Appendix A. Findings from the desk review

The aims of the desk review were to:

- understand how members of the public, including victims, describe and understand fraud and cybercrime; and
- evaluate the range of methodologies and questions used in previous studies to measure the prevalence of victimisation from fraud and cybercrime.

To meet these aims an evidence review was carried out, questions asked on surveys of the general population were identified and reviewed, and the expertise of this study’s reference group was drawn upon. This Annex presents findings from the desk review.

A1 Scope of crimes considered by the review

The scope of crimes considered as part of this review was shaped by the definitions of cyber-enabled and cyber-dependent crime used by the Serious and Organised Crime Strategy (Home Office, 2013: 5).

- Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other form of ICT\(^\text{11}\). These acts 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.

- Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT. For the purposes of the McGuire & Dowling review the following types of cyber-enabled crimes were 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).

The Strategy definition of cybercrime does not include online crimes against the person, such as online abuse and harassment. Stage one of this research considered online crimes against the person where these form a part of crimes already captured by the CSEW, for example using threatening behaviour. These are referred to as ‘online crimes’ in this annex.

\(^{11}\text{Information and Communications technology}\)
A1.1 Methods

Evidence review
Conducting the evidence review involved identifying and examining existing evidence reviews (McGuire & Dowling, 2013; Kerr et al, 2013; Button et al, 2009) and other literature on fraud, cyber and online crime (as listed in the references for this report). Evidence reviews were selected that had been carried out in the past five years, which were extensive in their coverage of the issues. The reviews were undertaken by recognised experts in the field, and/or worked for key stakeholder organisations, such as the Home Office or were peer reviewed by them. This enabled the research team to map the forms and features of offences falling within these categories.

Survey question review
Questions on fraud and cybercrime from the following national surveys were also reviewed to identify the range of questions and methodologies used to identify/explore these in recent years.

- Crime Survey for England and Wales (CSEW);
- Australian Personal Fraud Survey (APFS);
- Consumer Awareness Survey (CAS);
- Eurobarometer Survey on Cyber Security (ESCS);
- International Crime Victimisation Survey (ICVS);
- Ofcom Media Survey (OMS);
- Oxford Internet Institute Survey (OIS);
- Scottish Crime and Justice Survey (SCJS);
- US Federal Trade Commission Consumer Fraud Survey (US FTC-CFS); and
- US National Crime Victimisation Survey (US NCVS), including the Identity theft supplement questionnaire.

These surveys were identified as ones containing questions that sought to identify victims of fraud and cybercrime, which are asked of the general population (as opposed to businesses or other specific sub groups) and which used a structured questionnaire as part of a face-to-face or telephone interview. In addition, the research team also reviewed the reporting questions asked of the general public when they report an incident to Action Fraud.

Reference group
A reference group was set up consisting of a number of experts in the field of fraud, cyber and other online crime. Following the desk-review a half-day workshop was held

---

12 A similar survey is also carried out in The Netherlands but is only available in Dutch and so was not included in this review. See [http://www.cbs.nl/NR/rdonlyres/F117D870-C5F7-42F2-A7B8-B3D6A6F4F02F/0/2014veiligheidsmonitor2013vragenlijstpub.pdf](http://www.cbs.nl/NR/rdonlyres/F117D870-C5F7-42F2-A7B8-B3D6A6F4F02F/0/2014veiligheidsmonitor2013vragenlijstpub.pdf)
with the reference group. The review findings were presented and issues discussed in order to facilitate the development of the new questions.

A2 Considerations for the screener questions

Fraud

One of the primary challenges in measuring fraud prevalence is the wide range of ways in which fraud offences are committed; another is the lack of agreed definitions for different forms of fraud (Button et al, 2009). In this context, measuring fraud in household surveys, including the CSEW, has tended to focus on asking participants whether they have been a victim of fraud perpetrated in a range of different ways. For example, in the CSEW Mass-Marketing Module, participants are asked about ten different types of mass-marketing communication they may have received.13

This approach presents a particular challenge to measuring prevalence and volume of fraud victimisation over time. Fraudsters are constantly changing and adapting methods of perpetration in response to victims’ awareness and agencies’ detection and prevention strategies, which means that any list of fraud methods can become quickly outdated (Harvey et al, 2014). In the APFS (part of the Multi-Purpose Household Survey), conducted in 2007, 2010-11, and to be conducted again from July 2014, categories have had to be updated each time. In the 2010-11 results, it was noted:

‘Some of the types of selected scams included in 2010-11 differ from those in 2007 and it is not recommended to directly compare categories. While the categories of ‘lotteries’, ‘pyramid schemes’, and ‘chain letters’ are similar, the question wording changed from the wording used in 2007’ (Australian Bureau of Statistics, 2012).

As well as the examples quoted above, a number of other changes were reported between the first two times the survey was conducted. For the upcoming version of the survey, further categorisation changes have been made:

‘The scam categories have also been expanded to reflect current common scam experiences reported anecdotally and in other smaller Australian surveys. The scam types included will be: a lottery scam; an information request scam; a pyramid scheme; a relationship scam; an upfront payment scam; a financial advice scam; a computer support scam; a working from home scam; an online trading or auction site scam; other type of scam.’14

Further, unlike in surveys designed specifically to measure fraud only (for example, the APFS and the US FTC-CFS), the CSEW measures all forms of crime victimisation. The CSEW includes 25 screening questions15 that identify potential victims of household and personal crimes in the past 12 months. Presenting participants with a list of fraud methods, or inserting a large number of questions about the different ways of committing fraud within the screening questions has one notable draw back. The ways in which frauds are committed are ever-changing and questions could quickly become out-of-date and require frequent updating. Such amendments to the screener questions would risk affecting the comparability of survey estimates. Amendments might affect the way in which incidents are reported making it difficult to disentangle real change.

---

13 MMFRD1A-MMFRD1N
14 Personal communication between Shannon Harvey, NatCen Social Research, and Lisette Aarons, Assistant Director, National Centre for Crime and Justice Statistics, Australian Bureau of Statistics
from changes resulting from amendments to question wording. The CSEW screener questions have remained unchanged since the survey started.

Through the mapping of different ways in which fraud is committed and categorisation of these different forms, presented in section 2.1.1, the research team suggested ways to delineate frauds carried out in different ways to develop a small number of screener questions that could successfully identify victims of these crimes.

Cyber-enabled and online facilitated crimes other than fraud

While the categories of cyber-enabled and online facilitated crime other than fraud are potentially extremely broad, many of these crimes are not targeted at individual victims and are therefore not relevant to the CSEW, for example, online drug dealing. One type of cyber-enabled crime that is relevant to the CSEW is theft of personal information and data that are held digitally. In some cases such a theft may be a precursor to a fraud taking place, where stolen information is used as part of the deception or may occur as a result of the theft of a computer or smartphone.

Other crimes facilitated by the internet that do involve individual victims predominantly involve offences against the person, and are potentially covered by existing questions in the CSEW screening questions, for example questions about threats of violence. However, the context of the questionnaire as a whole, and the current wording of questions, means that it is unclear whether participants are including their experiences of internet facilitated crimes in their answers, although this seems unlikely. As the internet becomes increasingly interwoven in our lives, these questions may become increasingly unreliable for cyber-enabled and other online crimes, unless they are updated to specifically state whether or not participants are expected to include online incidents, or an alternative approach for identifying these offences is adopted.

Cyber-dependent crimes

Cyber-dependent crimes such as the spread of viruses and distributed denial of service attacks (DDoS) tend not to be directed at individual victims, although individuals may be victimised as a result. The primary challenge for measuring these forms of crime at the level of individual victims is that victims often will not know that they have been victimised in this way. In addition, the point at which an individual is technically counted as a victim may be unclear. One approach would be to follow the Home Office counting rules (Home Office, 2014), if the CSEW is to follow this classification.

A2.1 Categorising frauds, cyber and other online crimes

A2.1.1 Offline and cyber-enabled frauds

The research team mapped the different ways fraud is committed by reviewing existing evidence reviews (McGuire & Dowling, 2013; Kerr et al, 2013; Button et al, 2009), other literature on fraud (Fafinski & Minassion, 2009; Harvey et al, 2014), and questions on fraud contained in existing surveys (CSEW, APFS, CAS, SCJS, ESCS, ICVS, OMS, OIS, US FTC-CFS, and the US NCVS), identifying eight broad (yet potentially overlapping) categories of fraud, as shown in Figure 2.1, Chapter 2.

In developing the screener questions, experiences of fraud will need to be asked using a small number of questions. Figure 2.2 in Chapter 2 shows how the research team distilled the methods of fraud listed in Figure 2.1, focusing on the most intrinsic characteristics of the different ways of committing fraud: non-confidence and
confidence frauds. This provided a framework for how questions about fraud in the screener questions might be focused.

The SCJS is perhaps the most directly comparable survey to the CSEW, and currently has two questions in its screener questionnaire on fraud that covers non-confidence fraud.

- And <apart from anything you have already mentioned> since <INSERT DATE>, has anyone used any of your credit or bank cards, or your card details, to buy or pay for things or withdraw cash from your account without your permission? Yes, No, Don’t Know (DK), Refused (REF)\(^16\)

- And <apart from anything you have already mentioned> in that time, has anyone pretended to be you or used your personal details such as your name, address, date of birth or National Insurance number without your permission to do things such as obtain credit, open a bank account, apply for a mobile phone contract or state benefits or for official documents such as a driving licence or passport. Yes, No, DK, REF\(^17\)

Other surveys internationally are more comprehensive in asking about fraud, but are less directly comparable to the CSEW, since they are fraud surveys in their own right and have greater scope to ask detailed questions.

Table A.1 presents a range of examples of relevant questions identified from the review of survey questions against each of the fraud categories set out in Figure 2.2, chapter 2.

\(^{16}\) Victim Form Screener - CARDVIC2
\(^{17}\) Victim Form Screener - IDTHEF2
### Table A.1 Survey questions by fraud type

<table>
<thead>
<tr>
<th>Fraud category</th>
<th>Sub-category</th>
<th>Question</th>
<th>Question and Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-confidence fraud</td>
<td>Information theft</td>
<td>ASK IF SOMETHING STOLEN (QSTO, CODE 1). What was taken? ADD IF NECESSARY: Even if the property was recovered later. DO NOT PROMPT, PROBE: What else? MULTICODE OK. 1 Car / van 2 Motorcycle / motorised scooter / moped 3 Vehicle parts / accessories / car stereo 4 Briefcase / handbag / shopping bag 5 Purse / wallet 6 Cash (not from meter) 7 Cheque book 8 Credit card / switch card / debit card / store card / cheque card 9 Cash removed from bank account / charges added to credit card 10 Passport / driving licence / official ID card 11 Personal details – for example, from bank or loan statement, mobile phone bill, driving licence 12 Personal details – for example, from internet / computer / online 13 Mobile phone / Blackberry / PDA 14 MP3 player / portable music player 15 Jewellery 16 Clothes 17 Bicycle 18 Garden furniture, ornaments, plants or equipment (eg lawnmowers, spades, wheelbarrow) 19 TV / DVD / Video recorder 20 Other (SPECIFY) DK REF</td>
<td>QSTW in SCJS 2012-13 (Victim Form)</td>
</tr>
<tr>
<td>Fraudulent use of information</td>
<td></td>
<td>In the last 12 months, [have/has] [you/name of Random Person] been aware of anyone using [your/his/her] credit cards or [your/his/her] card details to make purchases or withdraw cash without [your/his/her] permission? 1. Yes 5. No</td>
<td>IDTQ2, IDTQ4, IDTQ14 and IDTQ27, in APFS 2010-11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I would like to ask about [this occasion / the most recent occasion] (that [your/name of Random Person’s] credit cards or card details were used to make purchases or withdraw cash without [your/his/her] permission). How were [your/his/her] credit cards or card details obtained? Interviewer: If 'telephone', ask &quot;Was it a mobile phone?&quot; 1. In person (i.e. purse stolen, skimming, etc.) 2. Telephone - Landline (including fax) 3. Mobile phone (including SMS) 4. Email/Internet 5. Post 6. Other</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the last 12 months, [have/has] [you/name of Random Person] been aware of anyone using [your/his/her] personal details, such as [your/his/her] drivers licence or Tax File Number, in stolen, fraudulent or forged documents without [your/his/her] permission? 1. Yes 5. No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the last 12 months, [have/has] [you/name of Random Person] been aware of anyone using [your/his/her] identity in any other way without [your/his/her] permission, such as conducting business, opening accounts or taking out loans illegally in [your/his/her] name? Interviewer: Ctrl K may be used here if necessary 1. Yes 5. No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Since ______<strong>, 20</strong> has someone used or attempted to use your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else? YES NO</td>
<td>2a, 3 and 4 in US NCVS – 2012 Identity Theft Supplement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Since ______<strong>, 20</strong> has someone used or attempted to use your personal information for some other reason? YES NO</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Since ______<strong>, 20</strong> has someone used or attempted to use your existing credit cards without your permission? Please do not include debit cards YES NO</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Since ______<strong>, 20</strong> has someone used or attempted to use your existing credit cards without your permission? Please do not include debit cards YES NO</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The table provides a summary of survey questions designed to collect data on fraud and cybercrime, specifically focusing on non-confidence fraud and fraudulent use of information. Each question is designed to capture specific types of fraud, including information theft and identity theft, with multiple choice options to address various scenarios and methods of fraud. The questions are structured to ensure that respondents can accurately report incidents of theft, misuse of personal information, and unauthorized use of their credit cards, among other forms of fraud. The table highlights the importance of including questions that are sensitive to individual privacy and the potential for misuse of personal data, reflecting the evolving nature of fraud and cybercrime in the digital age.
<table>
<thead>
<tr>
<th>Confidence fraud</th>
<th>Advance fee frauds</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; giving your information to the police when they were charged with a crime or traffic violation, or something else?</strong></td>
<td>YES NO</td>
</tr>
</tbody>
</table>

| **In the last 12 months [have/has] [you/(name of Random Person)] received any fake notifications of having won a lottery or prize for a draw that [you/he/she] didn't enter? Interviewer: If 'Readers Digest', ask "Were there any others?".** | YES 5. No |
| Did the notification require [you/him/her] to pay a fee, or provide [your/his/her] bank account details in order to collect [your/his/her] winnings? | YES 5. No |
| [How many of these notifications [have/has] [you/he/she] responded to / Did [you/he/she] respond to this notification] by providing money, or [your/his/her] personal details, or asking for more information? | 0 .. 999 |

| **In the last 12 months [have/has] [you/(name of Random Person)] received any chain letters involving requests for money?** | YES 5. No |
| I would like to ask a few questions about [this occasion/the most recent occasion] when [you/name of Random Person] responded (to a chain letter). Did [your/his/her] response include providing money? | YES 5. No |

| **In the last 12 months [have/has] [you/(name of Random Person)] received any fake requests asking [you/him/her] to have money transferred into [your/his/her] account in return for a commission or fee?** | YES 5. No |

<table>
<thead>
<tr>
<th><strong>Fraudulent sales</strong></th>
<th><strong>Fraudulent relationships</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In the last 12 months [have/has] [you/(name of Random Person)] received any invitations into pyramid selling schemes?</strong></td>
<td>YES 5. No</td>
</tr>
<tr>
<td>Did any of the schemes rely on recruiting new members to make money?</td>
<td>YES 5. No</td>
</tr>
<tr>
<td>I would like to ask a few questions about [this occasion/the most recent occasion] when [you/name of Random Person] responded (to an invitation into a pyramid scheme). Did [your/his/her] response include providing money?</td>
<td>YES 5. No</td>
</tr>
</tbody>
</table>

| **In the last 12 months [have/has] [you/(name of Random Person)] received any fake offers to supply [you/him/her] with financial or investment advice?** | YES 5. No |
| **Now changing the subject a little. Last year (in 1999), were you the victim of a consumer fraud? In other words, has someone when selling something to you or delivering a service cheated you in terms of quantity or quality of the goods/service?** | 1) yes ( 2 no (3) don't know |

| **I'd now like to ask some questions about different types of communication you may have received from strangers that might have involved a request for money. Looking at this card, have you personally EVER received any emails, texts, letters or phone calls from an individual or a company that you've never heard of before about any of the following? CODE ALL THAT APPLY. INTERVIEWER: THIS INCLUDES INTERNET POPUPS.** | MMFRD1A-MMFRD1N in CSEW Mass- Marketing Module |
| A. A big win in a lottery, prize draw, sweepstake or competition that you haven’t entered | |
| B. The chance to make an investment with a guaranteed high return (for example, shares, art, fine wine, etc.) | |
| C. Someone who invites you to get to know them with a view to a possible friendship or relationship (this may be via a website) | |
| D. Help in moving large sums of money from abroad | |
| E. Help in releasing an | |
6. F. An urgent request to help someone get out of some sort of financial trouble/7. G. A job offer, a franchise offer or other business opportunity/8. H. A loan on very attractive terms/9. I. Adopting or buying a pet/10. J. Some other type of similar request/11. SPONTANEOUS ONLY: Never read or listen to messages like these/12. K. None of these [Please describe what the similar type of request was about.]
In addition, the CSEW also includes a question asking participants whether they have personally experienced loss of money while using the internet:\(^{18}\):

- In the last 12 months, have you personally experienced any of the things mentioned on this card while using the internet? CODE ALL THAT APPLY
  1. A computer virus (or other computer infection)
  2. Loss of money through responding to communication (for example, fraudulent e-mails or online messages)
  3. Unauthorised access to/use of personal data (for example, banking information or social media/e-mail account)
  4. Online harassment, through repeated and/or related online contact that has caused fear, alarm or distress
  5. None of these

This question also encompasses other forms of online crime which are discussed in the next section.

A2.1.2 Other forms of cyber and online crime with individual victims

Other than fraud, our mapping of the evidence identified further forms of online crime which potentially or always include individual victims (rather than organisational victims). These fall into three broad categories:

- Offences against the person (for example, online stalking, harassment and sexual offences) – these offences include both internet-facilitated crimes and crimes wholly committed online (for example, harassment of an individual through hacking attacks).
- Interference with internet and computer access – these are cyber-dependent crimes, such as spreading viruses or malicious software and creating botnets, hacking, or DDoS attacks. These include 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.
- Theft of personal information or data held digitally, where no fraud has (yet) taken place.

Online offences against the person

As described in section A2.1.2 internet facilitated crime involving individual victims are generally offences against the person. The CSEW currently includes two screening questions that could encompass online offences against the person:\(^{19}\):

- And [apart from anything you have already mentioned], in that time, has anyone THREATENED to damage things of yours or THREATENED to use force or violence on you in any way that actually frightened you? Yes, No
- DURING THE LAST 12 MONTHS, HAVE YOU BEEN SEXUALLY INTERFERED WITH, ASSAULTED OR ATTACKED, EITHER BY SOMEONE YOU KNEW OR BY A STRANGER? Yes, No

---

\(^{18}\) EEXPINTA-H

\(^{19}\) THREVIOL and SEXATTAK
However it is unclear whether CSEW participants are including their experiences of online crimes in their answers to these questions. In addition, a view among the reference group was that the second question above was very contact focused and so would need a considerable amount of re-wording to include an online element.

The screener section of the SCJS survey asks the same question as the first CSEW question listed above, about ‘whether anyone has threatened to damage things of yours or threatened to use force or violence on you’\(^{20}\). Those who reported that a threat was made are asked whether this was made by some other means other than in person, to capture the distinction between verbal and written cyber and online offences (both offline and online). This is discussed further in A4 of this appendix.

**Interference with internet and computer access**

As described in section A2 cyber-dependent crimes such as the spread of viruses tend not to be directed at individual victims, although individuals can be victimised as a result. The CSEW currently includes one screener question that could encompass **interference with internet and computer access**\(^{21}\):

- And [apart from anything you have already mentioned], in that time has anything else of yours been DELIBERATELY DAMAGED or tampered with by vandals or people out to steal? Yes, No

Once again, the current wording of the question means that it is unclear whether participants are making the connection to experiences they may have had online across varying devices in their response, however this unlikely.

**Theft of personal information or data**

Theft of personal information or data may occur in a range of ways, depending on the form in which the information or data are held. Existing CSEW screener questions, which ask about theft\(^{22}\), may already pick up some theft of data although this seems unlikely and a specific screener question may be required. As noted in Table A.1 of this report question QSRW in the SCJS asks participants who report that they have had something stolen, what it was. The answer categories include code 12 – Personal details, for example, from internet/computer/online. In addition, the Ofcom Media Survey (OMS) also has a relevant question and code for this for participants who use the internet at home or elsewhere\(^{23}\):

- Which, if any, of the following have you personally experienced in the last 12 months?
  - Your credit card details being stolen as a result of buying something online.

**A2.2 Reference group discussion points for the screener questions**

There was general consensus among the reference group that the CSEW should include additional screening questions to capture fraud, cyber and other online crime. Different options were discussed about how to capture fraud, which are summarised below.

\(^{20}\) THREVIOL  
\(^{21}\) DELIBDAM  
\(^{22}\) For example, YRHOSTOL, PERSTHEF or OTHTHEF  
\(^{23}\) QING code 6
Include one screening question to identify fraud of any kind.

Include two screening questions to identify fraud based on the confidence/non-confidence conceptual framework presented in Chapter 2, Figure 2.2 (this was the option taken forward).

Include five screening questions to identify different types of confidence/non-confidence frauds based on the conceptual framework shown in Figure 2.1, Chapter 2.

If the first approach were to be adopted the sub categorisation of fraud could be captured in the Victimisation Module and reference group members suggested how Figure 2.2 could be amended to cover the three broad categories (theft of personal information, paying a fee and not receiving the expected goods/services, and relationship/be-friending fraud). This is further explored in section A4.4.

Other forms of cyber and online crime could be identified by the inclusion of new questions which follow or are based on the wording of existing screener questions (THREVIOL, SEXATTAK and XDELIBDAM). This would help to limit the impact on the time series data for existing screener questions, and help to ensure that more traditional offline crimes, which are currently identified by the screener questions are not subsequently lost as a result of including references to cyber and online crime. However this approach might increase interview length and participant burden. In addition, it was suggested that setting the context at the beginning of the CSEW by stipulating how the survey seeks to identify incidents of cyber-dependent, cyber-enabled offences, online and internet facilitated offences (using terms participants understand) could also help to address this issue.

**A3 Measuring volume for fraud, cyber and online crime**

**A3.1 Definitions – incidents, series and victimisation**

**A3.1.1 Fraud**

Incidents and series

While some frauds will clearly involve a single incident, confidence frauds in particular can involve numerous interactions with the fraudster(s), and a number of transactions over time. Further, victims may not be able to identify whether a series of transactions are part of the same fraud or are different frauds.

For example, NatCen’s research with victims of fraud found that victims often do not know how many times they are contacted or whether they are being contacted by the same or different people or companies in the completion of a fraud. They also may be contacted via different modes including online and by telephone (Kerr et al, 2013; Harvey et al, 2014). This presents particular challenges for the CSEW series questions, as it is not clear whether these victims would be able to answer whether the separate money transfers that they made were, “the same thing was done under the same circumstances and probably by the same people?” (CSEW Series). While they may not know if it was done, even “probably”, by the same people, there may also be a question as to whether it was done “under the same circumstances”. For example, in investment...
Frauds perpetrated over an extended period, the fraud may evolve from what was initially making a fraudulent investment to then being closer to advance fee fraud (such as being asked to put up a bond to guarantee the sale of their “shares”).

In non-confidence frauds, there is also a need to ensure an incident is clearly defined to make clear to the victim whether this relates to the number of transactions or individual uses of their personal information, or whether a number of transactions made in relation to a single theft would be a single incident or a series.

For example, this is dealt with in the APFS by seeking to identify "episodes", rather than individual transactions:

The survey sought to establish the number of ‘episodes’ of credit or bank card fraud or identity theft, that is, the number of times the respondent had their personal details stolen. The survey has not collected the number of individual transactions or cash withdrawals that occurred in each ‘episode’ before the breach was detected. For example, if a respondent's credit or bank card was stolen and was used to make five transactions before the card was cancelled, only the one episode of the card being stolen and used fraudulently was counted. (ABS, 2012)

Victimisation

In the Mass-Marketing Module of the current CSEW, a series of questions are asked about whether the respondent has received potentially fraudulent communications, followed by questions about whether they have responded to these and what loss they have experienced as a result. This is similar to other surveys conducted specifically on fraud, and allows a distinction to be made between fraud and attempted fraud.

