sample, who would receive the new questions. The existing CSEW sample size would remain unchanged so as not to affect cell sizes for existing analyses. The second would be to accept that there might be some effect but not attempt to measure it. The measurement of change may be subject to error and it may not be possible to do so confidently and cost-efficiently.

5.2.2 Assessing data quality

There are several metrics that could be used to assess data quality of the new questions and these are summarised in Figure 5.3.

---

Figure 5:2 Illustration of effective sample sizes needed to detect differences in survey estimates

<table>
<thead>
<tr>
<th>% point difference in estimates&lt;sup&gt;8&lt;/sup&gt;</th>
<th>Level of statistical confidence&lt;sup&gt;9&lt;/sup&gt;</th>
<th>Effective sample size (for each sample for example, control and treatment group)&lt;sup&gt;10&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>80%</td>
<td>3,841</td>
</tr>
<tr>
<td>2</td>
<td>95%</td>
<td>6,358</td>
</tr>
<tr>
<td>5</td>
<td>80%</td>
<td>686</td>
</tr>
<tr>
<td>5</td>
<td>95%</td>
<td>1,135</td>
</tr>
</tbody>
</table>

---

<sup>8</sup> Assumes P1 is 10%.

<sup>9</sup> Using a two-sided test.

<sup>10</sup> Value of α (type 1 error rate) is 0.05.
## Figure 5:3 Proposed data quality measures

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage of fraud &amp; cybercrime by new screening Qs</td>
<td>Do the new screening questions capture all types of fraud and interference with internet and computer access?</td>
<td>Include existing questions that ask about experience of cybercrime (EEXPINT) and Mass Marketing Fraud (MMFRD2) in the past 12 months. These items should be asked in a separate module, later in the interview. The responses to the new screeners and existing Qs should be compared. If the screening questions are answered no then one would expect that participants would not have experienced anything at EEXPINT or MMFRD2 indicate that they have experienced cybercrime or mass marketing fraud. The existing Qs indicate the participant has been victimised then an open follow up Q should ask ‘You mentioned that you experienced (answer(s) from EEXPINT or MMFRD2). Why didn’t you mention this earlier in the interview, when I asked [new screener Q]?</td>
</tr>
<tr>
<td>Validity of the new screening questions</td>
<td>If a participant answers ‘yes’ does the victim form end up being coded to the same type of incident as the screening Q indicated?</td>
<td>Comparison of the screening question response with the Home Office code assigned to the corresponding victim form.</td>
</tr>
<tr>
<td>Completeness of the victim form information</td>
<td>Can incidents be coded using the HO coding rules? What is the rate of non-coding/ coding to a high level category?</td>
<td>Examination of the victim codes assigned to the new screening question incidents.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Measure</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Accuracy of number of incidents</td>
<td>Inclusion of check questions to assess the validity and consistency with which the question is being interpreted.</td>
<td>Respondent debriefing questions could be asked to assess accuracy of initial response to number of incidents question. The question would check how the participant answered the question. Specifically, for non-confidence fraud the respondent debriefing question would check whether the answer given represents the number of times this type of incident has occurred or how many times within in each incident the participant’s information was used.</td>
</tr>
<tr>
<td>Item non-response</td>
<td>Assess levels of item non-response to new screening Qs, including the SERIES Qs and to victim form questions</td>
<td>Look at levels of missing data (don’t knows and refusals by question. Are there any patterns by type of crime or by how recently the crime took place?</td>
</tr>
<tr>
<td>Double counting</td>
<td>Have the proposed strategies for dealing with possible double counting been successful?</td>
<td>Is there evidence of double counting – more than one new screener Q being answered (yes), two or more victim forms being opened but transpires only one was needed because only one incident occurred? Which screener Qs are affected for example, CON and NONCON? NONCON &amp; CMACT?</td>
</tr>
</tbody>
</table>
5.2.3 Respondent debriefing questions

Respondent debriefing questions can be included, as part of the pilot questionnaire, to check that participants are interpreting survey questions as intended and or that they applied the survey rules as intended (for example, excluding internet enabled devices used for business).