However, this distinction applies specifically to what we have categorised as confidence frauds (see Chapter 2), and not to non-confidence frauds. As noted in the explanatory notes to the APFS:

The distinction between exposure and victimisation does not apply to identity theft or credit or bank card fraud - in these cases if a person simply became aware that these types of fraud had occurred; they were considered to be a victim, as they were not required to be exposed to a scam for victimisation to occur (ABS, 2012).

This distinction between the two forms of fraud is reflected in the wording of the screener questions in the SCJS (see section A2.1.1). The question on plastic card fraud (CARDVIC2) is worded to ensure that only victimisation is captured, while the question on identity theft (IDTHEF2) does not make this distinction. Both these questions (CARDVIC2 and IDTHEFT) only capture fraud victimisation and do not capture attempted confidence frauds.

A3.1.2 Other cyber and online crimes

For online offences against the person, the definition of victimisation in the context of the CSEW needs to be clearly set out. In many cases, online bullying and other harmful behaviour online may not constitute a criminal offence, and therefore needs to be carefully worded to ensure that crime victimisation is being accurately captured.

Further, victims of online harassment have reported experiences of receiving hundreds of messages in a short period, some of which may contain threats of violence, and/or may involve the same person harassing them. Survey questions need to be clear as to how participants are expected to count the number of incidents, or there is a risk that many victims of these experiences will simply answer ‘too many to remember’. This would affect the accuracy of the CSEW findings in terms of measuring the overall
volume and prevalence of this type of offence. Further, if they do know the actual number of messages they received, requiring a response between 1 and 96 may be insufficient. For example Caroline Criado Perex, the British journalist and feminist activist\textsuperscript{24} was reported to have received 50 threats an hour on twitter, after her involvement in the high profile campaign to gain better representation of women on banknotes\textsuperscript{25}. This presents a further challenge to measure crime in terms of volume as the inclusion of any new methods of crime could have a large impact on crime trends.

For **interference with internet or computer use**, once again the definition of victimisation needs to be clearly set out, and a crime classified in line with the definitions used in the Home Office Counting Rules (Home Office, 2014). Victims may not always be aware that a cyber-dependent crime such as being a victim of malware has taken place. Examples of malware include when computers are transformed into ‘robots’ or bots that can be controlled externally to send spam or conduct other criminal activities, or ‘ransomware’ which infects computer systems and restricts access while demanding a payment from the owner. Further, if they are aware it may be unclear how they are expected to count the number of incidents in relation to such an offence, as the malware may have facilitated many different frauds to take place online.

**A3.2 Application of the current series questions**

**A3.2.1 Fraud**

Currently in the CSEW, participants who say ‘yes’ to any of the screener questions are then asked the following question so that the volume of a range of offences can be estimated\textsuperscript{26}:

- How many times has this happened?

The same approach is taken on the SCJS, which includes screener questions on plastic card fraud and identity theft. However, it is not clear whether participants are providing the number of times that their personal details have been stolen or the number of times that their details have been used. The way the screener questions are worded implies that participants may be answering in terms of ‘how many times they have been used’ (see section A2.1.1, questions CARDVIC2 and IDTHEF2), and this is something that could be explored by the cognitive interviews at stage two.

Following the volume question asked in the screener, the CSEW establishes whether multiple incidents are related, i.e. incidents are ‘probably’ committed by the same person over a period of time. In their current form, these series questions may be sufficient to distinguish between the number of transactions or the number of thefts, however this is unlikely\textsuperscript{27}:

- You mentioned [NUMBER] incidents of [CRIME]. Were any of these very similar incidents, where the same thing was done under the same circumstances and probably by the same people?

\textsuperscript{24}http://en.wikipedia.org/wiki/Caroline_Criado-Perez
\textsuperscript{25}Laura Smith-Spark "Calls for action as female journalists get bomb threats on Twitter", CNN, 2 August 2013 at http://en.wikipedia.org/wiki/Caroline_Criado-Perez
\textsuperscript{26}For example NMOTTHEF
\textsuperscript{27}For example SIMILAR_1
An alternative method, however, is to make this distinction clearer in the screener question itself. For example, in the Identity Theft Supplement to the US NCVS, participants are asked:

- Now we would like to know how many times you were a victim of identity theft in the past 12 months. An incident of identity theft occurs when your identity is stolen. A stolen credit card or debit card may be used multiple times but this should be considered a single incident. You said that someone, in the past year, that is since [date reference period provided at previous question]. Did this happen to you once or more than once?

Similarly, in the US FTC-CFS, participants are asked:

- How many times has this happened to you in the past year? If you made multiple payments in connection with the same transaction, please only count this as one incident. Record number of times ____ [range 1-7] DK/REF

As discussed above, the existing series questions are likely to present challenges for victims of confidence frauds who simply do not know whether the crimes they experienced were part of a series or not.

### A3.2.2 Other cyber and online crimes

Similarly as for confidence frauds, victims of online offences against the person may have difficulty answering the current series questions. Where participants have experienced online stalking or harassment, for example, they may be unable to identify whether it was the same or different people who harassed them. Victims report that offenders may set up multiple profiles on social media accounts, for example, and they are unable to identify who is behind them (Webster et al, 2012).

Participants may also be unable to identify whether it was the same or different people behind incidents of interference with internet or computer use. For example, if a participant believes that he or she has received a number of viruses, and has even identified what type of viruses they are, he or she may not know that viruses were perpetrated by the same individual or group.

### A3.3 Implications of victimisation in the past-12 months

#### A.3.3.1 Fraud

The CSEW uses a reference period of 12 months, so participants are asked to report on crimes they, or members of their household, have experienced in the past year. For both confidence and non-confidence frauds people are not always immediately aware that they have been a victim of fraud, and it sometimes only becomes apparent after a significant length of time. For example in (Harvey et al., 2014) some participants who had been a victim of investment fraud only became aware of this when they experienced official disruption and the fraud was shut down by the Financial Conduct Authority or the police.

An alternative method is to extend the reference period. For example, in the APFS 2010-11 participants were asked to recall incidents of identity theft that they became aware of in the last five years, due to the low prevalence rates the survey had been recording. It was noted:

---

28 Q6a  
29 For example Q13.2
'Due to the relatively low prevalence of identity theft, details have been collected about incidents of identity theft that participants became aware of in the last 5 years prior to interview in 2010-11, compared to the last 12 months prior to interview in 2007. 2010-11 data describing characteristics of victims of identity theft relates to incidents in the last 12 months only and is comparable to similar tables in the 2007 publication'. (ABS, 2012)

However, as the CSEW is conducted each year and the reference period for fraud needs to be consistent with the current approach used for existing crimes identified in the survey; this would not necessarily be desirable here.

A3.3.2 Other cyber and online crimes

Of course a lack of awareness that an incident has occurred or that there is a considerable time lag between the incident occurring and the participant becoming aware of it affects other cyber and online offences as well as fraud. For example, a perpetrator may be stalking a victim on the internet without their knowledge. Furthermore, malware can be used to take over an individual’s computer so it can be used to collect personal or credit card details (which can be sold or used); or to commit criminal acts, such as accessing pornographic sites, (Goucher, 2010). However, it may not always be immediately apparent to the victim that such offences have taken place.

A3.4 Reference group discussion points for the screener and series questions

Reference group members generally agreed that the CSEW should continue to ask about crimes in the last 12 months for fraud, cyber and online crime. However, the hidden nature of forms of fraud, cyber and other online crime will mean that some participants may be unknowing victims and therefore their incidence(s) of victimisation will not be reported in the survey. In addition, given the potential complex nature of such offences and the potential ‘hidden’ nature of the perpetrator(s) involved, questions around the series and timing of the incident may also be challenging. It will still be important to try and identify if more than one incident is part of a series or not, but some victims may simply not know the answer to this. Asking them to identify when they became aware of the incident and basing the reporting on this measure instead may be the only practical option.

A4 Including fraud, cyber and other online crime in the Victimisation Module

Participants, who report that they have experienced one or more incidents of any crime type in the screener questions, are then asked to complete a Victimisation Module for each of the incidents, up to a maximum of six. The incidents asked about are automatically selected if the respondent reports more than six, to prioritise rarer crimes. For the first three incidents the respondent completes a long Victimisation Module, and for the second three a shorter Victimisation Module.

One of the challenges discussed in Chapter 3 is on managing the impact of question changes on the time series data, and in this respect it would be desirable if the victimisation questions remained unchanged. However there are a number of considerations to be acknowledged in the questions applicability to fraud, cyber and
other online crime to ensure the data collected is meaningful and useful. These challenges were considered some possible options to address them identified.

A4.1 Considerations for the Victimisation Module

The Victimisation Module collects three vital pieces of information:

- when the incident(s) took place;
- what happened; and
- other contextual information.

Each is discussed below in terms of measuring victimisation of fraud, cyber and other online crime. The information required to identify and code fraud, cyber-dependent, cyber-enabled crimes and other online crime is likely to be similar and as such the issues discussed in this chapter apply to all of these unless explicitly stated otherwise.

A4.1.1 Date when incident / series of incidences occurred

The first question in the Victimisation Module asks participants for the date the incident occurred, and instructions are provided for the interviewer if the respondent is uncertain of the exact date:

- I now want to ask you about WHEN the incident(s) you have just mentioned happened during the last 12 months. I'd like to mark on the calendar the date of each incident.

INTERVIEWER: FOR EACH CRIME, MARK ON THE CALENDAR THE DATE WHEN IT OCCURRED. THIS ONLY NEEDS TO BE ESTIMATED TO THE NEAREST MONTH. IF THE RESPONDENT IS HAVING DIFFICULTY REMEMBERING THE EXACT MONTH YOU MAY FIND IT USEFUL TO MARK SOME OTHER LANDMARK DATES ON THE CALENDAR (FOR EXAMPLE, BIRTHDAYS, ANNIVERSARIES, ETC.) WHICH CAN BE USED FOR REFERENCE POINTS. EXAMPLES OF SUCH EVENTS OR PERIODS CAN BE FOUND ON THE FRONT PAGE OF THE CALENDAR.

If the incident is part of a series of incidents participants have the option of providing the quarter in which the (most recent) incident occurred.

As described in section A3.1.1 some frauds clearly involve a single incident, however confidence frauds in particular can be complex and involve numerous interactions with the fraudster(s), a number of transactions over time, and encompass different fraud methods. For example, romance frauds generally take place over a period of time and can involve a number of different components, some of which may not be offences. This can include both identity fraud and mass-marketing fraud alongside other online offences against the person. The fraudster creates a fictitious profile on a dating website. Alongside persuading the victim to send money to them over a period of time Whitty & Buchanan (2012) also note additional offences may also occur, for example the victim may be convinced to commit sexual acts in front of a web cam which is then used to blackmail them.

Asking victims of fraud(s), cyber and online crime to provide a date/a month/a quarter when the incident occurred may be challenging, unlike for example a theft from the person, and clarification may be required. One approach would be to ask participants to locate a specific reference point in the experience (if they are able), for example

---

30 DISPLAY at the beginning of the Victimisation Module
when they first became aware of the fraud, or when money was transferred. This could be accompanied by guidelines for interviewers that state what to do when there have been multiple transactions, for example such as using the date of the last one. An alternative approach would be to give participants the option of answering with an extended time period over which the offence occurred, however even this may be difficult for some people to recall.

For example, the US NCVS identity theft supplement seeks to identify when participants became aware that the fraud had taken place, and their perceptions of the length of time the offence had taken place before this.31:

- In what month did you first discover that someone had misused or attempted to misuse your personal information?
- How long had your personal information been misused before you discovered it?

These issues also apply to asking about incidents of interference with internet or computer use. Here the particular challenge is that victims are unlikely to be aware that the crime(s) has taken place unless a problem, such as a virus, is detected and the source identified.

A4.1.2 Description of the incident

As part of the victimisation questions, interviewers ask participants to provide a short description of the incident. Interviewers then complete an incident checklist to ensure that sufficient information is captured to allow the incident to be coded using the Home Office Coding Rules. This may involve asking the participant additional questions, where the detail has not been captured in the description. Some additional questions may need to be added to the checklist to ensure that sufficient details have been captured about the fraud, cyber or online crime. In relation to incidents of interference with internet or computer use the reference group suggested that some questions contained in the 2014-15 CSEW module on online security may need to be incorporated into the checklist to ensure relevant information is collected.

A4.1.3 Characteristics of the incident

Questions included in this section encompass where and when the incident took place, the reason for the incident having occurred, whether anything was stolen or damaged and, whether force or violence was used. Participants are also asked about whether the police were informed or not about the offence.

Circumstances of the incident

As noted by McGuire & Dowling (2013:6), cybercrime is global in nature and is not constrained by national boundaries. This also applies to other forms of online crime. The CSEW estimates the volume and prevalence of crimes that happened in England and Wales only so that resources can be targeted effectively. ICSEW participants are asked the following two questions to ascertain where the incident took place:

- Can I just check, did it happen in this area (within 15 minutes' walk of here)?
Yes, No

- Did it happen in England or Wales or did it happen somewhere else?
  1. England or Wales
  2. Elsewhere

If a respondent answers ‘Elsewhere’ at WHERHAPP, and it is the long version of the module, it will switch to the shorter version. This could have significant implications for fraud, cyber and online crime incidences. For example, the victim may have been living in England or Wales throughout the offence, but perceive the offence as happening ‘elsewhere’. One reason for this may be because the victim transferred money to an account located abroad, or spoke to someone on the phone in relation to the fraud who was perceived to be based abroad. If the victim answered ‘elsewhere’, details about the incident would be lost. A similar question was asked on the SCJS 2012-13, with an additional category of ‘on the internet/online’, alongside a follow-up question to clarify where the respondent was living when the incident was perceived as happening online:

- Did it happen somewhere else in Scotland, or did it happen outside Scotland?
  PROBE IF OUTSIDE OF SCOTLAND: Did it happen in England or Wales or somewhere else?
  1. Somewhere else in Scotland
  2. England or Wales (END VICTIM FORM)
  3. Somewhere else (END VICTIM FORM)
  4. On the internet / online

- [ASK IF INCIDENT HAPPENED ONLINE (QSCO, CODE 4)]
  And where were you living when this occurred? Were you living … READ OUT:
  1. At this address
  2. Somewhere else within 15 minutes of here
  3. Somewhere else in Scotland
  4. England or Wales (END VICTIM FORM)
  5. Somewhere else (END VICTIM FORM)

The SCJS only records details of incidents which happen within Scotland so that the data can be used to assist with resource planning. Therefore, for an incident occurring online to be included, the respondent must have been living in Scotland at the time of the incident. If an incident occurred outside of Scotland then the victim form questionnaire terminates and the questionnaire moves on to the next victim form (or the start of the next section of the main questionnaire if the respondent has not experienced any further incidents).

A similar approach on the CSEW would help to identify offline compared to online incidences. It would also help to ensure that detail about any online incidents including fraud, cyber and online crimes was not lost because participants are routed to the shorter version of the questionnaire as they perceive the offence to have happened outside of England or Wales, even though they were resident within this jurisdiction at the time.

Participants are also asked to report on why they think the incident occurred. Interviews are given a list to code their responses and are asked not to prompt. Once again, it is sometimes unclear whether a response referring to fraud, cyber and online crimes would be coded to some of the example categories below, and some more clarification for interviewers may help with this. Some example codes and points of consideration are highlighted below:

33 QSCO and QWHERE
34 WHYHAP3A – WHYHAP3S L
1. Negligence/carelessness on the part of respondent or someone else (for example, door left unlocked)
   - Many victims of fraud blame themselves for the fraud taking place, for example they feel that they were naive and did not carry out the necessary checks before transferring funds. This is not the same as being negligent, and it would be important that any reporting of the CSEW findings did not reinforce this view among both victims of fraud and the general public.

2. Due to personal relationship/history between the victim and the offender (for example, conflicts with spouse/partner over children/property etc.)
   - Or as in the case of romance frauds the relationship between the victim and offender could have developed as the fraud progressed.

8. Was part of a series of incidents in area (i.e. number of houses broken into/cars stolen/offenders in area at the time)
   - Certain frauds target specific population groups, and when people report frauds they may also become aware that similar incidences are happening in their area/across a similar profile of people, so this may be relevant for fraud too.

9. The location of the car/house/property/person made it an easy target
   - A PC/laptop/digital device without the necessary protection software may also play a role in victims thinking that they were an easy target.

14. Offender was gang member/Incident was gang-related
   - Some participants could perceive this as being relevant for cyber-enabled, cyber-dependent crimes and other online crime; however it may be preferable to ask whether the crime was committed by an organised group of criminals instead, to distinguish between street gangs.

15. Offender was determined/not deterred by security measures
   - This could also be relevant for cyber-enabled, cyber-dependent and other online crimes.

17. Other (SPECIFY)
   - Code 17 could potentially capture other specific key reasons for fraud, cyber and other online crime occurring, to enable us to know more about the nature of the crime on which the volume estimates are based. An alternative approach would be to consider the advantages of adding additional tailored codes for whether there are any other key reasons fraud, cyber and other online crime occur and whether it would be advantageous to add these to the existing code frame.

Timing and location of incident

Participants are asked to provide details of the timing and location of the incident, including the day and time it occurred which would not be appropriate for crimes committed online. In addition, as discussed in A3.1, fraud, cyber and online crime may happen over a period of time and so pinpointing a time and day when the offence occurred could be challenging. In addition, the current questions about where the
incident happened\textsuperscript{35} may be misinterpreted in some cases, and an alternative approach would be to provide an additional code ‘online / over the internet’.

The location of the incident is captured in the CSEW at WHERE3, shown below.

- I’d now like to ask you about where the incident happened. Did the incident happen inside your own home or garage? CODE FIRST TO APPLY ATTEMPTED BREAK-INS COUNT AS HAPPENING INSIDE THE HOME/GARAGE
  1. Yes – inside own home (including attempted break-ins)
  2. Yes – inside garage that is next to the house/flat
  3. Yes – inside garage that is not next to the house/flat (for example, row of garages for flat/estate)
  4. No

This question may be appropriate for certain types of fraud, for example, signing up to a Ponzi scheme may have taken place in or near the victim’s place of work (WHERE3), however for cyber/online-dependent and/or cyber/online-enabled crimes (where part of the offence happened online and part happened at a physical location), this may be more difficult.

In the SCJS participants who report that the incident did not happen in or near their home or place of work (or don’t know or refuse to answer), are asked a follow-up question (Victim Form QTHME) to further establish where it took place. Interviewers are provided with a list of locations and instructed to probe for the best location. The list includes a number of other offline locations, for example in a pub and a car park, but also includes a category for ‘online /via the internet’. In this way the survey captures the distinction between offline and online offences.

**Damage to property**

If changes are made to the questionnaire so that victims of cyber and other online crime are routed to this section, one option would be to amend some of the question wording to include any damage to computer/other device equipment via online methods. For example to the following\textsuperscript{36}:

- Can I just check, did the person/ the people who did it damage, deface or mess up anything that belonged to you or to anyone else in your household (including any damage which may have been done getting in or out)? Yes, No

Depending on the level of comparable data required about cyber and online crimes compared to non-cyber and online crimes, a separate follow up question could establish the level and nature of damage to the computer/other equipment. This could include the costs of damage done, as is currently the case for other criminal damage offences.

**Theft and attempted theft**

The victim form collects additional information on what was stolen or about attempted theft. This section may, as the reference group suggest, be the place to include some additional questions relevant to the theft or attempted theft of personal information and data, currently contained in the CSEW’s Online Security Module.

\textsuperscript{35} WHERE1 SL
\textsuperscript{36} DEFAPROP SL
Use of force and violence

Participants are also asked about the use of force and violence in the offence. Our research with victims of fraud (Kerr et al, 2013 and Harvey et al, 2014) described how one of the impacts of being a victim of fraud is self-blame. This has implications for this set of questions as it would be vital that taking part in the CSEW does not perpetuate such feelings. One option would be to consider whether it is necessary for victims of fraud, cyber and online crime to be routed to all of the questions in this section. Another would be to review the appropriateness of some of the language used in the current questions, for example, the term ‘responsible’ in the question about responsibility of the crime, shown below37:

- Apart from the offenders, would you say you or anyone else were responsible in any way for what happened, because of something you or they did or forgot to do?
  INTERVIEWER: IF THE RESPONDENT SAYS THAT THE OFFENDER(S)
  WAS RESPONSIBLE FOR WHAT HAPPENED YOU SHOULD CODE 1 AT
  THIS QUESTION
  1. No - no-one
  2. Respondent
  3. Other household member
  4. Respondent AND other household member
  5. Someone else

However some questions would clearly be important to retain with perhaps some modification. For example, an additional category could be added to the question AWARE – shown below - to capture victims who ‘had some suspicions’, about the fraud.

- At the time the incident happened, were you or anyone else aware of what was happening? Yes, No

Lastly, the wording of the questions about force (USEFORCE, FORCWH2A, FORCWH2G, WHATFO3A, WHATFO3W) will also need to be revisited if we want to collect such data from victims of fraud, cyber and online crime, and particularly whether the CSEW is capturing the symbolic (as opposed to physical) force and violence involved in some forms of fraud, cyber and online crime. One view among the reference group was that rather than re-phrasing these questions, new questions and phrases may be included, for example asking about online aggression.

It is towards the end of this section that the questions focus on the impacts of the fraud, cyber and other online crime (EMOTREAC – TIMIMP) and all of the questions will be very relevant, as they would be for any victim group. There is also the option of participants being able to use the ‘other specify’ answer category for any specific impacts in relation to fraud, cyber and other online crime, if it is desirable to keep the answer categories appropriate for a large range of offences and consistent across the time series data. Question FINIMP asks participants to estimate how much they/their household lost overall as a result of the incident, and the largest answer category is ‘more than £500’. One consideration may be to reconsider the banding at this question, differentiating more at the lower value end, between £0 and £50 to further capture micro frauds38 and at the top end to identify larger financial amounts. For example,

37 OTHOFRE L
38 These are online frauds which are deemed to be too small to act upon by victims or the agencies (Wall, 2010a).
victims of investment fraud can lose hundreds of thousands of pounds (Harvey et al., 2014), reflected in the FCA’s CAS which included a financial loss category of over £500,000. Larger amounts of financial loss due to fraud are already included in the Online Security Module of the CSEW (question EEXPLOSS below), alongside an additional category for when the fraud has not yet been resolved.

- You said that you personally experienced loss of money in the last 12 months as a result of using the internet. How much money did you lose? Please DON’T include any money that was subsequently refunded by your bank, building society or credit card company but DO include any additional charges or costs that you incurred as a result of the incident.

IF NEEDED: PLEASE THINK ABOUT ALL THE WAYS IN WHICH YOU LOST MONEY AS A RESULT OF USING THE INTERNET IN THE LAST 12 MONTHS AND PROVIDE A TOTAL AMOUNT

1. None (i.e. 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

The question above also provides additional guidelines for victims who have had some/all of their money refunded, and this would also be a useful clarifying instruction at FINIMP if this question is asked of victims of fraud. Lastly, Levi (2009) puts forward the possibility of another form of financial impact in relation to identify theft. Victims applying for credit may suddenly find themselves denied because of debts previously unknown to them, or may even find bailiffs seizing their property to satisfy a debt that their ‘true selves’ never incurred.

Contact with the police about the incident

Participants are asked about any contact they had with the police about the offence, and all of this section is relevant and important for participants affected by fraud, cyber and online crime, especially as many of these types of offences do not get reported (McGuire & Dowling, 2013). The one possible change to consider would be at question CJSCONTA-I, which lists the agencies that the respondent or someone in their household may have had contact with other than the police. The list could be extended to include other agencies relevant for fraud and cyber and other online crime, for example Action Fraud, the UK’s national fraud reporting centre. This was felt to be the recommended approach among reference group members.

The ICVS also asks whether the offence was reported but does not ask about any specific organisations:

- (The last time) did you or anyone else report it to any public or private agency?
  Yes, No

In this way the question encompasses all possible private and public organisations where victims may report an offence. An alternative approach in the Online Security

---

39 34c
Module of the CSEW is to provide a tailored list of organisations for reporting a computer virus:

- You said that you had experienced a computer virus in the last 12 months. Did you report this to anyone? CODE ALL THAT APPLY
- INTERVIEWER NOTE: IF EXPERIENCED MORE THAN ONE COMPUTER VIRUS, THINK ABOUT THE LAST OCCASION
  1. The police
  2. Anti-virus software company
  3. Internet service provider
  4. Your bank, building society, or credit card company
  5. Action Fraud
  6. Other government agency
  7. Website administrator (for example, Facebook, eBay)
  8. Someone else
  9. No-one

If this module was retained then more detailed information about the reporting of computer viruses, unauthorised access or use of personal data and loss of money in the last 12 months as a result of using the internet could be captured here. This would have to be considered in line with changes to the victimisation module.

A4.2 Reference group discussion points for the Victimisation Module

The Victimisation Module is where more nuanced and detailed information about fraud could be captured. If the approach taken is of one broad screener question to capture fraud this is where we could then delineate what type of fraud it was. Some reference group members suggested that the conceptualisation of fraud in Figure 2.2 (chapter 2), could instead be split into three categories:

- Theft of personal information;
- Paying a fee and not receiving the expected goods/services. However, we will need to consider whether the distinction between receiving something sub-standard compared to receiving nothing at all needs to be captured; and
- Relationship/ befriending fraud.

It will be important to ensure that questions covering these types of fraud use appropriate terms that all respondents understand in a consistent way, and in the way the question designer intended. The reference group flagged that the third sub-category of fraud (relationship/befriending fraud) would require particular care. Question wording will be tested at the cognitive testing stage and suggestions from the reference group included:

- Experiencing a loss after being drawn into someone’s confidence;
- The fraud having a lack of commercial element to it or not; and
- Emotional pull/non-financial pull/having a personal connection with the fraudster(s).

In addition this module should also collect other important characteristics of fraud, cyber and online crime including the following:

- whether an individual had reported the offence and if not the reasons for this;

---

40 EVIRREPA-EVIRREPIC
the timing of the offence. Members generally agreed that asking participants for a specific time reference, such as when they first discovered the fraud would be a suitable approach. This could be followed by an additional question on the length of time it had taken the individual to resolve the issue (if at all); 
• the impact of the offence on the individual involved including change of behaviour and loss experienced (for example financial loss, time taken to resolve the issue and loss of access to services); and 
• prevention measures victims subsequently put in place and the reasons for this. Examples of existing questions on this include section 12.2 of the CSEW’s online security module about keeping safe online, and Q37 and Q37b of the CAS (on financial fraud).

A5 Online crime in the Self-Completion and Domestic Violence and Assault module

The CSEW includes a Self-Completion Module about domestic violence, sexual victimisation and stalking. Although revisions to this module were not the primary focus of this project some key considerations in capturing online victimisation are discussed. Online and internet facilitated forms of sexual abuse and harassment are increasingly being recognised (Webster et al, 2012) and there is a case for updating the module to capture these.

Less serious sexual assault

CSEW contains self-completion questions about ‘less serious’ sexual victimisation. As has been already discussed for previous sections of the CSEW the question wording at the moment does not make it clear whether victims of online and internet facilitated crimes should include their experiences here too. For example, question NIPV17, refers to an individual indecently exposing themselves to the victim (i.e. flashing) yet it is unclear whether participants who have experienced this online would give a positive response.

Serious sexual assault

The CSEW also contains self-completion questions about ‘more serious’ sexual assault. Again it is unclear whether participants should and would answer about online incidents.

• The next questions are about sexual assaults such as rape and attempted rape or being forced into some other sexual act when you were not capable of consent or when you made it clear you did not want to. These crimes affect both women and men. (Section 19.3 of the CSEW questionnaire 2013-14).

The follow up questions are all about serious sexual contact offences, however we do not know whether the internet played a role in anyway. We may want to revisit whether this is something which should and could be captured in this section with an additional question about the nature of the offence and whether the internet played any role in it.

41 As noted in the SCJS Technical report (Page and Twist, 2011:41) the terms ‘less serious sexual assault’ and ‘serious sexual assault’ distinguish between the two types of sexual assault which were asked about separately in the questionnaire. The terms do not relate to the seriousness of the impact on the individual experiencing an incident, as this may vary according to the particular circumstances of an incident.
Stalking

The CSEW includes self-completion questions about stalking. Questions in this section do refer specifically to online crime, namely receiving unwanted emails that were either obscene or threatening (for example NIPV772), and putting obscene information on the internet (for example NIPV832). However the types of online crime they refer to could be expanded to reflect the continually evolving nature of online stalking and harassment. For example alongside emails and putting obscene information on the internet, webcams, social network sites, internet discussion forums and hacking attacks can also play a role in this type of offence.

The SCJS has addressed this by including a question that explicitly refers to online offences against the person, (codes 2 and 3 below)\(^{42}\):

- Since <INSERT DATE>, has ANYONE done any of the following things to you? This may have been a partner, a family member, someone you knew casually, or a stranger. YOU CAN CHOOSE MORE THAN ONE ANSWER AT THIS QUESTION IF YOU WISH.
  1. Sent you a number of unwanted LETTERS OR CARDS that were either obscene or threatening
  2. Sent you a number of unwanted EMAILS OR TEXT MESSAGES that were either obscene or threatening
  3. Made a number of obscene, threatening or nuisance approaches to you via a SOCIAL NETWORKING SITE.
  4. Made a number of obscene, threatening, nuisance or silent PHONE CALLS to you
  5. Waited or loitered outside your home or workplace on more than one occasion
  6. Followed you around and watched you on more than one occasion

The CSEW could adopt a similar approach, however there is a potential need to regularly update as this is a fast-changing area.

Domestic violence

The CSEW includes a series of self-completion questions about domestic violence. Once again, the questions in this section do not explicitly refer to online crime offences, and it is unclear whether participants include online incidents. One implication of this is that with time they may become increasingly unreliable. For example question NIPV4:

- And has a partner or ex-partner frightened or threatened you in any way in the last 12 months? For example, they may have threatened to hurt you, to kill you, to use a weapon on you, or to hurt someone close to you [such as your children]?
  1. Yes 2. No 3. Don’t know/can’t remember 4. Don’t wish to answer

Again there may be a preference for also including a question about whether this form of victimisation took place online or offline, if this distinction is something the CSEW wants to capture.

\(^{42}\) SHO
Appendix B. Cognitive interview findings

B.1 Aims of stage 2 and study design

Stage two involved developing and testing, using cognitive interviewing methods, proposed new screening questions and testing a subset of questions contained in the victim form. 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 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.

This Annex presents the findings from cognitive interviews that took place over two rounds of testing. The first round, which took place in August 2014, involved 18 participants. The participants had previously taken part in the Crime Survey for England and Wales (CSEW) and given their consent to recontact. All were asked a subset of the existing CSEW screening questions before being asked the new questions. This subset of questions was asked to replicate, to some extent, the survey context in which the new screening questions would be asked, and to assess whether any current screening questions might pick up fraud or cybercrime offences. The questions included are contained in Appendix C.

Three new questions, one asking about experience of confidence fraud in the past 12 months, one about non-confidence fraud and one about theft of personal data and interference with internet and computer access were tested. If the participant answered ‘yes’ to a screening question then he or she was asked a follow up question asking how many times this had happened.

Findings from this first test were rapidly reviewed to identify any problems with the questions. Changes to problematic questions were agreed with ONS and revised questions tested in a second round of cognitive interviews in September 2014. This second round involved 19 participants, some of whom were CSEW participants who had given consent to being recontacted and some were participants recruited directly by interviewers because they had experienced a fraud or computer misuse act incident. This direct recruitment method was introduced so as to maximise the number of ‘victims’ and so ensure questions in the victim form were tested with as wide a range of people experiencing as wide a range of fraud and computer misuse act incidents as possible. In this second round of testing four new screener questions were tested: confidence and confidence fraud questions remained, in amended form with the theft of
data and interference with internet and computer access being split into two separate questions, one asking about interference with internet and computer access and one about theft of personal data. The order in which the new screening questions were asked also changed at round two, as follows.

<table>
<thead>
<tr>
<th>Round 1</th>
<th>Round 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence fraud</td>
<td>Confidence fraud</td>
</tr>
<tr>
<td>Non confidence fraud</td>
<td>Interference with internet and computer access</td>
</tr>
<tr>
<td>Theft of personal data and interference with internet and computer access</td>
<td>Theft of personal data</td>
</tr>
<tr>
<td></td>
<td>Non confidence fraud</td>
</tr>
</tbody>
</table>

In both rounds of testing incidents that had happened over a longer time period than the 12 months specified in the CSEW were included. This resulted in participants reporting incidents that had happened up to seven years ago. This extension to the reference period was adopted so as to maximise the number of victims of fraud and computer misuse identified by the screening questions, which could be followed up in the victim form and so allow testing of these questions. The findings distinguish, where appropriate, between cases where an incident took place within the 12 month reference period and those that took place outside it.

Those who answered ‘yes’ to one of the new screening questions were then asked a subset of questions from the victim form. Many of these questions were existing questions contained in the victim form, which we tested to assess how well they worked in relation to asking about fraud and computer misuse. However some questions currently contained in other modules in the questionnaire were also included. Again some modifications to questions were made between rounds one and two of testing, in light of findings from round one.

**B2 Screening questions findings**

Findings from rounds one and two of cognitive interviews are presented. Where the question wording remained the same between rounds then findings are reported for all cases; however where changes were made between rounds one and two we discuss findings for each round separately.

The new questions were asked at the end of the screening questionnaire, in the section asking about crimes the participant had experienced personally. Chapter 2.2 sets out the rationale for this decision. The current CSEW introduction to this section of questions, shown below, was read to participants before a subset of existing screening questions were asked. These included questions about theft from the person, threats to damage property or actual damage of property. The existing screener questions
included in the test were those where it was felt there might be a potential overlap with
the proposed new screening questions. As noted in section B1, if participants had not
experienced any incidents in the last 12 months then the interviewer asked if they had
experienced any incidents during the last 5 or so years. The text in purple indicates
new questions or modifications made to current CSEW questions, which were tested.

INTRO2

The next few questions are about things that may have happened to you
PERSONALLY [not the other people in your household] or that you discovered over the
last 12 months, that is since the first of September 2013, in which you may have been
the victim of a crime or offence. Again, I only want to know about things that have
happened in the period marked on the calendar, so we can build a picture of crime in
the last 12 months.

Please include anything that happened to you during that time – at home, in the street,
at work, in a shop, in a park, on a train, online or anywhere else.

B2.1 Confidence fraud

We tested two different version of this question at each round of testing, with the aim of
assessing whether one form of words better captured confidence frauds than the other.
The forms of words tested were as follows:

CON - [Apart from anything you have already mentioned], in that time has...

<table>
<thead>
<tr>
<th>Round 1</th>
<th>Round 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version A</td>
<td>Version B</td>
</tr>
<tr>
<td>...has anyone obtained money or goods from you under false pretences, using whatever means?</td>
<td>...has anyone conned you out of money or goods, in person or online?</td>
</tr>
</tbody>
</table>

The response options to this question were yes and no. The reference to ‘in person’ in
version B covered both face-to-face and telephone interactions. There was no
evidence to suggest that telephone interactions were being excluded.

Note that version B, ‘conned’, remained unchanged at round 2. When presenting
findings on this version we present combined findings from both rounds of testing.

B2.1.1 Types of crime considered

Participants were asked what they thought the question was asking them. Across all
three variants of the question there were participants who only thought about online
incidents, in-person incidents or, as was intended, incidents involving all modes of
communication. Consideration of online only incidents was less commonplace among participants asked the version ‘under false pretences’ at round one. There are several possible explanations for this: this may be chance, the sample being small and purposive. Alternatively the inclusion of the phrase 'by any means', which was not included in the other versions tested, may have encouraged participants to consider face-face incidents. There is some evidence support this hypothesis. There was no evidence, however, to suggest that those thinking only about one modus operandi of fraud had experienced a confidence fraud in any other mode.

Phishing emails were considered by some at this question but were discounted as participants had not responded to them. All participants were clear that the question was only asking about actual confidence frauds and not attempts.

B2.1.2 Understanding of the different versions of the question

Participants’ understanding of the question during the interview was explored. There were a number of similarities in the way in which these questions were understood but there were a few notable differences, which we discuss below.

<table>
<thead>
<tr>
<th>Under false pretences</th>
<th>Tricked or deceived</th>
<th>Conned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pretending to be someone or something you are not</td>
<td>Pretending to be something you are not</td>
<td>Obtaining money or processions from you under false pretences</td>
</tr>
<tr>
<td>Deception/ being lied to</td>
<td>Deliberately lying or misleading someone</td>
<td>Buying something that turns out to be fake</td>
</tr>
<tr>
<td>Obtaining personal information to use in a fraud</td>
<td>Tricking you into providing personal information to use in a fraud</td>
<td>Using unfair tactics to obtain money</td>
</tr>
<tr>
<td>Involving threats of violence</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Under false pretences

This version of the question, tested at round one, was the only one to include the phrase 'by whatever means'. The 'conned' version referred to ‘in person or online’ whereas the 'tricked or deceived' version made no reference to the mode of communication at all. ‘By whatever means’ was interpreted as involving some form of violence or threat of violence, or deviousness and contributed to the view among some that the question was concerned with confidence frauds that involved in-person contact with the perpetrator.
In addition, there was some confusion over the meaning of ‘under false pretences’. This confusion involved participants considering that the question was asking if someone was ‘pretending’ to be them, either by using their identity or their bank details. The distinction between confidence (CON) and non-confidence (NONCON) fraud questions was blurred in these circumstances and this may have been a contributory factor in two participants answering ‘yes’ to both screening questions, see section B2.9. The wording of this version of the question was changed ahead of round two to ‘tricked or deceived’ in an attempt to more clearly differentiate between this question and the other ‘new’ screener questions, and so reduce the potential for double counting.

**Tricked or deceived**

Round two participants thought about ‘being defrauded’, ‘being ‘mislead’ or this involving some kind of ‘pretence’ when answering this question. Being deceived could involve someone tricking you into providing personal information, such as bank account details.

**Conned**

The ‘conned’ version of the question was largely interpreted as intended. There were two exceptions. The first, at round one, was where a female participant, aged 34-54 thought about whether she had experienced any incidents of someone using her identity or card details online to buy things. She understood conned as meaning being ‘tricked’ – someone has told her something that isn’t true and has obtained money from her. However she did not appear to actually use this definition when thinking about her answer to the question. The other, a male participant, aged 55 plus, reported an incident of being sold a chair for his arthritis (round 2, incident 8 in Table B2.1). He described this as an incident of sales “sharp practice”, in which he had been targeted and deceived as to the value of the chair at a point when he was particularly vulnerable (he had recently been widowed and had come out of hospital). This case highlights the grey area between confidence fraud and consumer detriment. Section 4.5.1 discusses an approach which could be used in the victimisation module to establish whether the incident is a confidence fraud or consumer detriment.

One participant, at round two, commented that she did not like the word ‘conned’ – as this was slang and it was not clear to her what types of incident she should include.

**B2.1.3 Understanding of ‘goods’**

All three versions of the question referred to obtaining ‘money or goods’. The term ‘goods’ was interpreted in a range of different ways and reflected the types of incident participants had experienced (those who answered ‘yes’) or the sorts of incidents that came to mind (those who answered ‘no’ to this question).

- Commodities - clothes, food, jewellery, furniture, iPad, household appliances
- Bank/ credit card details
- Services
Participants continued to think of goods in these ways when answering subsequent screening questions.

**B2.2 Non confidence fraud**

Two version of this question, one at each round of testing were tested, see below. The wording was amended ahead of round two based on findings from round one testing.

**NONCON [Apart from anything you have already mentioned], in that time has…**

<table>
<thead>
<tr>
<th>Round 1</th>
<th>Round 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>…has anyone used or tried to use your personal information or account details in any way to buy goods or services without your permission or knowledge or to pretend to be you?</td>
<td>… has anyone used or tried to use your personal information or account details in any way to buy goods or services without your permission or knowledge?</td>
</tr>
</tbody>
</table>

The response options to this question were yes and no.

At round one both interviewers and participants, on occasion, commented on the length of the question and whether this could be simplified. In some cases participants thought the question was asking about only identity theft or someone trying to impersonate them or about credit card fraud.

In addition, there was a blurring in participants’ minds of the difference between NONCON and CMACT. Some participants thought about people “hacking” into their computer to obtain information about them, in some cases so that they could pretend to be them, in relation to both versions during probing.

It was agreed with ONS that this question should not include instances of someone pretending to be the respondent to buy goods or services as this would be covered by the CMACT question. We therefore amended the wording of this question and tested a revised wording at round 2, which attempted to make the question simpler and less wordy.

The placement of this question changed between rounds one and two. In round one this question was asked after asking about confidence fraud. In round 2 the question was asked after asking about interference with internet and computer access and theft of personal data. This was done to reduce the risks of double-counting observed at round one.

**B2.2.1Types of crime considered**

Participants at both rounds were asked about what types of crime came to mind when answering this question. The types of crimes considered were similar across both
rounds, with participants typically thinking about someone obtaining their bank or card details and using these to buy things. This could involve someone hacking into their online bank account, cloning their cards or physically stealing their cards. In a few cases participants also thought about someone stealing their personal details, such as their passport or National Insurance number.

B2.2.2 Understanding of key terms

The question asked about whether anyone had ‘used or tried to use your personal information or account details’. We explored participants’ understanding of ‘used or tried to use’ and ‘personal information or account details’.

Participants considered both attempts and actual use of their person information or account details. Attempts were considered to be where someone had been “unsuccessful” in trying to obtain or use of their account or personal information.

The types of information considered as being personal information and account details are shown below.

<table>
<thead>
<tr>
<th>Personal information</th>
<th>Account details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passport</td>
<td>Bank account number and sort code</td>
</tr>
<tr>
<td>Date of birth (of participant)</td>
<td>Credit cards/ store cards</td>
</tr>
<tr>
<td>Name &amp; address (of participant)</td>
<td>Account passwords</td>
</tr>
<tr>
<td>Telephone number</td>
<td>User ID</td>
</tr>
<tr>
<td>National Insurance number</td>
<td>Pin number</td>
</tr>
</tbody>
</table>

The distinction between personal information and account details was not always clear, with some participants noting that personal information could form part of account details, for example being part of the security questions used to access an online account. The inclusion of both personal information and account details in the question helped ensure that both types of information were considered.

B2.3 Interference with internet and computer access, and theft of personal data

Both rounds of testing included a question about computer misuse act incidents. Two versions of the question were tested at each round to establish whether one form of words was better at capturing this type of crime. At round one both versions asked about interference with internet and computer access and theft of personal data. The wording was as follows.

CMACT [Apart from anything you have already mentioned], in that time has…
<table>
<thead>
<tr>
<th>Version A</th>
<th>Version B</th>
</tr>
</thead>
<tbody>
<tr>
<td>... anyone stolen your personal information or details, or installed unwanted programs, including viruses, on any internet-enabled devices you use for personal use?</td>
<td>... anyone accessed information held digitally about you without your permission, altered your data without your permission or installed unwanted programs, including viruses, on any internet-enabled devices you use for personal use?</td>
</tr>
</tbody>
</table>

Findings from round one were inconclusive regarding which form of words was better. In both cases some participants focused solely on the stealing of financial information whereas others, who were more IT savvy or knew people who had had problems also talked about other personal data, such as someone getting on to Facebook, being compromised or misused.

Some participants found the question lengthy and confusing because there was a lot of information in it. In some cases participants focused on just one part of the question – details being ‘stolen’ off the internet or viruses. We proposed splitting the questions into two, one asking about the interference with internet and computer access, such as viruses, and one asking about the theft or unauthorised access of personal information, in an attempt to simplify the question and make it clearer. These recommendations were accepted and revised questions tested at round two.

Those with limited IT knowledge did not understand the phrase ‘unwanted programs’ and in two cases participants thought about software updates or pirate download sites for music or films respectively. At round two, the new VIRUS question, refer to section B2.4, attempted to clarify what we mean by unwanted software in terms of its purpose.

At round two we tested the following simplified versions of the theft of personal data question.
B2.3.1 Types of information considered

The types of information considered at these questions were similar, as can be seen below.

<table>
<thead>
<tr>
<th>(A) ‘stolen personal information or details’</th>
<th>(B) ‘accessed information held digitally about you without your permission’</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>Email address</td>
</tr>
<tr>
<td>Bank account/ card details</td>
<td>Bank account/ card details</td>
</tr>
<tr>
<td>Passwords</td>
<td>Account passwords (banking; social media; shopping)</td>
</tr>
<tr>
<td>Name, address</td>
<td>Name, address, telephone number</td>
</tr>
<tr>
<td>Birth/ marriage certificates</td>
<td>Photos</td>
</tr>
<tr>
<td>Financial information (not bank account details)</td>
<td>Financial information (not bank account details)</td>
</tr>
<tr>
<td>Medical information</td>
<td>Companies/ people adding to your personal information i.e. iTunes adding to your play list</td>
</tr>
</tbody>
</table>

Some participants considered their name, address and telephone number to be ‘personal’ information. This reflected participants’ view that this information was ‘private’ and should only be available to individuals and organisations to which they had given permission to hold these details. These participants did not like companies sharing their data. This also applied to email addresses. However an email address could also form part of the login to online accounts, and so people obtaining this information without participants’ knowledge or permission was of particular concern to some. However other participants did not consider an email address to be ‘personal information’ as it was in the public domain.
### B2.3.2 Understanding of the different versions of the question

The cognitive interviews explored participants understanding of the different formulations of this question. These understandings are presented below.

<table>
<thead>
<tr>
<th>Round 1</th>
<th>Round 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version A</strong></td>
<td><strong>Version B</strong></td>
</tr>
<tr>
<td>... anyone stolen your personal information or details, or installed unwanted programs, including viruses, on any internet-enabled devices you use for personal use?</td>
<td>...anyone accessed information held digitally about you without your permission, altered your data without your permission or installed unwanted programs, including viruses, on any internet-enabled devices you use for personal use?</td>
</tr>
</tbody>
</table>

| Someone “hacking” into your computer to access/steal account details or pretend to be you on social media | Someone “hacking” into your computer to access/steal account details, personal info or pretend to be you on social media | Stealing personal info / account details held online to pretend to be you and buy goods | Someone “hacking” into an online site (for example, a retailer) and stealing customers login/payment details |

| Personal info used to buy goods or services | Stealing personal info (or “identity”) and using it for own benefit | Stealing personal info/ account details by physically stealing paper records | Infringement of privacy – stealing personal things such as photos |

| Steal your wallet/phone/computer & try to get into your account or spend your money | Stealing personal info/ account details by physically stealing paper records | Infringement of privacy – stealing personal things such as photos |

| Only thought about viruses | Use of viruses to “steal” passwords | Someone installing software to steal personal info/account details | }
Generally participants considered details being stolen or obtained from digital sources – information held on a computer or online, in relation to both formulations of the question, even though version A did not explicitly state this. Version A encouraged a few participants to consider information not held digitally, such as the theft of bank cards or paper records, or to think about the theft of a smartphone or laptop and the risk of personal information being obtained. However none of those who participated in this study who considered the physical theft of data had actually experienced it.

As mentioned in section B2.3, at round one this question included reference to viruses and the inclusion of this additional clause led to a minority of participants considering only whether their computer had been infected with a virus (which could “steal” passwords). Those who talked about viruses stealing passwords worked in IT and had a greater awareness of how viruses are used to steal data.

B2.3.3 Understanding of key terms

Stolen/ accessed

Both versions of the question referred to personal information being either ‘stolen’ or ‘accessed’. Probing revealed that these two terms were understood in a similar way. Both terms were thought to mean information being taken or obtained without permission.

Held digitally

One version of the question (version B) referred to personal data being ‘held digitally’. Among those who took part in this test this term was generally understood to refer to information held on computers, smartphones and tablets, “the internet” or “in the cloud”.

One participant, an elderly lady who did not use the internet questioned whether ‘held digitally by you’ meant held on computer. She thought personal data were things like your name, address and telephone number.

B2.4 Interference with internet and computer access

At round two we included a separate question, asking about interference with internet and computer access. The question was worded as follows.