However, it will be important to prioritise the survey questions to be followed up, as this will add to the length of the interview and potentially inflate the estimate of interview length. A possible list of respondent debriefing questions is provided in Figure 5.4.

| Sensitivity | In self-completion module include a couple of questions to assess social desirability bias. For example, Earlier I asked you about whether you had been tricked or deceived. When you answered this question were there any incidents that you choose not to include? YesNo Why was that? Precoded list including Felt too embarrassed or ashamed |
| Personal crimes | Check if were self-employed at the time the incident occurred/became aware of it. If yes, check if participants included any fraud, theft of personal data or interference with internet or computer access against their business |
| Actual vs attempts | Check if participants reporting actual confidence fraud & theft of personal data or including attempts |
| Location | Check that participants answer was place where living when became aware of incident. Ask if living in England and Wales when incident actually occurred. Assess extent of missing data to both questions |
| Date of incident | Check date provided is date incident occurred. Possibly also ask date when incident actually took place to access (a) extent of time lag between occurrence and becoming aware, and (b) extent of missing data when asked for date occurred. |
| CON | Check confidence frauds involving telephone contact are being included |
| Number of incidents of NONCON | Check on how participants came up with their answer (see Figure 5.3, Accuracy of number of incidents) |

5.3 Developing rules

The current CSEW includes rules about the:

- prioritisation of incidents to follow up in the victimisation module; and

- number of incidents to be followed up, i.e. the number of incidents to follow up in the victimisation module.

The inclusion of additional crime incidents – up to five if online harassment is included as well as confidence and non-confidence fraud, theft of personal data and interference with internet and computer access – raises questions about what selection priority
these offences should be given and whether the current cap of five incidents to be followed up in the victimisation module is sufficient. The field test could provide useful data on which to base such rules. However some rules will be required for the field test itself and these should be considered.

5.4 Offence coding

The process of coding incidents of fraud, theft of personal data and interference with internet and computer access will need to be developed ahead of the large scale field test. It is envisaged that the new incidents would be coded using the latest Home Office counting rules and the current coding manual would require revision ahead of the field test. A soft launch of the large scale field test would allow the coding and editing program and manual to be tested and refined.

The current CAPI coding and editing program will need to be revised to incorporate the new incidents/ proposed new victimisation module.

Guidance for coders should be developed and refined in light of experience gained for the large scale field test.

The coding process should be evaluated as part of the field test in terms of whether the new victim form provides sufficient information to allow coding, whether the coding guidance is clear enough that coders can assign a code and the accuracy of codes assigned. Revisions should be made to the manual and the program based on findings from the field test.

5.5 Development time

The CSEW questionnaire is fairly complex and the offence coding and derivation of the volume of incidents estimates is complex. Making any form of change will require careful and thorough testing. Such testing could be undertaken with dummy data ahead of any field testing, to ensure that any major problems are dealt with.

This project was concerned with developing new screener questions. Further development work has been identified. However the recommendations from this project and any future development work need to be translated into CAPI programming script and this should be tested to ensure the program is working as intended. The scale of changes required to the current program is considerable and will take some time to implement. It is recommended that an estimate of the time required to produce a new CAPI program based on the recommendations contained in this report is obtained. This information should be used to plan the timing of the proposed large scale field test.

This project has made significant progress in developing a strategy for including new screener questions on fraud and cybercrime. Findings from small-scale, qualitative testing of this approach are promising and this study has made some clear recommendations on question wording. This study has also made a number of recommendations about further testing – both small scale cognitive testing, and larger-scale quantitative testing. The translation of these recommendations into a working
CAPI programme and coding manual should not be underestimated, however and there is still some way to go before the CSEW will be able to report on incidents of fraud and cybercrime in the same way as other offences.
References


Hache, A. C. and Ryder, N. (2011) ‘Tis the season to (be jolly?) wise-up to online fraudsters. Criminal on the Web lurking to scam shoppers this Christmas: a critical analysis of the United Kingdom’s legislative provisions and policies to tackle online fraud’, *Information and Communications Technology Law, (20) 1*, pp 35–56.


**Ofcom Media Survey** (2013), Ofcom


*Scottish Crime and Justice Survey* 2012-2013. Questionnaire and user notes. Scottish Government.


Whitty, M., and Buchanan, T. (2012). *The psychology of the online dating romance scam*, University of Leicester: UK