Apart from anything you have already mentioned, in that time has anyone…

installed software, including viruses, that collects information you do not want them to have on any internet-enabled devices you use?

1. Yes- ASK NVIRUS
2. No – GO TO CMACT
3. [Spontaneous] Does not have a computer – GO TO CMACT

This question was asked after the confidence fraud question.
B2.4.1 Types of crime considered
Participants were able to provide an answer to VIRUS, albeit commonly prefaced by ‘as far as I know’. Viruses that were caught by anti-virus software were included at this question by some participants.

B2.4.2 Understanding of key terms

Unwanted programs
At round one, viruses and ‘unwanted programs’ were asked about as part of the question asking about computer misuse, see section B2.3. The phrase ‘unwanted programs’ was interpreted in a variety of ways, reflecting participants knowledge of this type of threat. The types of programs mentioned were: malware and spyware; pornography; Trojans (programs that run in the background on your computer and collect data); and illegally downloading music or films. One female participant, aged 18-34 was unsure and thought it might refer to spam and ‘pop-ups’. In addition several, older female participants, aged 55 plus did not know what ‘unwanted programs’ would be. They either did not use the internet or used it very rarely.

Installed software
At round two, the question asked about whether ‘anyone had installed software, including viruses’. The phrase ‘has anyone installed software’ was taken literally by some participants, who thought it was asking them if someone had physically accessed their computer and installed a virus program. These participants varied in age. In a minority of cases participants thought about other types of software, beyond viruses. Software thought about was program upgrades, pornography, online banking software and "anything illegally downloaded" from an external source not known to the participant. Examples provided by the participant who considered this were music and films.

Internet enables devices
Generally this phrase was understood by participants as intended: it referred to any device that was used to access the internet, such as computers, tablets, smartphones, smart TVs and games consoles. However there was a small minority of participants who did not know what it referred to. These were all older participants, aged 65 and over who by their own admission were not IT savvy,

B2.5 Number of incidents
If participants answered ‘yes’ to a screening question they were asked a follow up question:

As far as you are aware, how many times has that happened? (CON ONLY: If you received multiple communications about the same scam please count as one incident).
This question establishes the number of incidents that have occurred and this information is used to estimate the volume of crimes that have occurred. Note that for confidence frauds, the question included an additional instruction to participants to include multiple communications about the same ‘scam’ as one incident.

The answers provided to this question are provided in Figure B2.1. There was some inconsistency in the way in which the question was answered. In some cases participants answered in relation to the theft of details (answering one), whilst in other cases they reported each time the card was used/ a transaction was made. Clear guidance is needed so that participants provide consistent information.
### Figure B2.1 Number of incidents recorded

<table>
<thead>
<tr>
<th>Round</th>
<th>Incident</th>
<th>Incident description</th>
<th>Screener Qs</th>
<th>No incidents reported</th>
<th>Which screener Q should have been coded yes(^{43})</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Bank account details being used by someone to purchase a computer on a monthly direct debit came to light when the participant noticed the payments on her statement and queried with the bank. This crime took place about 7 years ago.</td>
<td>CON. NONCON &amp; CMACT</td>
<td>1</td>
<td>NONCON</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>A bank card being cloned at a cash point in England and used to withdraw money in the US. This incident occurred about 3 years ago</td>
<td>CON &amp; NONCON</td>
<td>1</td>
<td>NONCON</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>An order for a crate of wine made over the internet, which never arrived. It turned out that the company was taking orders and money with no intention of delivering the goods. This incident happened in December 2013</td>
<td>CON</td>
<td>1</td>
<td>CON</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>Purchase of a computer on GumTree, which never arrived and the money paid for it was never refunded. This incident happened in December 2013</td>
<td>CON</td>
<td>1</td>
<td>CON</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>Use of bank details by an unknown person to top up a phone card (£50). This incident occurred 6 years ago</td>
<td>NONCON</td>
<td>n/a</td>
<td>NONCON</td>
</tr>
</tbody>
</table>

\(^{43}\) It should be noted that the cognitive interview did not include victim checklist questions, which are designed to assist with coding and as such the coding suggestion presented is a ‘best guess’ based on the information available.
### Figure B2.1 Number of incidents recorded

<table>
<thead>
<tr>
<th>Round</th>
<th>Incident</th>
<th>Incident description</th>
<th>Screener Qs</th>
<th>No incidents reported</th>
<th>Which screener Q should have been coded yes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>Took part in a survey that appeared as a pop up on the M&amp;S website. Gave card details to cover postage &amp; packaging of a free gift. Site turned out to be fake and several transactions we made from the card of £99 a time.</td>
<td>CON</td>
<td>1</td>
<td>CON</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Paid deposit for a flat in Berlin through an English letting agent but it turned out the flat did not exist. R was living outside England &amp; Wales at the time</td>
<td>CON</td>
<td>1 (4 emails but tricked only once)</td>
<td>CON</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>Someone had got R's card details and made various transactions, including an attempt to transfer money to another account. The bank contacted R about the incidents.</td>
<td>CON</td>
<td>1 (7 incidents of his card being used to buy things. Thought all being done by same person)</td>
<td>NONCON</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>Applied for a credit card online via the high street bank’s website, providing various details. A few days later received a call from XXX Cards about his application. He asked them to cancel it and remove his details but a month later received a letter saying his credit card application had been approved.</td>
<td>CMACT</td>
<td>1</td>
<td>CMACT</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>A number of online transactions were made using R's credit card details without her permission or knowledge. She discovered this when her bank contacted her about them. The cards were in her possession when this occurred. R answered ‘yes’ to both CMACT &amp; NONCON about the same incident</td>
<td>CMACT &amp; NONCON</td>
<td>4 (not sure whether to answer 1 or 4 because it was 1 incident that occurred but 4 transactions)</td>
<td>NONCON</td>
</tr>
<tr>
<td>Round</td>
<td>Incident</td>
<td>Incident description</td>
<td>Screener Qs</td>
<td>No incidents reported</td>
<td>Which screener Q should have been coded yes</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>R’s bank card was cloned and used to make cash withdrawals from her account. She discovered this when her bank contacted her to confirm the transactions. R answered ‘yes’ to both CON &amp; NONCON about the same incident. At NONCON realised that this was a better fit for her incident.</td>
<td>CON &amp; NONCON</td>
<td>2 - the card was used twice</td>
<td>NONCON</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>Ex partner had used R’s details to take out pay day loans, hacked into his email accounts and changed passwords, used R’s details to open an online sex account, taken out a mobile phone in his name and used it, claimed R was driving car when parking fines were incurred. There were quite a few different incidents and R reported different ones at CON, CMACT and NONCON</td>
<td>CON, CMACT, NONCON</td>
<td>CON = 1. One person doing many things NONCON - over 20 different incidents committed by the same person</td>
<td>CON, CMACT, NONCON</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>Sold a chair for arthritis, soon after R’s wife died, for £1,600, by someone who telephoned him. The seller (who R didn’t know) knew that the R had been in hospital with arthritis. The seller claimed it would stop his arthritis. When the chair arrived it was second hand and it did not help his arthritis. R felt he had been conned into buying it at such a high price</td>
<td>CON</td>
<td>1</td>
<td>NONE – CONSUMER DETRIMENT. INCIDENT OUT OF SCOPE</td>
</tr>
<tr>
<td>Round</td>
<td>Incident</td>
<td>Incident description</td>
<td>Screener Qs</td>
<td>No incidents reported</td>
<td>Which screener Q should have been coded yes</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>R bought a boat engine from someone over the internet but the engine never materialised. The engine was bought from someone in Scotland. R made several attempts to get his money back but to no avail. R reported the incident to the police.</td>
<td>CON</td>
<td>N/A</td>
<td>CON</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>R receives numerous fraudulent emails saying she has won a prize or such like and needs to give her bank details so it can be paid into her account. Thinks the fraudsters must have gained access to her personal details to have her email address. She says she 'generally' does not respond. Answers 'yes' to CON and CMACT in relation to these attempts to con her. R also had an incident where she had tried to pay a bill online and found she couldn't. Called her bank who told her they were investigating fraudulent activity (her card had been used in Nigeria earlier that day). She answered yes to NONCON</td>
<td>CON &amp; CMACT</td>
<td>CON = 1 NONCON = 2</td>
<td>NONCON</td>
</tr>
</tbody>
</table>

Note: NONCON = 2 Not enough evidence to demonstrate a crime. Not a CON as no response to email. Not a CMACT as no evidence that personal details were taken.
<table>
<thead>
<tr>
<th>Round</th>
<th>Incident</th>
<th>Incident description</th>
<th>Screener Qs</th>
<th>No incidents reported</th>
<th>Which screener Q should have been coded yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>11</td>
<td>R inadvertently clicked on Malware that added something to his browser that he didn't need. It was difficult to remove. R answered yes to VIRUS. R also reported an incident where a porn company claimed he had downloaded a film and needed to pay. They had gained his address details from his broadband provider. R was not sure exactly what other personal information the company had obtained. They threatened legal action if he did not pay and started by asking for a couple of £100 but this escalated to several thousand. He discovered that this was a scam by doing his own research. He felt this was a CON but R did not mention it at first (it occurred in April 2013) and he was embarrassed by it.</td>
<td>VIRUS, CON (but only disclosed on further probing)</td>
<td>VIRUS =2. These were two separate incidents of malware</td>
<td>VIRUS, CON</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>R reported several viruses (phishing) that her anti-virus software had picked them up and dealt with them in the past 12 months.</td>
<td>VIRUS</td>
<td>3</td>
<td>NONE: VIRUSES QUARENTINED BY ANTI VIRUS SOFTWARE OUT OF SCOPE</td>
</tr>
<tr>
<td>Round</td>
<td>Incident</td>
<td>Incident description</td>
<td>Screener Qs</td>
<td>No incidents reported</td>
<td>Which screener Q should have been coded yes?</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>----------------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>13</td>
<td>R receive an email, which appeared, at first sight, to be genuine saying that she had bought 9 tickets for a performance of Peter Pan and that she should open the attachment to view and print the tickets. It also provided links to click to the theatre. The email contained the last 4 numbers of a credit card that she had once had. At first she thought that this was a mistake and tried to ring the theatre but the line was constantly engaged. Next she went to the bank to stop any payment being made and it became apparent that this was an internet crime to try and get her to open the attachments, which would install viruses. She didn’t open them.</td>
<td>CMACT (also answered yes to NONCON for same incident but Interviewer did not read ‘apart from anything you have already mentioned’.</td>
<td>1</td>
<td>CMACT – no evidence that money was taken from account but credit card details had been obtained.</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>Someone used R’s credit card to buy an air line ticket without his permission. Incident happened in last 5 years.</td>
<td>CMACT (also answered yes to NONCON for same incident but Interviewer did not read ‘apart from anything you have already mentioned’. R was not sure what the difference between CMACT &amp; NONCON was</td>
<td>NONCON- N/A CMACT - N/A</td>
<td>NONCON</td>
</tr>
<tr>
<td>Round</td>
<td>Incident</td>
<td>Incident description</td>
<td>Screener Qs</td>
<td>No incidents reported</td>
<td>Which screener Q should have been coded yes</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td>R had several viruses so answered yes to VIRUS. R had an email from an online retailer telling him their site had been hacked and that customers should change their passwords. He answered ‘yes’ to CMACT. R’s credit card had been cloned and used. The bank contacted him to check if he had made the transaction, which he hadn’t. This happened about 5 yrs ago. He answered yes to NONCON.</td>
<td>VIRUS, CMACT, NONCON</td>
<td>VIRUS =1 NCON= N/A NONCON= N/A</td>
<td>VIRUS, CMACT, NONCON</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>Bought a camera online. Paid using his credit card but never received a confirmation email. He looked up the company and found out it was a scam. He contacted his credit card company at this point.</td>
<td>CON</td>
<td>2 - bought fake item on EBay in Nov and in Jan bought camera online that didn't exist</td>
<td>INSUFFICIENT INFORMATION TO DETERMINE IF A CON</td>
</tr>
</tbody>
</table>
B2.6 Sorting out the series

The CSEW screening section includes a number of questions that establish whether, for multiple incidents of the same crime, these are part of a series or not, and for those incidents that are part of a series, the pattern of that series. We included these questions in our tests. The questions were as follows.

**+SIMILAR** [ASK IF MORE THAN ONE INCIDENT OF CRIME]

You mentioned [WRITE IN NUMBER OF INCIDENTS FROM NCON NONCON/CMACT/VIRUS_____] incidents of [INCIDENT\(^{44}\)]. 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?

3. Yes
4. No

**ALLPART**

(As far as you are aware) Were all the incidents of ... [INCIDENT] ...part of a series or were any of them separate incidents?

1. All were part of a series – GO TO FORM 2, INTCHK3
2. Some were separate incidents, the rest were a series – ASK XNUMS

**+XNUMS** [ASK IF ALLPART = 2 (SOME SEPARATE, REST SERIES)]

How many of the [NUMBER INCIDENTS AT, for example, NCON_____] incidents were SEPARATE incidents?

**ENTER NUMBER ________**

SIMILAR was asked only of four participants, who had indicated at earlier questions that they had experienced more than one incident of a particular type of fraud or computer misuse act offence. No one in this test was asked ALLPART or XNUMS and as such data on the appropriateness of these existing CSEW questions for the new screening questions is limited.

All participants correctly interpreted SIMILAR as asking about whether the same people committed the crime at each occasion. Participants’ ability to answer this question depended on what they knew about the circumstances in which offences took place. For example, one female respondent, aged 18-34 could not provide an answer to this question.

“I really don’t know. I just know my details were stolen and I don’t know how it happened or where it happened. All I know is it happened.”

\(^{44}\)Example of ^INCIDENT textfils from R2, version A
IF CON, ^INCIDENT= “tricking or deceiving you to obtain money or goods.”
IF VIRUS, ^INCIDENT= “installing software, including viruses, on any internet-enabled devices you use.”
IF CMACT, ^INCIDENT= “stealing your personal information or details.”
IF NONCON, ^INCIDENT= “using or trying to use your personal information or account details to buy goods or services without your permission or knowledge.”
Female, aged 18-34, NONCON=yes, bank card cloned

In another case where the participant’s credit card was used without her knowledge or permission she knew how many times it had been used and answered ‘yes’ to SIMILAR because the bank had told her each transaction was part of the same incident.

B2.7 Crimes missed by the screening questions

At the end of the cognitive interview participants who had not mentioned being the victim of a fraud, theft of personal data or interference with internet or computer access were asked whether they had experienced any specific incidents covered by these screening questions. These ‘experience’ questions are currently included in follow up modules of the CSEW questionnaire.

**EEXPINT SHOW CARD**

In the last 12 months, have you personally experienced any of the things mentioned on this card while using the internet? CODE ALL THAT APPLY

1. A computer virus
2. Loss of money
3. Unauthorised access to/use of personal data (for example, e-mail account/bank account)
4. Upsetting images/illegal images
5. Abusive/threatening behaviour
6. None of these
MMFRD1

Looking at this card, have you personally EVER received any emails, texts, letters or phone calls from an individual or a company that you've never heard of before about any of the following?

Now thinking about the LAST 12 MONTHS, have you personally received any of these emails, texts, letters or phone calls from an individual or a company that you've never heard of before?

SHOW CARD

CODE ALL THAT APPLY. INTERVIEWER: THIS INCLUDES INTERNET POPUPS

1. A big win in a lottery, prize draw, sweepstake or competition that you haven’t entered
2. The chance to make an investment with a guaranteed high return (for example, shares, art, fine wine, etc.)
3. Someone who invites you to get to know them with a view to a possible friendship or relationship (this may be via a website)
4. Help in moving large sums of money from abroad
5. Help in releasing an inheritance
6. An urgent request to help someone get out of some sort of financial trouble
7. A job offer, a franchise offer or other business opportunity
8. A loan on very attractive terms
9. Adopting or buying a pet
10. Some other type of similar request
11. None of these
12. SPONTANEOUS ONLY: Never read or listen to messages like these

There was no evidence to suggest that the new screener questions were failing to detect the types of incidents covered by EEXPINT and MMFRD1.

Participants did, in some cases, report computer problems or having received mass marketing fraud emails but did not include these because they had not responded to them.

B2.8 Willingness to answer

Participants who took part in this study were willing to provided a ‘yes’ or ‘no’ answer to the new screening questions. However some participants expressed reservations, on further probing at the end of the interview, about whether in the actual survey people would be willing to provide this type of information as they felt the information was sensitive and participants may feel embarrassed about admitting and or discussing being a victim of such crimes. Further, larger-scale testing is required to assess likely item non-response to these questions and to assess the extent of any under-reporting (people answering ‘no’ when the true answer is ‘yes’). Respondent debriefing questions could also be added to the end of the self-completion module to check if any additional incidents have occurred that have not been captured earlier in the interview, see section 5.2.3.
B2.9 Potential double counting

A minority of participants (7) answered ‘yes’ to more than one screening question about the same incident, which could result in double-counting. The circumstances in which this occurred are presented in Figure B2.2 below.
### Figure B2.2 Circumstances in which ‘double-counting’ arose

<table>
<thead>
<tr>
<th>Incident</th>
<th>Incident description</th>
<th>Rational for answering multiple screener Qs about same incident</th>
<th>Q version</th>
<th>Which screener Q should have been coded ‘yes’&lt;sup&gt;45&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>(R1) 1</td>
<td>Bank account details being used by someone to purchase a computer on a monthly direct debit. Came to light when the participant noticed the payments on her statement and queried with the bank. This crime took place about 7 years ago.</td>
<td>CON - thinking about someone using her card. They had accessed her card details and used cards to buy goods. NONCON - thinking about someone impersonating her, using her card CMACT - thinking about someone getting hold of her card details</td>
<td>B</td>
<td>NONCON</td>
</tr>
<tr>
<td>(R1) 2</td>
<td>A bank card being cloned at a cash point in England and used to withdraw money in the US. This incident occurred about 3 years ago</td>
<td>CON - Not clear why she said yes here. Initially was thinking about people collecting for charity. NONCON - someone pretending to be you by using your card</td>
<td>A</td>
<td>NONCON</td>
</tr>
<tr>
<td>(R2) 5</td>
<td>A number of online transactions were made using the participant’s credit card details without her permission or knowledge. She discovered this when her bank contacted her about them.</td>
<td>CMACT – thought about her credit card details were stolen NONCON – thought about her card details being used to buy things without her permission</td>
<td>A</td>
<td>NONCON</td>
</tr>
</tbody>
</table>

<sup>45</sup> It should be noted that the cognitive interview did not include victim checklist questions, which are designed to assist with coding and as such the coding suggestion presented is a ‘best guess’ based on the information available.
<table>
<thead>
<tr>
<th>Incident</th>
<th>Incident description</th>
<th>Rational for answering multiple screener Qs about same incident</th>
<th>Q version</th>
<th>Which screener Q should have been coded ‘yes’</th>
</tr>
</thead>
<tbody>
<tr>
<td>(R2) 6</td>
<td>Participant’s bank card was cloned and used to make cash withdrawals from her account. She discovered this when her bank contacted her to confirm the transactions. She answered yes to both CMACT &amp; NONCON about the same incident</td>
<td>CON – thought Q was asking if she had been a victim of an online crime. She felt she had been tricked because her card had been cloned. NONCON – realised at NONCON this was a better fit for the incident</td>
<td>B</td>
<td>NONCON</td>
</tr>
<tr>
<td>(R2) 10</td>
<td>The participant receives numerous fraudulent emails saying she has won a prize or such like and needs to give her bank details so it can be paid into her account. Thinks the fraudsters must have gained access to personal details to have her email address. She says she ‘generally’ does not respond. Answers yes to CON and CMACT in relation to these emails.</td>
<td>CON – thinking about email she received that were trying to ‘con’ her into providing person information CMACT – thinking about the fact the fraudsters had obtained her email address and other information about her such as the internet sites she tends to visit. Sees this as an infringement of her privacy</td>
<td>B</td>
<td>Not enough evidence to demonstrate a crime. Not a CON as no response to email. Not a CMACT as no evidence that personal details were taken</td>
</tr>
<tr>
<td>(R2) 13</td>
<td>She received an email which appeared to be genuine saying that she had bought 9 tickets for a performance of Peter Pan and that she should open the attachment to view and print the tickets. It also provided links to click to the theatre. The email contained the last 4 numbers of a MasterCard that she had once had. At first she thought that this was CMACT – thinking of her email address being stolen, She wonders if this is the right place to say ‘yes’ NONCON – thinking about her old credit card details being included in the email.</td>
<td>CMACT – no evidence that money was taken from account but credit card details had been obtained.</td>
<td>A</td>
<td>CMACT</td>
</tr>
</tbody>
</table>
## Figure B2.2 Circumstances in which ‘double-counting’ arose

<table>
<thead>
<tr>
<th>Incident</th>
<th>Incident description</th>
<th>Rational for answering multiple screener Qs about same incident</th>
<th>Q version</th>
<th>Which screener Q should have been coded ‘yes’\textsuperscript{45}</th>
</tr>
</thead>
<tbody>
<tr>
<td>R2 14</td>
<td>Someone used his credit card to buy an air line ticket without his permission. The incident happened in last 5 years. He answered yes to both CMACT &amp; NONCON for same incident. He was not sure what the difference between CMACT &amp; NONCON was.</td>
<td>CMACT – thinking about the fact his card details must have been stolen. NONCON – thinking about the use of his card details without his permission. The Interviewer did not read ‘apart from anything you have already mentioned’ as part of the question.</td>
<td>A</td>
<td>NONCON</td>
</tr>
<tr>
<td></td>
<td>a mistake and tried to ring the theatre but the line was constantly engaged. Next she went to the bank to stop any payment being made and it became apparent that this was an internet crime to try and get her to open the attachments, which would install viruses. She answered yes to both CMACT &amp; NONCON for same incident.</td>
<td>The interviewer forgot to read ‘apart from anything you have already mentioned’ as part of the question.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
There appear to be several factors contributing to this apparent double-counting:

- the interviewer not reading out the text in brackets - ‘apart from anything you have already mentioned’ - before reading the screener question (this related to one interviewer);
- participants answering ‘yes’ to the first question that seemed to cover the incident, not realising that they would be asked further screening questions that might better describe the incident; and
- for CMACT and NONCON, participants reporting the theft of bank/card details and the use of this information as two separate incidents when in fact they were two steps involved in one incident.

Several remedies are proposed.

- At the start of the new questions include a short introduction that tells participants that they are now going to be asked four questions about their experience of fraud and computer misuse.
- Show these 4 types of crime on a show card
- In CAPI the bracketed text ‘Apart from anything you have already mentioned’ is programmed only to appear if the participant has answered ‘yes’ to any of the preceding screening questions.
- The inclusion of checks on the coding of CMACT and NONCON (see section 4.1) with guidance on the priority order for coding when incidents are linked.
B3 Victim form findings

In the CSEW, participants who report that they have experienced one or more incidents of any crime type in the screener questions are then asked to complete a Victimisation Module for each of the incidents, up to a maximum of six. For cognitive testing purposes participants were asked to answer this module about the most recent incident they had experienced, if there had been more than one within each type.

B3.1 Date of incident

The existing questions on the date of incident were tested to assess if victims of confidence and non-confidence fraud, theft of personal data or interference with internet or computer access would be able to answer these questions. The questions tested were as follows:

**DATE OF INCIDENT (FOR A SERIES OF INCIDENTS)**

**DATESERA [ASK IF SERIES OF SIMILAR INCIDENTS]**

You mentioned a series of [ENTER NUMBER FROM CNUMSER_______] similar incidents of someone tricking or deceiving you to obtain money or goods since the **first September 2013**. When did these incidents happen? CODE ALL THAT APPLY

1. Before the **first of September 2013**
2. Between **September and November 2013**
3. Between **December 2013 and February 2014**
4. Between **March and May 2014**
5. Between **June and August 2014**
6. Between the **first of September 2014** and the present

**NQUART1-5**

How many incidents of this kind happened between…. 

a) … **September and November 2013** NO. [ ]

b) … **December 2013 and February 2014** NO. [ ]

c) … **March and May 2014** NO. [ ]

d) … **June and August 2014** NO. [ ]

e) …the **first of September 2014** and the present NO. [ ]

104 NatCen Social Research | Developing questions on fraud and cybercrime for the CSEW
MTHRECIIn [ASK IF MORE THAN ONE INCIDENT IN A QUARTER AT NQUART]

In which month did the most recent of these incident(s) happen?

INTERVIEWER EXPLAIN: IF PART OF SERIES, THE FOLLOWING QUESTIONS REFER TO THE MOST RECENT INCIDENT IN SERIES.

CODE MONTH

DATE OF INCIDENT (FOR SINGLE INCIDENTS)

MTHINC2  [ASK IF SINGLE INCIDENT]

You said that, since the first of September 2013, you had an incident of [CRIME TYPE … someone tricking or deceiving you to obtain money or goods. In which month did that happen?

1. September…13 September – GO TO CHKREC12
   Don’t know → ASK QTRINCID

QTRINCID  [ASK IF MTHINC2=DK]

In what quarter did the incident happen? Was it ...

1. Before the first of September 2013
2. Between September and November 2013
4. Between March and May 2014
5. Between June and August 2014
6. Between the first of September 2014 and the present
7. Don’t know

CHKREC12

And can I just check, did the incident happen before or after the first of September 2013?

1. Before the first of September 2013
2. After the first of September 2013

These questions were included in both rounds one and two of testing and findings relate to both rounds.

Participants were generally able to provide an answer. Even if they were unable to recall the exact month, they were able to indicate the time period in which the incident took place. Facilitators to recall included:

- a recent incident;
• significant life events or times of the year around the same time as the incident;
• the incident had a significant impact on the participant;
• paperwork about the case; and,
• the calendar provided by the interviewer.

Some difficulties in recalling the date were identified. Those participants who had experienced an incident more than 12 months ago, in some cases found it difficult to recall the exact date. This problem would not occur in the actual survey. In addition, one participant who reported having had a virus found it difficult to provide an exact date when incidents of phishing occurred as he was uncertain when they had been identified by his anti-virus software. (If should be noted that this incident falls outside the intended scope of the new screener question on interference with computer and internet access). Another participant, who said that she had experienced theft of personal data, described how while she knew the date she became aware that her personal details had been obtained she did not know when someone ‘got hold of those details’. Lastly there was also a view that asking people to recall the timeframe could be a difficult for those trying not to think about the experience.

The date that was actually reported varied. The date the incident occurred and the date when the participant became aware that the incident had occurred were reported. Factors influencing which date was reported were:

• whether the participant knew when the incident had actually occurred; and
• the type of incident.

These factors were interlinked. Those who said that they had experienced a confidence fraud, theft of personal data or interference with computer or internet access incident reported when the crime had taken place. For example, one participant referred to the transfer of money connected with the offence, rather than when he realised he had been a victim 3-4 weeks later and contacted the police. In contrast, participants who said that they had been a victim of non-confidence fraud referred to when they became aware of the incident. For example, one participant gave the date she was informed by the bank that money had been taken out of her account. One interpretation is that participants gave a time reference point based on their own involvement with the incident, and in cases of non-confidence fraud it can be difficult to know when personal details were actually stolen.

There were cases where there was a very short timeframe between when the incident happened and they became aware of it. In such cases, both points (when it occurred and when they became aware) were included in responses as both dates fell within the same month. For example, one participant had ordered an item on the internet and realised the website was fake when he placed the order.
B3.2 Description of incident

Participants in both rounds were asked the current CSEW question, DESCRINC, which asks:

Before I ask you a number of detailed questions to enable us to classify exactly what happened can you tell me, very briefly, about the incident?

IF PART OF A SERIES RECORD THE MOST RECENT OCCASION.

PROBE FOR DETAILS OF NATURE AND CIRCUMSTANCES OF INCIDENT. (FOR EXAMPLE, WHO WAS THE VICTIM, WHO WAS THE OFFENDER, WHERE DID IT HAPPEN, WHAT DID THEY DO, HOW DID THEY FIND OUT ABOUT THE INCIDENT?)

All participants were able to provide a description of the incident. The level of detail report varied, and some participants added more detail or points of clarification when the interviewer re-read their summary, which is the intention. Participants generally felt that the summary was a fair account of the incident and agreed with it.

In the actual survey additional incident checklist questions are asked, see Figure 4.2, to ensure that sufficient information is captured to enable the incident can be coded to the Home Office coding rules. The cognitive interviews undertaken as part of this study did not include a set of incident check questions and incidents were not coded. It is therefore not possible to comment on whether incidents captured in the cognitive interview could be successfully coded. However, in Chapter 5 we recommend that the quality of the incident descriptions for the new screener questions be assessed as part of a larger field test.

B3.3 Where the incident happened

Round one tested the existing CSEW questions that establish where the incident happened, VICTAREA and WHERHAP, with some modification. In addition a new question, WHERELIVE was included. This approach was based on that taken by the Scottish Crime and Justice Survey (see Appendix A, section A4.1.3). These questions are shown below.

CIRCUMSTANCES OF INCIDENT
VICTAREA    [ASK ALL]

Can I just check, did it happen in this area (within 15 minute walk of here)?

1. Yes ➔ GO TO WHYHAP3
2. No ➔ ASK WHEREHAPP
3. (spontaneous) Don’t know ➔ ASK WHEREHAPP
WHERHAPP [ASK IF VICTAREA = NO OR DK/REF]

Did it happen in England or Wales or did it happen somewhere else?

1. England or Wales } → GO TO WHYHAP3
2. Elsewhere (not online) → ASK WHERELIVE
3. On-line, over the internet → ASK WHERELIVE

IF INCIDENT HAPPENED ONLINE (WHERHAPP CODE 3)
WHERLIVE

And where were you living when this occurred? 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)

Findings for these questions are based on five cases where round one participants indicated they had been victims of fraud, theft of personal data and interference with computer and internet access.

There was some inconsistency noted in the way in which VICTARE was answered, with participants either answering in relation to where they were when they found out about the incident or about where the incident took place. Figure B3.1 summarises the rational for answers to VICTARE and the answer given to WHEREHAP.

All participants answered ‘no’ to VICTAREA (whether the incident happened in the participant’s local area). Some participants felt that it was difficult to answer and only provided a response after the interviewer repeated it.
Figure B3. 1 Summary of rational for answer to VICTAREA & WHEREHAP

<table>
<thead>
<tr>
<th>Incident</th>
<th>VICTAREA</th>
<th>Rational</th>
<th>WHEREHAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident 1</td>
<td>No</td>
<td>Even though found out about incident at home had been told fraudster lived in another city in England and Wales</td>
<td>England &amp; Wales</td>
</tr>
<tr>
<td>Incident 2</td>
<td>No</td>
<td>Even though found out about incident at home she had been told by the bank that her card had been cloned at an ATM in another town she had visited. The cloned card was used in the US</td>
<td>England &amp; Wales</td>
</tr>
<tr>
<td>Incident 3</td>
<td>No</td>
<td>She thought the company were based in another part of England and Wales</td>
<td>England &amp; Wales</td>
</tr>
<tr>
<td>Incident 4</td>
<td>No</td>
<td>Unclear of rational used</td>
<td>Online</td>
</tr>
<tr>
<td>Incident 5</td>
<td>Yes</td>
<td>She found out about the fraud when she was at home, although she knew it had taken place somewhere away from her area, in London</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Based on the findings and recommendations from Round 1 the questions VICTAREA and WHEREHAPP were not asked at Round 2, and instead this section began with WHERLIVE – ‘And where were you living when this occurred?’ The rational for this strategy is described in section 2.2.

Testing found that participants were generally able to provide an answer to this question. Those that found it relatively easy to answer and were confident in their response easily recalled their physical location at the time. For example, one incident involved the delivery of goods and an email both received at the participant’s home address, and in another case relevant documentation reinforced the participant’s confidence in her response.

However, not all participants found the question easy to answer. This was because they had moved around the time of the incident or over the timeframe in which similar incidences had occurred. Difficulty in responding was compounded by a shift in thinking about the most recent and former incidences, and when information about the incident was received via mobile phone. In addition, one participant found the process of answering the question stressful as it encouraged him to think about incidents before the most recent one, while another participant questioned its purpose, as the incident had taken place abroad.
B3.3 Why the incident happened

At rounds one and two participants were asked the CSEW victimisation module question WHYHAP3. This question asks:

Can you tell me why you thing this incident happened?

Verbatim responses were record at this question and the cognitive interview explored participants’ feelings about being asked for this information.

The question was answered in one of three ways:

- those who placed the onus on themselves (this included victims of confidence fraud, theft of personal data and interference with computer and internet access);
- those who placed the onus on the offender and nature of the offence (this include victims of non-confidence fraud, theft of personal data and interference with computer and internet access); and,
- those who ‘did not know’ (these were all cases of non-confidence fraud) because they did not know how it had been committed. This suggests that some participants interpreted the question as asking about ‘how’ the incident was committed rather than ‘why’.

Some participants would be happy to answer this question if asked in the survey, and found it a relatively easy question. They felt they understood how the incident occurred or that there was nothing personal about it. In addition, it was hoped that the findings may help the Criminal Justice System respond appropriately to similar incidences in the future and ensure such crimes do not happen to others.

However, not all participants found this question straightforward. One participant who tended to lapse into describing the circumstances for all of the incidences he had experienced, did so again instead of focusing on the most recent confidence fraud. Some participants who said that they had experienced a non-confidence fraud also found this question difficult to answer because they did not know whether the question was asking about how or why the incident took place, or did not know how to respond when for example, the incident had not physically affected them.

Further, some viewed this as a sensitive question, especially when they felt embarrassed or uncomfortable about the incident. One view was that asking ‘why an incident happened’ implied an individual was at fault. The fact that some participants placed the onus on themselves when asked to describe why it took place may add further evidence to this. This requires careful consideration, as noted Appendix A; many victims of fraud feel that they are to blame for the offence. It is vital that the CSEW does not perpetuate such feelings among those taking part in the survey and when reporting the results. Lastly, another view was that this was a ‘silly’ question. The participant felt that the reason that the incident occurred was obviously because someone else was trying to steal his money. He went onto explain how if asked such a question in a survey he would want to terminate the questionnaire at this point.
B3.4 Whether the devices involved were solely for personal use

It was agreed with ONS that a new question should be designed and included at round two, which established whether theft of personal data or interference with internet and computer access involved a device used for the participant’s own personal use. The question asked was:

**PERUSE**

You mentioned that someone had stolen your information or details. Did this happen from a computer enabled device that you used for your own personal use?

Three participants were asked this question. One participant answered yes. He found the question easy to answer and provided examples of devices which were only for his personal use. The other two participants answered don’t know (one initially said ‘no’ but then immediately changed his mind). They may have misinterpreted the question because they explained how it was difficult to answer as they did not know how someone had obtained their details and how the incident had occurred.

B3.5 Location of incident

The location of the incident is currently captured in the CSEW at question WHERE1, which asks:

*Where did this incident happen?*

The question was included in rounds one and two of testing and we report findings from both rounds by the type of incident participants experienced. In the CSEW the question includes a set of precoded answer options that the interviewer uses to code the participants’ answer. In testing, verbatim responses were recorded.

Testing found that participants who said that they had been a victim of a confidence fraud were generally able to answer this question. However, the reasons underpinning the responses of ‘online’ and/or ‘at home’ varied. When participants referred to where the crime was committed/incident occurred they said online. In one case this was felt to be the ‘easy’ answer option as physically the perpetrators may be located anywhere. When participants referred to how they had become involved in the fraud/where they were when it happened they said at home, and for some this applied to both where the offence was committed and where they were at the time. One participant felt that she had given this response as she had carried on her train of thought from the previous question. A further response was both online and at home. Lastly, one participant who said they were a victim of a confidence fraud said that they technically ‘did not know’ how the perpetrator(s) had attempted to use his information, however this question should have been coded in the screener section as a non-confidence fraud instead.

Participants who said they had been a victim of theft of personal data or interference with internet or computer access were also able to answer and responded in one of
three ways. They either provided the location where they first became aware of the incident (home), where it was committed (cyberspace), or both where they became aware and where the crime was committed (home and abroad).

Lastly, participants who said that they had been a victim of non-confidence fraud were found to have particular difficulty with this question (as noted above for the case incorrectly coded at the screener). They were unsure how the perpetrator(s) had accessed and used their personal information. Responses included the internet, the city where the crime took place, or that they simply did not know.

**B3.6 Method of entry**

A new question was tested at rounds one and two, HACK, which was asked victims of non-confidence fraud at rounds one and two. It asked:

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

Uncertainty around how the incident occurred and whether the perpetrators involved had used this type of information to gain access to account(s); meant participants answered ‘don’t know’ or ‘no’. While some found it relatively easy to answer, others had difficulty because they were unable to comment on the nature of the information held by the perpetrator(s). In addition, one participant described how the incident had lacked face to face contact with the perpetrator, but he had willingly transferred money over because it was a confidence trick. Another participant had an idea about how the perpetrator had gained his details, yet was unsure how he had been targeted.

**B3.7 Cost of incident (money and time)**

Questions on the costs of crime, both money and time were tested. These questions were modified from existing questions contained in the CSEW in different modules of the questionnaire. At round one the following questions were tested.

**FRLOSS**

[Still thinking about this most recent incident] Did you lose any money? 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. Yes – ASK FRLOSS2
2. No – GO TO CMACHK
FRLOSS2

How much money 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 (i.e. all money was refunded)
2. Less than £1
3. Up to £5
4. Up to £10
5. £1,000 or more
6. Not yet resolved

ASK FRLOSS3

GO TO CMACHK

FRLOSS3 [ASK IF FRLOSS2 CODED 5 – LOST £1000 OR MORE]

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

ENTER AMOUNT TO NEAREST £1,000

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

TRIGHT

How much time, overall, do you estimate you spent dealing with this incident to put things right? If it is still on-going 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

Money involved

Participants provided details about the amount of money lost and found this a relatively easy process. Reasons included being able to recall the amount spent on a credit card statement or the amount of money transferred to the offender. One participant also liked how the answer categories at question FRLOSS2 (How much money, if any, did you personally lose?), were broad categories rather than asking for an exact amount. Other participants reported that they had not lost any money. They may have received refunds and therefore answered the question correctly by saying they did not personally lose any money.

These questions were modified ahead of round two. FRLOSS was dropped and FRLOSS2 amended so that it asked How much money, if any, did you personally lose? Answer option one was also modified to 1. None OR all money was refunded.

Participants were able to answer the questions on the costs of the crime in terms of money, especially if they had supporting documents which helped them recall the information. However, unlike in Round 1, one participant would have preferred to provide specific amounts rather than choose one of the broader answer categories. In addition, not all participants felt that they were immediately clear about what amounts should be included at this question, and it only became apparent when the interviewer re-read the question. One participant initially wondered whether a cancelled transaction included a refund; however this did not affect his response of zero. After thinking about this he then went on to define that a refund would have involved money going out of his account and then being paid back in. Further, not all participants automatically included additional charges or costs unless they were specifically probed to do so, and one participant felt it may be helpful to include examples of additional costs in the question wording. Finally, not all those taking part in the cognitive testing were at a stage where they could calculate additional costs as the matter was not yet resolved and this situation should be captured in a new answer option.

Time involved

The time involved questions remained unchanged between rounds one and two. When asked about the time it had taken to resolve the incident one participant reported that it was unresolved. When asked about how much time overall had been spent dealing with the incident so far, responses ranged from one hour to over 15 hours. One participant found this question difficult to answer. Although the incident happened outside of the 12 month reference period, her feedback indicates how she was unclear whether the question was asking for a timeframe starting from when the incident began to when it ended, or about the time she had actually spent addressing it.

There was some evidence of under-reporting. For example, a participant described how she had initially only thought about the phone calls made in relation to the incident, but not the waiting time for the replacement card to arrive. In addition there was feedback about the categories and how they jumped from a couple of hours to a couple of days. This also meant that the answer given could be an underestimation. For
example, a participant spent 4-5 hours but selected a couple of hours as this was the most accurate for him.

Finally, the question was difficult to answer where an ongoing case was looked like it was never going to be resolved. It was felt that one way to address this would be to have a ‘never resolved’ answer category.

B3.8 Impact of incident

Finally, existing questions on the impact of the incident on the victim were tested to assess their acceptability. The same set of questions was tested at both rounds one and two and is listed below.

**EMOTREAC**

SHOW CARD 1

Many people have emotional reactions after incidents in which they are victims of crime. Looking at this card did you PERSONALLY have any of these reactions after the incident?

1. Yes – ASK WHEMOT
2. No – GO TO IMPACT2

**WHEMOT** [ASK IF EMOTREAC = YES]

SHOW CARD

Which 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. Other (SPECIFY)
HOWAFF1  [ASK IF EMOTREAC = YES]

Overall, how much were you affected? Were you affected ...READ OUT

1. Very much
2. Quite a lot
3. or just a little?

Participants were able to provide answers to the set of ‘Impact’ questions and some felt fine answering these. They felt such questions were to be expected, the wording sat well with their own experience, and they had received information from Victim Support. However, there was a view that the questions could be difficult to answer if they were about a violent or traumatic experience, and some participants did report feeling embarrassed or finding it difficult to describe how they felt as this was not something they generally discussed with others.

Types of emotional reactions after incidences

At the moment the CSEW firstly asks whether participants have had any emotional reactions on a show card (EMOTREAC), and then asks which of the listed reactions they have had (WH杖MOT). Interviewers suggested that the questions ‘EMOTREAC’ and ‘WH杖MOT’ be combined and ask ‘Which, if any, of these reactions did you personally have, after the incident’. While participants were willing to provide an answer to this some other reactions to include were identified. These included: feeling vulnerable, surprised, foolish and embarrassed, frustrated, feeling deceived and alone, and attempted suicide. The range of emotional reactions associated with fraud and cyber crime, means that an ethical approach to asking such questions, and having the necessary support mechanisms in place is vital. In addition, a participant felt that code (8) ‘crying/tears’ was too specific as people may be reluctant to admit to this, and a preferable code would be a more general term such as ‘emotional’.

In addition to the overall findings above there was specific feedback which is helpful to report here. One participant went through the list on the show card, speaking about each reaction in turn. However, the interviewer felt that his response of a ‘yes’ at ‘EMOTREAC’ may have been prompted because he saw one of the codes first (7 – difficulty sleeping). It was felt that it may be beneficial to have a ‘none of these’ option at the end of the show card, which would be necessary anyway if the two questions are combined as suggested above. Furthermore, interviewer feedback described how he felt one participant thought about his reaction during the incident and while he was waiting to know whether he had been a victim of a crime or not, rather than ‘after the incident’ as implied in the question wording.

How much people were affected after incidents

Those who reported an emotional reaction after the incident were then asked whether they were affected ‘very much’, ‘quite a lot’ or ‘just a little’ (HOWAFF1). Participants were generally able to provide a response to this question. However, one participant found it difficult to choose between the answer categories ‘very much’ and ‘quite a lot’. She could not decide whether to base the answer on her initial reaction when she became aware an email she had received was actually an attempt at ‘internet crime’, or
her subsequent feelings once she had established no harm had been done i.e. she realised no money had been taken and that she had not opened any attachments which contained viruses.

Things which may have happened as a result of the incident

Finally, participants were asked whether any of the things listed on a show card happened to them as a result of the incident (IMPACT2). The cognitive testing found that some people had no difficulty answering this question and felt the set of answer categories were comprehensive. However, ‘other’ responses included going to the bank to ascertain whether there had been any use of the cards and to ask their advice; very careful monitoring of emails, anything online; and gradually replacing passwords. In addition, an incident had ruined a participant’s credit history and he could no longer get finance for a car or a mortgage.

There was also some feedback on the specific codes for this question. Firstly, a participant described how they had checked their existing security measures were working, rather than code 8 -taking additional precautions, and had only realised after probing that they had not suffered any financial loss because the money had been refunded. For code 15 (I use the internet less/I am more cautious online), one view was that the code referred to two separate and distinct things and should be split into two, especially as one could use the internet more and still be more cautious online.

Lastly participants thought about code 17 – ‘I no longer use the internet in public places’, and what they understood by this phrase. Participants’ descriptions included references to public places where the internet is accessed, for example internet cafes, public transport, at work, educational establishments and in the bank. They also described a range of types of internet/web based activity including data roaming, Wi-Fi, hotspots, and a cloud. Types of devices included other people’s computers and personal tablets. One participant debated whether he should also include his phone accessing the internet but decided against this. In addition, a participant mentioned the physical threat of someone looking over her shoulder when using an internet enabled device in a public space.

B3.9 Other issues

At a few points in this chapter participants’ experiences and reactions have prompted us to think about the best ethical approach when asking such questions. When asked to reflect on their general experiences of the survey questions some participants described how this is a ‘tricky’ subject area when an individual has been a victim and especially if they are trying not to focus on it or ‘block it out’. Ethical considerations for administering the questionnaire were also raised and specifically whether any questions were more suitable for a self-completion format, and ensuring participants were directed to the appropriate form of help and support. Other more general comments related to decreasing the number of overall questions, making some questions shorter, providing examples of the aspect of the experience the question was trying to identify, and being able to go into the specifics of the incident earlier on in the questionnaire.
Appendix C. Test materials

Test questions and cognitive probes

Rounds 1 and 2, versions A and B

Recruitment documents
Stage 1: Introduction

Aims: To introduce the study and collect informed consent.

- Thank participant

- Introduce yourself and NatCen Social Research. We are an independent, not for profit, research organisation.

- Explain we are doing this study on behalf of the Office for National Statistics. The ONS are responsible for the Crime Survey for England and Wales. This survey collects information about people’s experience of crime and the criminal justice system. The survey is run every year and you kindly took part in 2013.

- Some new questions have been developed and we would like to try these out, to see whether they are working as intended. During this interview you will be asked some CSEW survey questions, including some new questions. I will explore how you went about answering them to see if the questions are clear and appropriate.

- Taking part is entirely voluntary – this isn’t a ‘test’ and there are no ‘right or wrong’ answers.

- Stress confidentiality. The findings from all the interviews will be written up as report. We never include the names of the people who take part in our reports.

- Explain that you will be recording the interview so that you don't have to make lots of notes during the interview.
  
  o Recorder is encrypted and only the research team at NatCen will have access to the recordings.
  
  o Check this is OK with the participant.

- The interview will last around 60 minutes. Everyone who takes part receives a £20 high street voucher to thank them for their time.

- Ask whether participant has any questions before you start.
Stage 2: Background

Aims:
- To ‘warm participant up’.
- To double-check screening details are correct.
- To get background information on participant’s use and confidence in using the internet and computers/tablets/smart phones.

- Explain before we ask the new survey questions would like to collect a little bit of background about the participant

- Double check details from screening.

- Explore:
  - Who lives with participant as part of their household?
  - How long lived at this address.
  - Employment status

- Use of computers/internet
  - Frequency of using internet
    - How often they use internet
    - What mainly use internet for
  - Confidence in using computers/internet
  - Devices used to access internet
    - Computer/tablet/mobile/other
    - Locations where access takes place (home, work, library, public space)
    - Device shared with anyone else
Stage 3: Think aloud training

Aim:
- To explain the ‘Think Aloud’ process and to encourage thinking aloud behaviours.
- Explain that you are going to ask the participant some survey questions. Whilst they try to answer these questions you want to know their first impressions of these questions and what they are thinking about.
- Explain the ‘Think Aloud’ technique using a scenario of your choice (the windows example is given below but you are welcome to use an alternative). Part of this is to get the participant used to talking.

Windows example: I would like you to have a practice at ‘thinking aloud.’ I am going to ask you a question and I want you to tell me what you are thinking as you work out your answer…

‘How many windows are there in your home?’ Please describe what you are thinking as

- Encourage think aloud through rest of interview…
### Stage 4 CSEW SCREENER QUESTIONS

**Aims of cognitive testing**
- to get first impressions of the new screening questions
- to explore understanding of the new screening questions
- to explore whether fraud or cybercrime are being picked up in existing screener questions
- to explore any difficulties

** Protocol**
- **Ask all screening questions, encouraging participants to think aloud as they answer. Record their answers at each question.**
- **Probe on the following questions once all screening questions are complete. Remind participant of question and their response**

#### Intro

**SHOW RESPONDENT LIFE EVENTS CALENDAR**

Before asking you about crimes or incidents that may have happened to you over the last 12 months I’d like to give you a calendar. I’d like you to keep this in front of you when answering the next part of the interview.

If at any stage you are unsure about whether or not something happened in the last 12 months you may find looking at the calendar will help to prompt your memory.

**INTERVIEWER:** **MARK OFF THE CORRECT 12 MONTH REFERENCE PERIOD ON THE CALENDAR, THAT IS SINCE THE FIRST OF [‘DATE’] UNTIL PRESENT, AND HAND TO RESPONDENT**

#### Intro1

I’m now going to ask you about things that may have happened over the last 12 months, that is since the **first of August 2013**, in which you may have been the victim of a crime or offence. This doesn’t mean that crimes that may have happened before this time are unimportant, but we want to build a picture of just the last 12 months so we can measure how people’s experience of crime changes from one year to the next.

I am only concerned with incidents that have happened to YOU PERSONALLY [or to people who are NOW members of your household].

I don’t just want to know about serious incidents – I want to know about small things too.

**Motstole**

In the time since **first of August 2013**, have you or anyone else now in your household had anything stolen off [your/their] vehicle or out of it (parts of the vehicle, personal possessions or other things)?

1. Yes – **ASK NMOTSTOL**
2. No – **GO TO YRHOTHEF**

**NMOTSTOL [ASK IF MOTSTOLE = YES]**

How many times has this 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

YRHOTHEF   [ASK ALL]

During the last 12 months, that is first of August 2013, has anyone GOT INTO this house/flat without permission and STOLEN or TRIED TO STEAL anything?

1. Yes – ASK NYRHTHEF
2. No – GO TO YRHOSTOL

NYRHTHEF   [ASK IF YRHOTHEF = YES]

How many times has this 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

YRHOTRY   [ASK ALL]

[Apart from anything you have already mentioned], in that time have you had any evidence that someone has TRIED to get in without permission to STEAL or to CAUSE DAMAGE?

1. Yes – ASK NYRHOTRY
2. No – GO TO YRHOSTOL

NYRHOTRY   [ASK IF YRHOTRY = YES]

How many times has this 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

YRHOSTOL   [ASK ALL]

[Apart from anything you have already mentioned], in that time was anything STOLEN out of your house/flat?

1. Yes – ASK NYRHOSTO
2. No – GO TO INTRO2

NYRHHOSTO   [ASK IF YRHOSTOL = YES]
How many times has this 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
INTRO2

The next few questions are about things that may have happened to you PERSONALLY [not the other people in your household] or that you discovered over the last 12 months, that is since the first of August 2013, in which you may have been the victim of a crime or offence. Again, I only want to know about things that have happened in the period marked on the calendar, so we can build a picture of crime in the last 12 months.

Please include anything that happened to you during that time – at home, in the street, at work, in a shop, in a park, on a train, online or anywhere else.

PERSTHEF  [ASK ALL]

Since the first of [*DATE*], [apart from anything you may have already mentioned], was anything you were carrying stolen out of your hands or from your pockets or from a bag or case?

1. Yes – ASK NPERSTH
2. No – GO TO OTHTHEF

NPERSTH  [ASK IF PERSTHEF = YES]

How many times has this 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

OTHTHEF  [ASK ALL]

And [apart from anything you have already mentioned], in that time has anything (else) of yours been STOLEN, from a cloakroom, an office, a car or anywhere else you left it?

1. Yes – ASK NOTHTHEF
2. No – GO TO DELIBDAM

NOTHTHEF  [ASK IF OTHTHEF = YES]

How many times has this 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

DELIBDAM  [ASK ALL]

And [apart from anything you have already mentioned], in that time has anything else of yours been DELIBERATELY DAMAGED or tampered with by vandals or people out to steal?

1. Yes – ASK NDELIBDA
2. No – GO TO THREVIOL

NDELIBDA  [ASK IF DELIBDAM = YES]

How many times has this 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

THREVIOL  [ASK ALL]

And [apart from anything you have already mentioned], in that time, has anyone THREATENED to damage things of yours or THREATENED to use force or violence on you in any way that actually frightened you?

1. Yes – ASK NTHREVIO
2. No – GO TO CON

NTHREVIO  [ASK IF THREVIOL = YES]

How many times has this 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
**CON**

[Apart from anything you have already mentioned], in that time has anyone...obtained money or goods from you under false pretences, using whatever means?

1. Yes – ASK NCON
2. No – GO TO NONCON

**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

**NONCON**

[Apart from anything you have already mentioned], in that time has anyone used or tried to use your personal information or account details in any way to buy goods or services without your permission or knowledge or to pretend to be you?

1. Yes– ASK NNONCON
2. No – GO TO CMACT

**NNONCON**

[ASK IF NONCON=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__________

**Version B**

**CON**

[Apart from anything you have already mentioned], in that time has anyone...conned you out of money or goods, in person or online?

1. Yes – ASK NCON
2. No – GO TO NONCON

**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

**NONCON**

[Apart from anything you have already mentioned], in that time has anyone used or tried to use your personal information or account details in any way to buy goods or services without your permission or knowledge or to pretend to be you?

1. Yes– ASK NNONCON
2. No – GO TO CMACT

**NNONCON**

[ASK IF NONCON=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__________
CMACT

[Apart from anything you have already mentioned], in that time has anyone… stolen your personal information or details, or installed unwanted programs, including viruses, on any internet-enabled devices you use for personal use?

1. Yes- ASK NCMACT
2. No – GO TO PROBES

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

CMACT

[Apart from anything you have already mentioned], in that time has anyone… accessed information held digitally about you without your permission, altered your data without your permission or installed unwanted programs, including viruses, on any internet-enabled devices you use for personal use?

1. Yes- ASK NCMACT
2. No – GO TO PROBES

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

NOW ASK COGNITIVE PROBES OVERLEAF
Screening probes

Con probes
- How did you go about answering this question?
- In your own words what do you think this question is asking? Probe for understanding of:
  - ‘under false pretences’ / ‘conned’
  - ‘goods’
  - ‘whatever means’ / ‘in person or online’
  Explore what types of crimes participant was thinking about here.
- How easy or difficult did you find this question to answer? Explore reasons
- How did you feel about answering this question?
- What time period were you thinking about when answering this question? From when to when?
- How confident are you that your answer is accurate, where 0 is not at all confident and 10 is completely confident?

NCON probes
- How did you go about answering this question?
- Check: Did participant receive multiple communications about the same con/scam?
- How easy or difficult was it to answer this question? Explore reasons

NONCON probes
- How did you go about answering this question?
- In your own words what do you think this question is asking? Probe for understanding of:
  - ‘used’, ‘tried to use’
  - ‘personal information’ / ‘account details’
  - ‘pretend to be you’
  Explore what types of crimes participant was thinking about here
- How easy or difficult did you find this question to answer? Explore reasons
- How did you feel about answering this question?
- What time period were you thinking about when answering this question? From when to when?
- How confident are you that your answer is accurate, where 0 is not at all confident and 10 is completely confident?
**NNONCON probes**

- How did you go about answering this question?
- How easy or difficult was it to answer this question? Explore reasons
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

**CMAT Probes**

- How did you go about answering this question?

- In your own words what do you think this question is asking? Probe for understanding of:

  - ‘stolen’ / ‘accessed’
  - ‘your personal information or details’ / ‘information about you’, ‘held digitally’
  - ‘unwanted programs’ other than viruses
  - ‘internet enabled devices’
  - devices ‘you use for personal use’
  Explore what types of crimes participant was thinking about here

- How easy or difficult did you find this question to answer? Explore reasons

- How did you feel about answering this question?

- What time period were you thinking about when answering this question? From when to when?

**NCMACT probes**

- How did you go about answering this question?
- How easy or difficult was it to answer this question? Explore reasons
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.
If participant said they had anything stolen at any of the earlier screening questions:

MOTSTOLE, YRHOSTEF, YRHOSTY, YRHOSTOL, PERSTHEF, OTHTHEF = yes

Probes

- Explore whether any personal information was stolen or lost? By personal information we mean any information that could be used to obtain goods or services without the participant’s permission or (could) enable someone to gain access to personal information about the participant (such as accounts, records etc).

- Explore whether the participant was reporting that the incident happened in the last 12 months or that the participant discovered that the incident had occurred, in the last 12 months. If the latter explore when the incident actually occurred.

- (IF NECESSARY) Did you include any incidents at this question that you included at CON, NONCON or CMACT? Explore which incidents included at which Q and why included at subsequent question (i.e. mentioned more than once)?

If participant said they had something damaged or someone threatened to damage something of theirs:

DELIBDAM OR THREVIOL =yes

Probes

- Explore what was damaged or threatened to be damaged.

- Explore whether the participant was reporting that the incident happened in the last 12 months or that the participant discovered that the incident had occurred, in the last 12 months. If the latter explore when the incident actually occurred.

- (IF NECESSARY) Did you include any incidents at this question that you included at CMACT? Explore which incidents included at which Q and why included at subsequent question (i.e. mentioned more than once)?
• CHECKING WHETHER ANY INCIDENTS ARE A SERIES

INTCHK

IS CON=YES, NONCON=YES OR CMACT=YES AND NCON>1, NNONCON>1 OR NCMACT>1?
1 YES - ASK INTRO 4
2 NO, CON, NONCON OR CMAC=YES BUT NCON, NNONCON OR NCMACT=1 GO TO INTVIC (p19)
3 NO, CON, NONCON OR CMAC=NO GO TO EEXPINT (p47)

INTRO4 [ASK CON=YES, NONCON=YES OR CMACT=YES AND NCON>1, NNONCON>1 OR NCMACT>1]

I am now going to ask you some more about the time since [the first of August 2013].

+SIMILAR_26 [ASK IF NCON > 1]

You mentioned [WRITE IN NUMBER OF CON INCIDENTS FROM NCON____] incidents of someone (A) obtaining money or goods from you under false pretences. (B) conning you out of goods or money, using whatever means. 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_27 [ASK IF NNONCON > 1]

You mentioned [WRITE IN NUMBER OF NONCON INCIDENTS FROM NNONCON____] incidents of someone using or trying to use your personal information or account details in any way to buy goods or services without your permission or knowledge or to pretend to be you. 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 NCMACT > 1]

You mentioned [WRITE IN NUMBER OF CMACT INCIDENTS FROM NCMACT____] incidents of someone (A) stealing your personal information or details, or installing unwanted programs, including viruses, on any internet-enabled devices you use for personal use? (B) someone accessing information held digitally about you without your permission, altering your data without your permission or installing unwanted programs including viruses on any internet-enabled devices you use for personal use. 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

NOW ASK COGNITIVE PROBES
SORTING OUT THE SERIES PATTERN

INTCHK1: INTERVIEWER: HAS PARTICIPANT REPORTED EXPERIENCING A …
1. CONFIDENCE FRAUD (CON=1)
2. NON-CONFIDENCE FRAUD (NONCON=1)
3. COMPUTER MISUSE ACT CRIME (CMACT=1)

ALLPART

(As far as you are aware) Were all the incidents of [TYPE OF CRIME (A)] someone obtaining money or goods from you under false pretences (B) someone conning you out of goods or money, using whatever means

(A) …someone using or trying to use your personal information or account details in any way to buy goods or services without your permission or knowledge or to pretend to be you… (B) …someone using or trying to use your personal information or account details in any way to buy goods or services without your permission or knowledge or to pretend to be you

(A) …someone stealing your personal information or details, or installing unwanted programs, including viruses, on any internet-enabled devices you use for personal use (B) …someone accessing information held digitally about you without your permission, altering your data without your permission or installing unwanted programs, including viruses, on any internet-enabled devices you use for personal use

…part of a series or were any of them separate incidents?

1. All were part of a series – GO TO PROBES
2. Some were separate incidents, the rest were a series – ASK XNUMSEP

+XNUMSEP [ASK IF ALLPART = 2 (SOME SEPARATE, REST SERIES)]

How many of the incidents were SEPARATE incidents?

ENTER NUMBER _______
Can we now think about the separate incidents of ^CRIME that is, those incidents which were NOT part of the series. Can you tell me the date of the [earliest/second/etc] separate incident?

IF R NOT SURE WHEN INCIDENT TOOK PLACE RECORD DATE R FOUND OUT ABOUT EACH INCIDENT.

INTERVIEWER: IF RESPONDENT IS NOT SURE, USING THE CALENDAR MAY HELP

1. EARLIEST MONTH_______ YEAR_______
2. 2nd MONTH_______ YEAR_______
3. 3rd MONTH_______ YEAR_______
4. 4th MONTH_______ YEAR_______
5. 5th MONTH_______ YEAR_______

INTERVIEWER FILL IN TABLE BELOW. ENTER ANSWERS FROM PREVIOUS QS TO CALCULATE TOTAL AND USE TOTAL IN CNUMSER ABOVE

NCMACT - XNUMSEP _____ = CNUMSER_______

So there were [CNUMSER_______] incidents of ^CRIME making up the SERIES?

INTERVIEWER - PLEASE CONFIRM, OR GO BACK AND AMEND CODING.

1. Yes
2. No

Could you tell me the date of the MOST RECENT incident in the series?

IF DON'T KNOW THE EXACT DATE, PLEASE ENTER ESTIMATE.

INTERVIEWER: IF RESPONDENT IS NOT SURE, USING THE CALENDAR MAY HELP.

IF FRAUD OF CYBER CRIME AND R NOT SURE WHEN INCIDENT TOOK PLACE RECORD DATE R FOUND OUT ABOUT INCIDENT

MONTH_______ YEAR_______

INTERVIEWER CHECK: Were one or more separate incidents followed by a series of incidents, and THEN another one or more separate incidents?

1. Yes – ASK INC1X
2. No – GO TO PROBES
+INC1X  [ASK IF SEPARATE INCIDENT, FOLLOWED BY A SERIES OF INCIDENTS FOLLOWED BY ANOTHER SEPARATE INCIDENT, +PATTERN=1]

Of the [+XNUMSEP____] separate incidents, how many were there BEFORE the series began?

ENTER NUMBER ______

+INC2X  [ASK IF SEPARATE INCIDENT, FOLLOWED BY A SERIES OF INCIDENTS FOLLOWED BY ANOTHER SEPARATE INCIDENT, +PATTERN=1]

And how many separate incidents were there AFTER the series ended?

ENTER NUMBER ______

NOW GO COGNITIVE PROBES OVERLEAF
Ask probes for each form (1, 2 and or 3)

**ALLPART probes**

- How did you go about answering this question?
- What did you think of as being… ‘an incident’? …part of a series?
- How easy or difficult was it to answer this question? Explore reasons
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

**XNUMSEP probes**

- How did you go about answering this question?
- What did you think of as being ‘a separate incident’?
- How easy or difficult was it to answer this question? Explore reasons
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

**SEPDATES/ LATEST probes**

- How did you go about answering this question?
- How easy or difficult was it to answer this question? Explore reasons and whether participant gave date first aware crime took place or date actually took place.
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

- **INTVIC: INTERVIEWER: YOU ARE NOW GOING TO ASK THE VICTIM FORM Qs. IF R HAS EXPERIENCED BOTH FRAUD(S) AND COMPUTER MISUSE ACT INCIDENTSTHEN ASK A VICTIM FORM ABOUT JUST ONE.**
VICTIMISATION MODULE

Aims:
- To explore whether participants understand the new victimisation questions.
- To explore what level of detail victims of fraud and cyber crime are able and willing to provide.
- To explore whether participants know the date when an incident occurred and if not do they report the date they first found out about the incident.
- To check whether participants are consistent when giving dates (i.e. giving dates for when found out about incident or when it occurred).
- Ask the victimisation questions, recording the participant’s answer.
- Encourage the participant to think aloud as they answer the questions… PROMPT ‘tell me what you are thinking’.
- Ask probes at the end of each section.

INTRO

I now want to ask you about WHEN the incident(s) you mentioned of…
(CON) someone obtaining money or goods from you under false pretences
(NONCON) someone using or trying to use your personal information or account details in any way to buy goods or services without your permission or knowledge or pretending to be you
(CMACT) someone stealing your personal information or details, or installing unwanted programs, including viruses, on any internet-enabled devices you use for personal use

happened during the last 12 months. I'd like to mark on the calendar the date of each incident.

INTERVIEWER: FOR EACH CRIME, MARK ON THE CALENDAR THE DATE WHEN IT OCCURRED. THIS ONLY NEEDS TO BE ESTIMATED TO THE NEAREST MONTH.

IF FRAUD OR CYBER CRIME RECORD DATE RESPONDENT FOUND OUT ABOUT THE INCIDENT

IF THE RESPONDENT IS HAVING DIFFICULTY REMEMBERING THE EXACT MONTH YOU MAY FIND IT USEFUL TO MARK SOME OTHER LANDMARK DATES ON THE CALENDAR (FOR EXAMPLE, BIRTHDAYS, ANNIVERSARIES, ETC.) WHICH CAN BE USED FOR REFERENCE POINTS. EXAMPLES OF SUCH EVENTS OR PERIODS CAN BE FOUND ON THE FRONT PAGE OF THE CALENDAR.

DATE OF INCIDENT (FOR A SERIES OF INCIDENTS)

DATESERA [ASK IF SERIES OF SIMILAR INCIDENTS]

You mentioned a series of [ENTER NUMBER FROM CNUMSER_______] similar incidents of someone stealing your personal information or details, or installing unwanted programs, including viruses, on any internet-enabled devices you use for
personal use since the first August 2013. When did these incidents happen?

ALL THAT APPLY

1. Before the first of August 2013
2. Between August and October 2013
4. Between February and April 2014
5. Between May and July 2014
6. Between the first of August 2014 and the present

NQUART1-5
How many incidents of this kind happened between….

a) … August and October 2013
   NO. 

b) … November 2013 and January 2014
   NO. 

c) … February and April 2014
   NO. 

d) … May and July 2014
   NO. 

e) … the first of August 2014 and the present
   NO. 

MTHRECPN
[ASK IF MORE THAN ONE INCIDENT IN A QUARTER AT NQUART]

SL
In which month did the most recent of these incidents happen?

INTERVIEWER EXPLAIN: IF PART OF SERIES, THE FOLLOWING QUESTIONS REFER TO THE MOST RECENT INCIDENT IN SERIES.

1. August
2. September
3. October
4. November
5. December
6. January
7. February
8. March
9. April
10. May
11. June
12. July
13. August
14. Don't know

NOW ASK COGNITIVE PROBES
Probes for date series incident occurred
- How easy or difficult was it to answer these questions (provide dates)? Explore reasons
- CHECK: what dates are being provided here: dates offences took place or dates when participant became aware crime had been committed?
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

DATE OF INCIDENT (FOR SINGLE INCIDENTS)

MTHINC2 [ASK IF SINGLE INCIDENT]
You said that, since the first of August 2013, you had an incident of ^CRIME. In which month did that happen?

1. August
2. September
3. October
4. November
5. December
6. January
7. February
8. March
9. April
10. May
11. June
12. July
13. August
14. Don't know → ASK QTRINCID

QTRINCID [ASK IF MTHINC2=DK]
In what quarter did the incident happen? Was it ...

1. Before the first of August 2013
2. Between August and October 2013
4. Between February and April 2014
5. Between May and July 2014
6. Between the first of August 2014 and the present
7. Don't know

CHKRECI2
And can I just check, did the incident happen before or after the first of August 2013?

2. Before the first of August 2013
3. After the first of August 2013
• How easy or difficult was it to answer these questions (provide dates)? Explore reasons
• CHECK: what dates are being provided here: dates offences took place or dates when participant became aware crime had been committed?
• On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.
DESCRIPTION OF INCIDENT

DESCRINC

Before I ask you a number of detailed questions to enable us to classify exactly what happened can you tell me, very briefly, about the incident?

IF PART OF A SERIES RECORD THE MOST RECENT OCCASION.
PROBE FOR DETAILS OF NATURE AND CIRCUMSTANCES OF INCIDENT. (FOR EXAMPLE, WHO WAS THE VICTIM, WHO WAS THE OFFENDER, WHERE DID IT HAPPEN, WHAT DID THEY DO, HOW DID THEY FIND OUT ABOUT THE INCIDENT?)

NOW ASK COGNITIVE PROBES

Probes on description of incident
Read back the description. Does the participant feel is a fair summary? Explore any changes the participant feels are needed

Check that the summary covers the following information. If a relevant point is not covered then collect this information

- Were bank details and or other personal information requested and/or passed on?
- Was money requested and or sent/transfered?
- Was anything actually stolen? Probe for details
  - Was any money taken without permission or prior knowledge from a personal bank, building society or credit card account? PROBE what is being included as a ‘personal account’.
- Were any personal cards used *without permission or prior knowledge* to take money from personal bank or building society accounts or to charge money to a personal credit or debit card?
- Has money been taken from a personal bank or building society account or credit card in some [other] way which involved personal details being used *without permission or prior knowledge*?
- Were any personal cards ACTUALLY stolen at any point before money was taken from a personal bank, building society or credit card account?
- Was any personal information held in a computerised form, such as data of birth, medical or social security information accessed, stolen or tampered with *without permission*?
- Were any other online accounts, such as store accounts, social media or email accounts accessed, stolen, or tampered with *without permission*? Exclude bank/building society account

- Did any goods or services purchased turn out to be fake or non-existent? Probe details

- Was any property damaged, such a computer or digital device? Probe for details

- Did participant have any contact with the offenders? If so collect details mode(s) of contact.

- How did the respondent find out about the incident? Probe for details

**CIRCUMSTANCES OF INCIDENT**

**VICTAREA**  [ASK ALL]
Can I just check, did it happen in this area (within 15 minutes walk of here)?

1. Yes  ➔  GO TO WHYHAP3
2. No  ➔  ASK WHEREHAPP
3. (spontaneous) Don’t know  ➔  ASK WHEREHAPP

**WHERHAPP**  [ASK IF VICTAREA = NO OR DK/REF]
Did it happen in England or Wales or did it happen somewhere else?

1. England or Wales  ] ➔  GO TO WHYHAP3
2. Elsewhere (not online)  ➔  WHYHAP3
3. On–line, over the internet  ➔  LIVE

**IF INCIDENT HAPPENED ONLINE (WHERHAPP CODE 3)**

**WHERLIVE**
And where were you living when this occurred? 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)
Probes for VICTAREA – WHERLIVE
Ask for each question
- How easy or difficult was it to answer these questions? Explore reasons and participant’s ability to recall information
- How did you go about answering these questions?
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you to each of these questions? Explore reasons for rating.

WHYHAP3 [ASK ALL]
Can you tell me why you think this incident happened?
OPEN: RECORD VERBATIM ANSWER

Probes for WHYHAP
- How easy or difficult was it to answer these questions? Explore reasons and whether any answer options caused confusion
- How did you feel about being asked this question? Explore feelings
- If this question were asked in the survey would you answer it? Why?

TIMING AND LOCATION OF INCIDENT

WHERE1
Where did this incident happen?
Open (probe where occurred/ methods of communication used for example, face-to-face on doorstep, telephone, online etc)

Probes
- How did you go about answering this question?
- How easy or difficult was it to answer this question? Why?
COSTS OF CRIME

CMALOSS ASK IF CMACT= YES

[Still thinking about this most recent incident] Has this incident cost you money? 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. Yes – ASK CMALOSS1
2. No – GO TO TRES

CMALOSS1 How much money 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 (i.e. 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

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

TRIGHT

How much time, overall, do you estimate you spent dealing with this incident to put things right? If it is still on-going 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

Probes

CMALOSS
• How did you go about answering this question? Get participant to talk you through what they included and excluded
• CHECK: did they include money refunded (for example, through insurance)
• How easy or difficult was it to answer this question? Why?

CMALOSS1
• How did you go about answering this question? Get participant to talk you through how they calculated their losses and costs
• How easy or difficult was it to answer this question? Why?
• CHECK: did they include money refunded (for example, through
insurance)?

- CHECK: did they include personal losses/costs or did they include businesses losses/costs (if self-employed) or joint losses/costs (from a joint account/card etc)?
- Replay participant’s answer to them. Does this sound about right? Explore whether they would like to change their answer and why?

**TRES**
- How did you go about answering this question?
- How easy or difficult was it to answer this question? Why?

**TRIGHT**
- How did you go about answering this question?
- How easy or difficult was it to answer this question? Why?

**IMPACT**

**EMOTREAC  [ASK ALL]**

SHOW CARD 1
Many people have emotional reactions after incidents in which they are victims of crime. Looking at this card did you PERSONALLY have any of these reactions after the incident?

1. Yes – ASK WHEMOT
2. No – GO TO IMPACT2

**WHEMOT  [ASK IF EMOTREAC = YES]**

SHOW CARD 1
Which 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. Other (SPECIFY)

**HOWAFF1  [ASK IF EMOTREAC = YES]**

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 2
Looking at this card what, 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 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/ I am more cautious online
16. I no longer use certain internet sites/ services
17. I no longer use the internet in public places
18. Other (SPECIFY)
19. No impact

Probes
• How did you feel about being asked these questions? Explore reasons

WHEMOT
• Are there any reactions missing from the card?

IMPACT2
• What did you understand by ‘I no longer use the internet in public places’? Explore what types of internet/web based activity the participant does in public places and whether this has changed as a result of being a victim of fraud or cyber crime.
Stage 6: More general exploration of experiences of fraud cyber crime

Aim:
- To explore whether participants have experienced fraud or cyber crime not captured by the survey questions
- To understand why certain crimes/ experiences were missed

General probes for those who mentioned they had experienced fraud or computer misuse act offences

- Have you experienced any types of fraud or computer-related crime not captured by the questions I’ve asked you today?
- If so, explore when experienced and whether considered including them
- How could we improve the questions so as to encourage people to tell us about these types of crimes?

END INTERVIEW
- Is there anything else you would like to tell us?
- Thank the participant for their time and give them their incentive voucher.
- Provide the ‘further resources’ leaflet. Explain that you will be giving this to everyone who takes part.
- Reassure them about confidentiality
- Answer any questions they may have

ASK NEXT SET OF Q IF CON, NONCON AND CMACT ANSWERED NO

EEXPINT [ASK IF CON, NONCON AND CMACT=NO]

SHOW CARD 3
In the last 12 months, have you personally experienced any of the things mentioned on this card while using the internet? CODE ALL THAT APPLY

1. A computer virus
2. Loss of money
3. Unauthorised access to/use of personal data (for example, e-mail account/bank account)
4. Upsetting images/illegal images
5. Abusive/threatening behaviour
6. None of these
MMFRD1A [ASK ALL]

SHOW CARD 4
Looking at this card, have you personally EVER received any emails, texts, letters or phone calls from an individual or a company that you've never heard of before about any of the following?
CODE ALL THAT APPLY

INTERVIEWER: THIS INCLUDES INTERNET POPUPS

1. A big win in a lottery, prize draw, sweepstake or competition that you haven't entered
2. The chance to make an investment with a guaranteed high return (for example, shares, art, fine wine, etc.)
3. Someone who invites you to get to know them with a view to a possible friendship or relationship (this may be via a website)
4. Help in moving large sums of money from abroad
5. Help in releasing an inheritance
6. An urgent request to help someone get out of some sort of financial trouble
7. A job offer, a franchise offer or other business opportunity
8. A loan on very attractive terms
9. Adopting or buying a pet
10. Some other type of similar request – ASK OTMFR2
11. None of these – GO TO PROBES, STAGE 6
12. SPONTANEOUS ONLY: Never read or listen to messages like these – GO TO PROBES, STAGE 6

MMFRD2A- [ASK IF MMFRD1 CODED 1-10]

SHOW CARD 4
Now thinking about the LAST 12 MONTHS, have you personally received any of these emails, texts, letters or phone calls from an individual or a company that you've never heard of before?
CODE ALL THAT APPLY

INTERVIEWER: THIS INCLUDES INTERNET POPUPPS

1. A big win in a lottery, prize draw, sweepstake or competition that you haven't entered
2. The chance to make an investment with a guaranteed high return (for example, shares, art, fine wine, etc.)
3. Someone who invites you to get to know them with a view to a possible friendship or relationship (this may be via a website)
4. Help in moving large sums of money from abroad
5. Help in releasing an inheritance
6. An urgent request to help someone get out of some sort of financial trouble
7. A job offer, a franchise offer or other business opportunity
8. A loan on very attractive terms
9. Adopting or buying a pet
10. Some other type of similar request
11. None of these

Probes
- Did you consider any of these when answering the screening questions? Explore why/why not
- Have you ever experienced any of these crimes? If so, explore when experienced and whether considered including them
- How could we improve the questions so as to encourage people to tell us about these types of crimes?
End of interview

- *Is there anything else you would like to tell us?*
- *Thank the participant for their time and give them their incentive voucher.*
- *Provide the ‘further resources’ leaflet. Explain that you will be giving this to everyone who takes part.*
- *Reassure them about confidentiality*
- *Answer any questions they may have*
SERIAL NO: __________

Stage 1: Introduction

**Aims:** To introduce the study and collect informed consent.

- Thank participant

- Introduce yourself and NatCen Social Research. We are an independent, not for profit, research organisation.

- Explain we are doing this study on behalf of the Office for National Statistics. The ONS are responsible for the Crime Survey for England and Wales. This survey collects information about people’s experience of crime and the criminal justice system. The survey is run every year and you kindly took part in 2013.

- Some new questions have been developed and we would like to try these out, to see whether they are working as intended. During this interview you will be asked some CSEW survey questions, including some new questions. I will explore how you went about answering them to see if the questions are clear and appropriate.

- Taking part is entirely voluntary – this isn’t a ‘test’ and there are no ‘right or wrong’ answers.

- Stress confidentiality. The findings from all the interviews will be written up as report. We never include the names of the people who take part in our reports.

- Explain that you will be recording the interview so that you don’t have to make lots of notes during the interview.
  - Recorder is encrypted and only the research team at NatCen will have access to the recordings.
  - Check this is OK with the participant.

- The interview will last around 60 minutes. Everyone who takes part receives a £20 high street voucher to thank them for their time.

- Ask whether participant has any questions before you start.
Stage 2: Background

Aims:
- To ‘warm participant up’.
- To double-check screening details are correct.
- To get background information on participant’s use and confidence in using the internet and computers/ tablets/smart phones.

- Explain before we ask the new survey questions would like to collect a little bit of background about the participant
- Double check details from screening.
- Explore:
  - Who lives with participant as part of their household.
  - How long lived at this address.
  - Employment status

- Use of computers/ internet
  - Frequency of using internet
    - How often they use internet
    - What mainly use internet for
  - Confidence in using computers/ internet
  - Devices used to access internet
    - Computer/ tablet/ mobile/ other
    - Locations where access takes place (home, work, library, public space)
    - Device shared with anyone else
Stage 3: Think aloud training

Aim:

- To explain the ‘Think Aloud’ process and to encourage thinking aloud behaviours.

- Explain that you are going to ask the participant some survey questions. Whilst they try to answer these questions you want to know their first impressions of these questions and what they are thinking about.

- Explain the ‘Think Aloud’ technique using a scenario of your choice (the windows example is given below but you are welcome to use an alternative). Part of this is to get the participant used to talking.

**Windows example:** I would like you to have a practice at ‘thinking aloud.’ I am going to ask you a question and I want you to tell me what you are thinking as you work out your answer…

‘How many windows are there in your home?’ Please describe what you are thinking as they work out your answer…

- Encourage think aloud through rest of interview…
Stage 4 CSEW SCREENER QUESTIONS

Aims of cognitive testing
- to get first impressions of the new screening questions
- to explore understanding of the new screening questions
- to explore whether fraud or cyber crime are being picked up in existing screener questions
- to explore any difficulties

Protocol
- Ask all screening questions, encouraging participants to think aloud as they answer. Record their answers at each question.
- Probe on the following questions once all screening questions are complete. Remind participant of question and their response
- If participant has not experienced a fraud or computer misuse act incident in the past 12 months: repeat the questions asking about the past 5 years.
- If participant has experienced more than one type of incident (a CON, NONCON and /or CMACT) then ask part one of the victim form about each type in turn. We want to collect the description of the incident so that we can explore any double counting that may occur.
- Ask part 2 of the victim form about the most recent incident. You just ask part 2 once.

INTRO
SHOW RESPONDENT LIFE EVENTS CALENDAR

Before asking you about crimes or incidents that may have happened to you over the last 12 months I’d like to give you a calendar. I’d like you to keep this in front of you when answering the next part of the interview.

If at any stage you are unsure about whether or not something happened in the last 12 months you may find looking at the calendar will help to prompt your memory.

INTERVIEWER: MARK OFF THE CORRECT 12 MONTH REFERENCE PERIOD ON THE CALENDAR, THAT IS SINCE THE FIRST OF [‘DATE’] UNTIL PRESENT, AND HAND TO RESPONDENT

INTRO1

I’m now going to ask you about things that may have happened over the last 12 months, that is since the first of September 2013, in which you may have been the victim of a crime or offence. This doesn’t mean that crimes that may have happened before this time are unimportant, but we want to build a picture of just the last 12 months so we can measure how people’s experience of crime changes from one year to the next.

I am only concerned with incidents that have happened to YOU PERSONALLY [or to people who are NOW members of your household].

I don’t just want to know about serious incidents – I want to know about small things
too.

**MOTSTOLE**

In the time since *first of September 2013*, have you/you or anyone else now in your household had anything stolen off [your/their] vehicle or out of it (parts of the vehicle, personal possessions or other things)?

1. Yes – ASK NMOTSTOL
2. No – GO TO YRHOTHEF

**NMOTSTOL**  [ASK IF MOTSTOLE = YES]

How many times has this 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

**YRHOTHEF**  [ASK ALL]

During the last 12 months, that is *first of September 2013*, has anyone GOT INTO this house/flat without permission and STOLEN or TRIED TO STEAL anything?

1. Yes – ASK NYRHTHEF
2. No – GO TO YRHOTRY

**NYRHTHEF**  [ASK IF YRHOTHEF = YES]

How many times has this 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

**YRHOTRY**  [ASK ALL]

[Apart from anything you have already mentioned], in that time have you had any evidence that someone has TRIED to get in without permission to STEAL or to CAUSE DAMAGE?

1. Yes – ASK NYRHOTRY
2. No – GO TO YRHOSTOL

**NYRHOTRY**  [ASK IF YRHOTRY = YES]

How many times has this 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
YRHOSTOL  [ASK ALL]
[Apart from anything you have already mentioned], in that time was anything STOLEN out of your house/flat?

1. Yes – ASK NYRHOSTO
2. No – GO TO INTRO2

NYRHOSTO  [ASK IF YRHOSTOL = YES]

How many times has this 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
INTRO2

The next few questions are about things that may have happened to you PERSONALLY [not the other people in your household] or that you discovered over the last 12 months, that is since the first of September 2013, in which you may have been the victim of a crime or offence. Again, I only want to know about things that have happened in the period marked on the calendar, so we can build a picture of crime in the last 12 months.

Please include anything that happened to you during that time – at home, in the street, at work, in a shop, in a park, on a train, online or anywhere else.

PERSTHEF  [ASK ALL]

Since the first of ["DATE"], [apart from anything you may have already mentioned], was anything you were carrying stolen out of your hands or from your pockets or from a bag or case?

1. Yes – ASK NPERSTH
2. No – GO TO OTHTHEF

NPERSTH  [ASK IF PERSTHEF = YES]

How many times has this 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

OTHTHEF  [ASK ALL]

And [apart from anything you have already mentioned], in that time has anything (else) of yours been STOLEN, from a cloakroom, an office, a car or anywhere else you left it?

1. Yes – ASK NOTHTHEF
2. No – GO TO DELIBDAM

NOTHTHEF  [ASK IF OTHTHEF = YES]

How many times has this 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

DELIBDAM  [ASK ALL]

And [apart from anything you have already mentioned], in that time has anything else of yours been DELIBERATELY DAMAGED or tampered with by vandals or people out to steal?

1. Yes – ASK NDELIBDA
2. No – GO TO THREVIOL
NDELIBDA  [ASK IF DELIBDAM = YES]

How many times has this 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

THREVIOL  [ASK ALL]

And [apart from anything you have already mentioned], in that time, has anyone THREATENED to damage things of yours or THREATENED to use force or violence on you in any way that actually frightened you?

1. Yes – ASK NTHREVIO
2. No – GO TO CON

NTHREVIO  [ASK IF THREVIOL = YES]

How many times has this 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
<table>
<thead>
<tr>
<th>CON</th>
<th>Version A</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Apart from anything you have already mentioned], in that time has anyone…tricked or deceived you to obtain money or goods?</td>
<td></td>
</tr>
<tr>
<td>1. Yes – ASK NCON</td>
<td></td>
</tr>
<tr>
<td>2. No – GO TO VIRUS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CON</th>
<th>Version B</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Apart from anything you have already mentioned], in that time has anyone…conned you out of money or goods, in person or online?</td>
<td></td>
</tr>
<tr>
<td>1. Yes – ASK NCON</td>
<td></td>
</tr>
<tr>
<td>2. No – GO TO VIRUS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NCON</th>
<th>Version A</th>
</tr>
</thead>
<tbody>
<tr>
<td>[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.</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
</tr>
<tr>
<td>ENTER NUMBER_________</td>
<td></td>
</tr>
<tr>
<td>97 More/too many to remember</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NCON</th>
<th>Version B</th>
</tr>
</thead>
<tbody>
<tr>
<td>[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.</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
</tr>
<tr>
<td>ENTER NUMBER_________</td>
<td></td>
</tr>
<tr>
<td>97 More/too many to remember</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VIRUS</th>
<th>Version A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apart from anything you have already mentioned], in that time has anyone…installed software, including viruses, that collects information you do not want them to have on any internet-enabled devices you use?</td>
<td></td>
</tr>
<tr>
<td>1. Yes- ASK NVIRUS</td>
<td></td>
</tr>
<tr>
<td>2. No – GO TO CMACT</td>
<td></td>
</tr>
<tr>
<td>3. [Spontaneous] Does not have a computer – GO TO CMACT</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VIRUS</th>
<th>Version B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apart from anything you have already mentioned], in that time has anyone…installed software, including viruses, that collects information you do not want them to have on any internet-enabled devices you use?</td>
<td></td>
</tr>
<tr>
<td>1. Yes- ASK NVIRUS</td>
<td></td>
</tr>
<tr>
<td>2. No – GO TO CMACT</td>
<td></td>
</tr>
<tr>
<td>3. [Spontaneous] Does not have a computer – GO TO CMACT</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NVIRUS [ASK IF VIRUS=YES]</th>
<th>Version A</th>
</tr>
</thead>
<tbody>
<tr>
<td>As far as you are aware, how many times has that happened?</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
</tr>
<tr>
<td>ENTER NUMBER_________</td>
<td></td>
</tr>
<tr>
<td>97 More/too many to remember</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NVIRUS [ASK IF VIRUS=YES]</th>
<th>Version B</th>
</tr>
</thead>
<tbody>
<tr>
<td>As far as you are aware, how many times has that happened?</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
</tr>
<tr>
<td>ENTER NUMBER_________</td>
<td></td>
</tr>
<tr>
<td>97 More/too many to remember</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CMACT</th>
<th>Version A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CMACT</th>
<th>Version B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
[Apart from anything you have already mentioned], in that time has anyone...stolen your personal information or details?
INTERVIEWER NOTE: DETAILS INCLUDE DATA THAT ARE NOT IN THE PUBLIC DOMAIN SUCH AS BANKS ACCOUNTS, EMAIL & SOCIAL MEDIA ACCOUNTS, NATIONAL INSURANCE DATA ETC.
1. Yes- ASK NCMACT
2. No – GO TO NONCON

<table>
<thead>
<tr>
<th>NCMACT [ASK IF CMACT=YES]</th>
<th>NONCON [ASK IF NONCON=NO]</th>
</tr>
</thead>
<tbody>
<tr>
<td>As far as you are aware, how many times has that happened?</td>
<td>[Apart from anything you have already mentioned], in that time has anyone...gained access to information held digitally about you without your permission?</td>
</tr>
<tr>
<td>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</td>
<td>INTERVIEWER NOTE: DETAILS INCLUDE DATA THAT ARE NOT IN THE PUBLIC DOMAIN SUCH AS BANKS ACCOUNTS, EMAIL &amp; SOCIAL MEDIA ACCOUNTS, NATIONAL INSURANCE DATA ETC.</td>
</tr>
<tr>
<td>ENTER NUMBER__________</td>
<td>ENTER NUMBER__________</td>
</tr>
<tr>
<td>97 More/too many to remember</td>
<td>97 More/too many to remember</td>
</tr>
</tbody>
</table>

1. Yes- ASK NNONCON
2. No – GO TO PROBES

<table>
<thead>
<tr>
<th>NNONCON [ASK IF NONCON=YES]</th>
<th>NNONCON [ASK IF NONCON=NO]</th>
</tr>
</thead>
<tbody>
<tr>
<td>As far as you are aware, how many times has that happened?</td>
<td>[Apart from anything you have already mentioned], in that time has anyone used or tried to use your personal information or account details in any way to buy goods or services without your permission or knowledge?</td>
</tr>
<tr>
<td>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</td>
<td></td>
</tr>
<tr>
<td>ENTER NUMBER__________</td>
<td>ENTER NUMBER__________</td>
</tr>
<tr>
<td>97 More/too many to remember</td>
<td>97 More/too many to remember</td>
</tr>
</tbody>
</table>

1. Yes- ASK NNONCON
2. No – GO TO PROBES

NOW ASK COGNITIVE PROBES OVERLEAF
Screening probes

**Con probes**

- How did you go about answering this question?
- In your own words what do you think this question is asking? Probe for understanding of:
  - ‘tricked or deceived you’ / ‘conned you’
  - ‘goods’
  - ‘whatever means’
  Explore what types of crimes participant was thinking about here.
- How easy or difficult did you find this question to answer? Explore reasons
- How did you feel about answering this question?
- What time period were you thinking about when answering this question? From when to when?

**NCON probes**

- How did you go about answering this question?
- Check: Did participant receive multiple communications about the same con/scam?
  How easy or difficult was it to answer this question? Explore reasons

**Virus probes**

- How did you go about answering this question?
  - In your own words what do you think this question is asking? Probe for understanding of: ‘installed software’
  - ‘Internet enabled devices’
  Explore what types of crimes participant was thinking about here
- How easy or difficult did you find this question to answer? Explore reasons
- How did you feel about answering this question?
- What time period were you thinking about when answering this question? From when to when?
- How confident are you that your answer is accurate, where 0 is not at all confident and 10 is completely confident?
NVirus probes

How did you go about answering this question?

- How easy or difficult was it to answer this question? Explore reasons

- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

CMAT Probes

How did you go about answering this question?

- In your own words what do you think this question is asking? Probe for understanding of:
  - ‘stolen’ / ‘accessed’
  - ‘your personal information or details’ / information about you’, ‘held digitally’

  Explore what types of crimes participant was thinking about here

- How easy or difficult did you find this question to answer? Explore reasons

- How did you feel about answering this question?

- What time period were you thinking about when answering this question? From when to when?

- How confident are you that your answer is accurate, where 0 is not at all confident and 10 is completely confident?

NCMACT probes

How did you go about answering this question?

- How easy or difficult was it to answer this question? Explore reasons

- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.
**NONCON probes**

- How did you go about answering this question?
- In your own words what do you think this question is asking? Probe for understanding of:
  - ‘used’, ‘tried to use’
  - ‘personal information’ / ‘account details’
  - ‘goods or services’
  
  Explore what types of crimes participant was thinking about here
- How easy or difficult did you find this question to answer? Explore reasons
- How did you feel about answering this question?
- What time period were you thinking about when answering this question? From when to when?
- How confident are you that your answer is accurate, where 0 is not at all confident and 10 is completely confident?

**NNONCON probes**

- How did you go about answering this question?
- How easy or difficult was it to answer this question? Explore reasons
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.
If participant said they had anything stolen at any of the earlier screening questions:

MOTSTOLE, YRHOSTHET, YRHOSTRY, YRHOSTTOL, PERSTHET, OTHETHET = yes

Probes

• Explore whether any personal information was stolen or lost? By personal information we mean any information that could be used to obtain goods or services without the participant’s permission or (could) enable someone to gain access to personal information about the participant (such as accounts, records etc).

• Explore whether the participant was reporting that the incident happened in the last 12 months or that the participant discovered that the incident had occurred, in the last 12 months. If the latter explore when the incident actually occurred.

• (IF NECESSARY) Did you include any incidents at this question that you included at CON, NONCON or CMACT? Explore which incidents included at which Q and why included at subsequent question (i.e. mentioned more than once)?

If participant said they had something damaged or someone threatened to damage something of theirs:

DELIBDAM OR THREVIOI =yes

Probes

• Explore what was damaged or threatened to be damaged.

• Explore whether the participant was reporting that the incident happened in the last 12 months or that the participant discovered that the incident had occurred, in the last 12 months. If the latter explore when the incident actually occurred.

• (IF NECESSARY) Did you include any incidents at this question that you included at CMACT? Explore which incidents included at which Q and why included at subsequent question (i.e. mentioned more than once)?
CHECKING WHETHER ANY INCIDENTS ARE A SERIES

INTCHK
IS CON=YES, NONCON=YES OR CMACT=YES AND NCON>1, NNONCON>1 OR NCMACT>1?
1 YES - ASK INTRO 4
2 NO, CON, VIRUS CMACT OR NONCON =YES BUT NCON, NVIRUS, NCMACT OR
NNONCON =1 GO TO INTVIC (p17)
3 NO, CON, VIRUS, CMACT, NONCON=NO GO TO EEXPINT (p47)

INTRO4 [ASK CON=YES, NONCON=YES OR CMACT=YES AND NCON>1, 
NNONCON>1 OR NCMACT>1 ]

I am now going to ask you some more about the time since [the first of September 2013].

+SIMILAR_26 [ASK IF NCON > 1]
You mentioned [WRITE IN NUMBER OF CON INCIDENTS FROM NCON____] incidents of someone tricking or deceiving you to obtain money or goods. 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 someone installing software, including viruses, on any internet-enabled devices you use. 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 stealing your personal information or details. 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 NNONCON > 1]
You mentioned [WRITE IN NUMBER OF NONCON INCIDENTS FROM NNONCON____] incidents of someone using or trying to use your personal information or account details 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

NOW ASK COGNITIVE PROBES
General

- In your own words what do you think this question is asking? Probe for understanding of:
  - incidents

For each question explore

- How did you go about answering this question?
- How easy or difficult was it to answer this question? Explore reasons

On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

SORTING OUT THE SERIES PATTERN

ALLPART

(As far as you are aware) Were all the incidents of [TYPE OF CRIME] ...part of a series or were any of them separate incidents?

1. All were part of a series – GO TO FORM 2, INTCHK3
2. Some were separate incidents, the rest were a series – ASK XNUMSEP

+XNUMSEP [ASK IF ALLPART = 2 (SOME SEPARATE, REST SERIES)]

How many of the [NUMBER INCIDENTS AT NCON_____] incidents were SEPARATE incidents?

ENTER NUMBER _______
Ask probes for each form (1, 2 and or 3)

**ALLPART probes**

- How did you go about answering this question?
- What did you think of as being ‘an incident’? …part of a series?
- How easy or difficult was it to answer this question? Explore reasons
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

**XNUMSEP probes**

- How did you go about answering this question?
- What did you think of as being ‘a separate incident’?
- How easy or difficult was it to answer this question? Explore reasons
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.

**INTVIC:** INTERVIEWER: YOU ARE NOW GOING TO ASK THE VICTIM FORM Qs. IF R HAS EXPERIENCED BOTH FRAUD(S) AND COMPUTER MISUSE ACT INCIDENTS THEN ASK PART A OF THE VICTIM FOR ABOUT EACH ONE. ASK PART 2 ABOUT THE MOST RECENT INCIDENT.
VICTIMISATION MODULE

Aims:

- To explore whether participants understand the new victimisation questions.
- To explore what level of detail victims of fraud and cyber crime are able and willing to provide.
- To explore whether participants know the date when an incident occurred and if not do they report the date they first found out about the incident.
- To check whether participants are consistent when giving dates (i.e. giving dates for when found out about incident or when it occurred).
- Ask the victimisation questions, recording the participant’s answer.
- Encourage the participant to think aloud as they answer the questions… PROMPT ‘tell me what you are thinking’.
- Ask probes at the end of each section.

INTRO5

I now want to ask you about WHEN the incident(s) you mentioned of crime happened during the last 12 months. I’d like to mark on the calendar the date of each incident.

INTERVIEWER: FOR EACH CRIME, MARK ON THE CALENDAR THE DATE WHEN IT OCCURRED. THIS ONLY NEEDS TO BE ESTIMATED TO THE NEAREST MONTH.

IF FRAUD OR CYBER CRIME RECORD DATE RESPONDENT FOUND OUT ABOUT THE INCIDENT

IF THE RESPONDENT IS HAVING DIFFICULTY REMEMBERING THE EXACT MONTH YOU MAY FIND IT USEFUL TO MARK SOME OTHER LANDMARK DATES ON THE CALENDAR (E.G. BIRTHDAYS, ANNIVERSARIES, ETC.) WHICH CAN BE USED FOR REFERENCE POINTS. EXAMPLES OF SUCH EVENTS OR PERIODS CAN BE FOUND ON THE FRONT PAGE OF THE CALENDAR.

DATE OF INCIDENT (FOR A SERIES OF INCIDENTS)

DATESERA [ASK IF SERIES OF SIMILAR INCIDENTS]

You mentioned a series of [ENTER NUMBER FROM CNUMSER_______] similar incidents of someone tricking or deceiving you to obtain money or goods since the first September 2013. When did these incidents happen? CODE ALL THAT APPLY

1. Before the first of September 2013
2. Between September and November 2013
4. Between March and May 2014
5. Between June and August 2014
6. Between the first of September 2014 and the present
NQUART1-5
How many incidents of this kind happened between….

a) … September and November 2013 NO.
b) … December 2013 and February 2014 NO.
c) … March and May 2014 NO.
d) … June and August 2014 NO.
e) … the first of September 2014 and the present NO.

MTHRECIN [ASK IF MORE THAN ONE INCIDENT IN A QUARTER AT NQUART]
SL
In which month did the most recent of these incident(s) happen?

INTERVIEWER EXPLAIN: IF PART OF SERIES, THE FOLLOWING QUESTIONS REFER TO THE MOST RECENT INCIDENT IN SERIES.

1. September
2. October
3. November
4. December
5. January
6. February
7. March
8. April
9. May
10. June
11. July
12. August
13. September
14. Don’t know

NOW ASK COGNITIVE PROBES

Probes for date series incident occurred
• How easy or difficult was it to answer these questions (provide dates)? Explore reasons
• CHECK: what dates are being provided here: dates offences took place or dates when participant became aware crime had been committed?
• On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.
DATE OF INCIDENT (FOR SINGLE INCIDENTS)

MTHINC2  [ASK IF SINGLE INCIDENT]
You said that, since the first of September 2013, you had an incident of [CRIME TYPE] … someone tricking or deceiving you to obtain money or goods. In which month did that happen?

1. September
2. October
3. November
4. December
5. January
6. February
7. March
8. April
9. May
10. June
11. July
12. August
13. September
14. Don’t know → ASK QTRINCID

QTRINCID  [ASK IF MTHINC2=DK]
In what quarter did the incident happen? Was it …

1. Before the first of September 2013
2. Between September and November 2013
4. Between March and May 2014
5. Between June and August 2014
6. Between the first of September 2014 and the present
7. Don’t know

CHKRECI2
And can I just check, did the incident happen before or after the first of September 2013?

1. Before the first of September 2013
2. After the first of September 2013

Probes for date single incident occurred
- How easy or difficult was it to answer these questions (provide dates)? Explore reasons
- CHECK: what dates are being provided here: dates offences took place or dates when participant became aware crime had been committed?
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you? Explore reasons for rating.
DESCRIPTION OF INCIDENT

DESCRINC

Before I ask you a number of detailed questions to enable us to classify exactly what happened can you tell me, very briefly, about the incident?

IF PART OF A SERIES RECORD THE MOST RECENT OCCASION. PROBE FOR DETAILS OF NATURE AND CIRCUMSTANCES OF INCIDENT. (E.G. WHO WAS THE VICTIM, WHO WAS THE OFFENDER, WHERE DID IT HAPPEN, WHAT DID THEY DO, HOW DID THEY FIND OUT ABOUT THE INCIDENT?)

NOW ASK COGNITIVE PROBES
Probes on description of incident

Read back the description. Does the participant feel is a fair summary? Explore any changes the participant feels are needed

Check that the summary covers the following information. If a relevant point is not covered then collect this information

Were bank details and or other personal information requested and/or passed on?

Was money requested and or sent/transferred?

Was anything actually stolen? Probe for details

Was any money taken without permission or prior knowledge from a personal bank, building society or credit card account? PROBE what is being included as a ‘personal account’.

Were any personal cards used without permission or prior knowledge to take money from personal bank or building society accounts or to charge money to a personal credit or debit card?

Has money been taken from a personal bank or building society account or credit card in some [other] way which involved personal details being used without permission or prior knowledge?

Were any personal cards ACTUALLY stolen at any point before money was taken from a personal bank, building society or credit card account?

Did any goods or services purchased turn out to be fake or non-existent? Probe details

Did participant have any contact with the offenders? If so collect details mode(s) of contact.

How did the respondent find out about the incident? Probe for details
CIRCUMSTANCES OF INCIDENT

WHERLIVE
And where were you living when this occurred? Were you living … READ OUT:
6. At this address
7. Somewhere else within 15 minutes of here
8. Somewhere else in England and Wales
9. Somewhere else (END VICTIM FORM)

Probes for WHERLIVE
Ask for each question
- How easy or difficult was it to answer these questions? Explore reasons and participant’s ability to recall information
- How did you go about answering these questions?
- On a scale of 0 to 10, where 0 is not at all sure and 10 is certain, how sure of your answer are you to each of these questions? Explore reasons for rating.

WHYHAP3 [ASK ALL]
Can you tell me why you think this incident happened?
OPEN: RECORD VERBATIM ANSWER

Probes for WHYHAP
- How easy or difficult was it to answer these questions? Explore reasons and whether any answer options caused confusion
- How did you feel about being asked this question? Explore feelings
- If this question were asked in the survey would you answer it? Why?
Stage 6: More general exploration of experiences of fraud cyber crime

Aim:
- To explore whether participants have experienced fraud or cyber crime not captured by the survey questions
- To understand why certain crimes/ experiences were missed

General probes for those who mentioned they had experienced fraud or computer misuse act offences

- Have you experienced any types of fraud or computer-related crime not captured by the questions I've asked you today?
- If so, explore when experienced and whether considered including them
- How could we improve the questions so as to encourage people to tell us about these types of crimes?

END INTERVIEW

- Is there anything else you would like to tell us?
- Thank the participant for their time and give them their incentive voucher.
- Provide the 'further resources' leaflet. Explain that you will be giving this to everyone who takes part.
- Reassure them about confidentiality
- Answer any questions they may have

ASK NEXT SET OF Q IF CON, NONCON AND CMACT ANSWERED NO

SHOW CARD 3
In the last 12 months, have you personally experienced any of the things mentioned on this card while using the internet? CODE ALL THAT APPLY

1. A computer virus
2. Loss of money
3. Unauthorised access to/use of personal data (e.g. e-mail account/bank account)
4. Upsetting images/illegal images
5. Abusive/threatening behaviour
6. None of these
SHOW CARD 4
Looking at this card, have you personally EVER received any emails, texts, letters or phone calls from an individual or a company that you’ve never heard of before about any of the following?
CODE ALL THAT APPLY

INTERVIEWER: THIS INCLUDES INTERNET POPUPS

1. A big win in a lottery, prize draw, sweepstake or competition that you haven’t entered
2. The chance to make an investment with a guaranteed high return (e.g. shares, art, fine wine, etc.)
3. Someone who invites you to get to know them with a view to a possible friendship or relationship (this may be via a website)
4. Help in moving large sums of money from abroad
5. Help in releasing an inheritance
6. An urgent request to help someone get out of some sort of financial trouble
7. A job offer, a franchise offer or other business opportunity
8. A loan on very attractive terms
9. Adopting or buying a pet
10. Some other type of similar request (SPECIFY ____________________)
11. None of these – GO TO PROBES, STAGE 6
12. SPONTANEOUS ONLY: Never read or listen to messages like these – GO TO PROBES, STAGE 6

MMFRD2A- [ASK IF MMFRD1 CODED 1-10]

SHOW CARD 4
Now thinking about the LAST 12 MONTHS, have you personally received any of these emails, texts, letters or phone calls from an individual or a company that you’ve never heard of before?
CODE ALL THAT APPLY

INTERVIEWER: THIS INCLUDES INTERNET POPUPs

1. A big win in a lottery, prize draw, sweepstake or competition that you haven’t entered
2. The chance to make an investment with a guaranteed high return (e.g. shares, art, fine wine, etc.)
3. Someone who invites you to get to know them with a view to a possible friendship or relationship (this may be via a website)
4. Help in moving large sums of money from abroad
5. Help in releasing an inheritance
6. An urgent request to help someone get out of some sort of financial trouble
7. A job offer, a franchise offer or other business opportunity
8. A loan on very attractive terms
9. Adopting or buying a pet
10. Some other type of similar request
11. None of these

Probes
- Did you consider any of these when answering the screening questions? Explore why/why not
- Have you ever experienced any of these crimes? If so, explore when experienced and whether considered including them
- How could we improve the questions so as to encourage people to tell us about these types of crimes?
End of interview

- *Is there anything else you would like to tell us?*
- *Thank the participant for their time and give them their incentive voucher.*
- *Provide the ‘further resources’ leaflet. Explain that you will be giving this to everyone who takes part.*
- *Reassure them about confidentiality*
- *Answer any questions they may have*
Dear

Developing new questions for the Crime Survey for England and Wales

Thank you for taking part in the Crime Survey for England and Wales last year: we really appreciate your help. I'm writing to tell you about a new research study we are doing that we would like your help with. The aim of this research is to develop some new questions to be included in future crime surveys in England and Wales.

This new research is being conducted by NatCen Social Research, an independent research organisation, on behalf of ONS. You can find out more information about NatCen and this new research in the enclosed leaflet or visit them online at www.natcen.ac.uk.

An interviewer from NatCen may be in touch with you by telephone to ask if you are willing to participate in a face-to-face interview. If you choose to take part in an interview it will last around one hour and will take place at a time of your choosing.

Any information you provide will be held in the strictest of confidence and will be handled securely throughout the study. Participation in this research is voluntary. Everyone who takes part in an interview will receive a £20 high street voucher, as a small token of thanks.

If you do not want to take part please let NatCen know by 8th August 2014. You can contact Sophie Green on freephone 0800 xxxxx or email NAME@natcen.ac.uk Alternatively, you can return the enclosed form to NatCen in the freepost envelope provided. If you have any questions about the research please contact Sophie Green or my team. Your contribution will help us improve our reporting of crime statistics. We hope that you decide to take part.

Yours sincerely,

John Flatley

Head of Crime Statistics and Analysis

EMAIL: CrimeStatistics@ons.gsi.gov.uk

Direct recruitment letter
Trying out new questions to be included in the Crime Survey for England and Wales

We are developing some new questions for the Crime Survey for England and Wales on fraud and internet crimes. We want to try out the questions before the questionnaire is used to interview thousands of people.

This new research is being conducted by NatCen Social Research, an independent research organisation, on behalf of the Office for National Statistics (ONS). You can find out more information about NatCen and this new research in the enclosed leaflet or visit us online at www.natcen.ac.uk.

Taking part involves a face-to-face interview. If you choose to take part in an interview it will last around one hour and will take place at a time of your choosing.

Any information you provide will be held in the strictest of confidence and will be handled securely throughout the study. Participation in this research is voluntary. Everyone who takes part in an interview will receive a £20 high street voucher, as a small token of thanks.

If you are interested in taking part then please contact Sophie Green on freephone 0800 XXXXX or email NAME@natcen.ac.uk. If you have any questions about the research please contact Sophie Green or myself. Your contribution will help improve the reporting of crime statistics.

Yours sincerely,

Debbie Collins
Recruitment screening questionnaire

CSEW Fraud and Cyber Crime Cognitive Testing

Screening questionnaire

Introduction

My name is [AS APPROPRIATE] and I work for NatCen Social Research, an independent research institute.

We are carrying out this study on behalf of the Office for National Statistics. The ONS are responsible for the Crime Survey for England and Wales. This survey collects information about people’s experience of crime and the criminal justice system. The survey is run every year and you kindly took part in 2013. You should have recently received a letter from us letting you know we might call.

Some new questions have been developed and we would like to try these out, to see whether they are working as intended. During this interview you will be asked some CSEW survey questions, including some new questions and I will explore how you went about answering them to see if the questions are clear and appropriate.

Taking part is entirely voluntary – this isn’t a ‘test’ and there are no ‘right or wrong’ answers.

What will taking part involve?

Taking part in this study will involve talking to one of our interviewers at a time and location convenient for you.

The interview would last about an hour, and, if you take part, you will be given a 20 pound high street voucher for your time. All information will be treated in the strictest confidence and used for research purposes only.

Taking part is entirely voluntary. With your consent, we would like to audio record the interview. This will allow the researcher to focus completely on what you are saying. No one outside the research team will have access to the audio recording or to any information that could identify that you took part in the study. The audio recording will be deleted at the end of the project.

IF WILLING TO TAKE PART GO ON. IF NOT, THANK THEM AND END

Screening Questions
Can I just ask you a few questions to see if you are eligible to take part in the interview?

**Q1. Sex of participant (do not ask this, just record)**

- Male □
- Female □

**Q2. Are you?**

- 18-34 □
- 35-54 □
- Or 55+ □

**Q3. What is your highest qualification?**

- A level or higher □
- GCSE or lower □

**Q4. Have you yourself ever used the internet or World Wide Web in the last 12 months for any reason (other than your work)?**

- Yes □ IF YES ASK Q5
- No □ IF NO ASK Q6

**Q5. How often do you usually use the internet or World Wide Web for any reason (other than your work)?**

READ OUT

- Once or more per week □
- Less than once or more per week □
Q6. Do you have any physical or mental health conditions or illnesses lasting or expected to last for 12 months or more?

Yes ☐
No ☐

Check your individual quota sheets to decide if the participant is eligible to take part in an interview or not.

If the participant is not eligible, thank them and close. If a participant is eligible ask them what time appointment they would like.

Collect contact details for ALL screened in people:

Name of participant .................................................................
Address .....................................................................................
..............................................................................................
..............................................................................................
..............................................................................................
Postcode .....................................................................................
Telephone number ........................................................................
Date and time of interview .................................................................

POST SCREENING: Thank the participant.
Appendix D. Cognitive testing methodology

This study employed a qualitative method – that of cognitive interviewing – to test proposed new questions on fraud and cybercrime to be included in the screener and victimisation modules of the CSEW. Cognitive interviewing methods explore what participants think about when attempting to answer a survey question. Information on cognitive processes is gathered using a combination of think aloud and probing techniques (see for example, Beatty and Willis, 2007; Collins, 2003; Willis, 2005). The sampling strategy used for this study was purposive and findings are based on a thematic analysis of the interview data using the Framework method (Spencer et al, 2003). In the rest of this Annex we describe in more detail the methodology used for this study.

Data Collection

Ethical approval and protocol

All stages of this research were approved by NatCen’s Research Ethics Committee (REC), which includes external experts and specialists in methodology. In obtaining ethical approval for this study, a pre-specified research protocol was set out and agreed. Any subsequent amendments to this protocol were resubmitted and approved by the REC.

On the day of the research, a full description of what the research involved was given to participants prior to interview. Participants had the opportunity to ask any questions about the research and were only included in the project if they provided consent (all did so).

Recruitment

Participants were recruited using two methods.

Recruitment of CSEW participants

At rounds one and two participants were recruited from among people who had participated in a CSEW interview during 2013 and had given consent to be recontacted, by a third party. Interviewers were asked to recruit participants with particular characteristics: age, sex, highest qualification and internet usage, and fill preset quotas. In addition participants from different ethnic groups and those with long-standing health problems were recruited, as these groups are known to be more likely to have been victims of fraud and cyber crime offences.

Before interviewers made contact, sample members were sent a letter telling them about the study and providing them with information on how to opt out if they did not wish to be contacted. After two weeks the cognitive interviewers telephoned potential participants, carried out a short screening interview to check sample members’ details
and eligibility to take part in the study. Appointments were made with those participants who were willing to take part.

**Recruitment through interviewers’ networks**

At round two, to boost the number of victims interviewed, interviewers were asked to recruit half of their target number of interviews through their own networks. Victims of fraud, theft of data and interference with internet and computer access were recruited from among interviewers’ friends and family, people known to the interview or through asking participants interviewed at round one if they knew someone who had had an experience of one of the crimes of interest who would be willing to take part. All would-be recruits were provided with a letter and study leaflet that explained the purpose of the research and what taking part involved in broad terms.

Would-be research participants were asked to contact the research team using a freephone number or email, who provided them with some background information about the study and asked them a short screening questionnaire to ensure eligibility in the study. Copies of the recruitment materials are included in Appendix C.

**Qualitative sampling approach**

This study involved a qualitative sampling approach. Unlike quantitative sampling methods, which are concerned with producing statistical estimates of the prevalence of characteristics or phenomena of interest to the study in the wider target population, qualitative sampling methods involve the study of far fewer people, but explore in more depth those individuals, settings, subcultures, and scenes, so as to generate a deeper understanding of individual perspectives, understandings and behaviours.

In contrast to the probability sampling techniques used in quantitative studies, qualitative studies, including those using cognitive interviewing methods, deploy purposive sampling approaches which involve the development of a framework of the variables that might influence an individual's contribution. The choice of variables is based on the researcher's practical knowledge of the research area and available literature and evidence (see for example, Bryman, 2012; Ritchie et al, 2003).

**Profile of participants**

A purposive sample of 37 participants was recruited, 18 in round one and 19 in round 2. The recruitment strategy was designed to include men and women of different ages, levels of education, and internet usage. We also included some participants with health conditions or disabilities and those from black and minority ethnic (BME) groups. The characteristics of participants are presented in table D.1. The table indicated the number of participants we interviewed who reported being a victim of fraud or cybercrime. In total we interviewed 24 victims of fraud or cybercrime, five in round one and 19 in round 2.
Table D.1  Participant characteristics

<table>
<thead>
<tr>
<th>Characteristics of participants</th>
<th>R1</th>
<th>R2</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sex</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>9</td>
<td>9</td>
<td>18</td>
</tr>
<tr>
<td>Female</td>
<td>9</td>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-34</td>
<td>5</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>35-54</td>
<td>3</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>55+</td>
<td>10</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GCSE or lower</td>
<td>6</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>A Level or higher</td>
<td>12</td>
<td>13</td>
<td>25</td>
</tr>
<tr>
<td><strong>Personal internet use</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does not use</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Used in past 12 months</td>
<td>16</td>
<td>19</td>
<td>35</td>
</tr>
<tr>
<td>Once or more per week</td>
<td>15</td>
<td>18</td>
<td>33</td>
</tr>
<tr>
<td>Less than once a week</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Health Condition</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>6</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>No</td>
<td>12</td>
<td>15</td>
<td>27</td>
</tr>
<tr>
<td><strong>Ethnicity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White British</td>
<td>15</td>
<td>16</td>
<td>31</td>
</tr>
<tr>
<td>BME</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>** Experienced incident in past 5 yrs**</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud or cyber crime</td>
<td>5</td>
<td>16</td>
<td>21</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>18</td>
<td>19</td>
<td>37</td>
</tr>
</tbody>
</table>
Fieldwork protocols

Before each interview, a member of the research team spoke to the participant individually about the study and answered any questions he or she had about the study. Once the participant fully understood the study and what taking part involved, verbal or written consent was gained. If the team member believed that the person did not understand the study or felt coerced or influenced in any way to take part in the study they were not interviewed. Some basic demographic information was collected at the recruitment stage. Everyone who took part in the interviews was given a £20 high street voucher, a thank you letter, and a leaflet providing them with details of organisations that they could approach, should they wish to, for further information and support. Copies of the recruitment materials are contained in Appendix C.

The research involved face-to-face cognitive interviews carried out by four experienced cognitive interviewers. All the interviews took place in participants’ homes. The interviews were audio recorded, with the participant’s consent, using encrypted digital recorders. At the start of the interview, the interviewer explained the structure and the purpose of the interview. The interviewer then asked the survey questions. The interviewer used an interview protocol, which contained instructions on when to use think aloud and when to probe, using scripted probes, to follow up on specific elements.

Interview protocol

An interview protocol was developed and used with all participants. In the interview, participants were asked the survey questions, a section at a time. They were asked all the screening questions first, then the victim form test questions. These questions were asked in ‘chunks’. Participants were asked to think aloud as they went about trying to answer the survey questions. The interviewer then asked a number of scripted and spontaneous, elaborative and expansive probes.

These interviewing techniques are described in more detail in the next section.

Appendix A contains a copy of the interview protocol and the probes used. Cognitive interviews are semi-structured and interviewers were encouraged to supplement the protocol with spontaneous probes in order to fully explore any issue that arise.

Think aloud

Think aloud, or verbal protocol, is a method that requires participants to talk aloud while solving a problem or performing a task. It was originally developed by Ericsson and Simon (1980) and has been widely applied in cognitive psychology research. Think aloud has become an established means of observing different forms of behaviour requiring individuals to verbalise their thought processes and actions (Gray & Wardle, 2013).

Think aloud can be carried out in two ways:

- concurrently: at the time the subject is solving the problem or answering the question (known as a ‘live’ report), or
- retrospectively: after the event.
Concurrent think aloud requires minimal input from the investigator (Ericsson and Simon, 1993) whilst retrospective think aloud data can either involve uninterrupted accounts of the event or can be facilitated by retrieval or other cues such as video recordings of the event or specific questions about what happened (Taylor & Dionne, 2000).

In this research concurrent think aloud was used to explore participants' initial reactions and thoughts on being asked a survey question.

**Probing**
Immediately after the think aloud, participants were asked a series of cognitive probes to explore in more detail their understanding of the question and specific terms it contained.

Probes were asked retrospectively, after all the screening questions were asked, and after each set of victimisation module questions. Work by Conrad and Blair (2009) suggests that respondent-driven cognitive interviewing techniques, in which think aloud takes place prior to any probing, improves the reliability of error detection.

**Analysis**
A Framework approach to data management and analysis was used. Framework is a matrix approach where data is summarised into cells with a row representing an individual case and a column representing a common theme across the data. The advantage of this approach is that it facilitates the analysis of different aspects of an individual's processing of information and the information features that influence understanding as well as enabling analysis of particular themes across different cases (see Collins, 2014).

All notes were 'summarised' into an analytical framework set up in Excel. This analytical framework consisted of a number of descriptive and analytical categories, reflecting the interview protocol. The framework included a summary of the characteristics of participants: such as their sex, age, ethnicity, highest educational qualification and interview location. The framework was organised by each of the test questions. Under each question a summary was made of each interview's findings pertinent to the think aloud and each cognitive probe. An additional 'other' category was included for each card, to capture any other comments made by the participant that had not been anticipated in the design of the probes. Thus, data could be read horizontally as a complete case record for an individual, or vertically by question, looking across all cases.

**Study limitations**
This study has a number of limitations that should be born in mind when considering its findings and these are discussed below.

**Limitations of cognitive interviewing**
Cognitive interviews are qualitative in nature, involving an in-depth interviewing approach and typically small, purposive samples. In these interviews we can explore the cognitive processes that go on while a participant is attempting to make sense of
the information provided. The method helps us identify different types of problem that participants encounter and provides us with evidence about why these problems occur. However, cognitive interviewing cannot provide quantitative information on the extent of the problem or the size of its impact on survey estimates. Samples are usually too small, and cases not selected with a known and equal chance to support such extrapolation.

The method relies on participants' ability to articulate their thought processes; however not everyone can do this (well). Moreover it is thought that cognitive interviewing favours people with a higher level of education, as they find it easier to articulate their thoughts, particularly when using think aloud (Fowler, 1995). A further point to note is that not all thought is conscious and therefore capable of being articulated. Our interview protocol was designed to use a range of cognitive interviewing techniques to ameliorate these problems.

The method may also change participants' usual behaviour, for example participants may spend more time reading and/or considering information presented than they would in a real life setting and this could lead to spurious findings (see for example Wilson et al, 1995). In our study we were not principally concerned with participants' reading behaviour; rather we assessed understanding of the questions using a range of cognitive techniques..

References for Appendix D


