Crime Survey
for England & Wales

CSEW Fraud and Cyber-crime Development: Field Trial

TNS BMRB

JN123456

Contents

1. Executive Summary

The Crime Survey for England and Wales (CSEW) was designed back in the early 1980s to provide estimates of victimisation among adults aged 16 and over living in households in England and Wales. The method by which crimes recorded by the CSEW has not changed since the survey started. A series of questions are used to identify and then collect detailed information on, any potentially criminal incidents experienced by respondents or the household in the previous 12 months. The information collected is then reviewed to determine whether what has been reported represents a crime or not, and, if so, what offence code should be assigned to the crime.

Whilst the CSEW has changed little over the last thirty years, the ways in which some crimes are being committed has. Criminals can now take advantage of new technologies such as the internet to both expand the scope of existing crime types and develop new ones, particularly in the area of fraud which has spawned new (cyber) crimes such as interference with internet and computer access. As questions aimed at identifying fraud and other cyber offences were not part of the original survey design, it is not currently possible to include these new offences in the main estimate of CSEW crime.

In order to address this issue, over the last 18 months ONS has been engaged in a programme of work to place questions relating to fraud and cybercrime onto the survey, and thus enable the CSEW to provide such estimates for the first time. The research has involved several stages of development including: a desk review; the development and testing of new questions using a mix of qualitative and quantitative research; and a large scale field trial of 2,000 interviews. The first two of these stages were undertaken by NatCen Social Research on behalf of ONS and the findings published in April 2015[1]. Building on the initial development work, ONS has spent the last nine months working with the CSEW field contractor, TNS, to implement the recommendations made by NatCen including the large scale field trial. This report details the findings of the field trial and recommendations for taking the work forward.

[1] Developing questions on fraud and cybercrime for the CSEW, Collins, D et al

2. Background

The Crime Survey for England and Wales (CSEW), is a face-to-face victimisation survey in which people resident in households in England and Wales are asked about their experiences of a range of crimes in the 12 months prior to the interview. As a result the survey provides an estimate of the number of victims and the number of incidents of crime experienced by the household population. These are derived from two linked modules of questions referred to as the 'screener' and 'victimisation' modules. The former includes a series of screening questions to identify incidents that are followed up in more detail in the victimisation module. The latter collects details such as what, when, and how the incident occurred. Once the data are returned to a central office, all screener and victimisation modules are reviewed by specially trained coders in order to determine whether what has been reported represents a crime or not, and, if so, what offence code should be assigned to the crime. The coding rules approximate the way in which the police should record the same incident and follow, as far as possible, the Home Office Counting Rules for recorded crime. Apart from some minor changes, the code frame and the instructions to coders for the core survey have remained stable since 1982.

Until recently fraud or cyber-crime were not covered by either the screener or victim modules and therefore not included in the survey's main estimates. Attempts have been made in the past to explore elements of these crime types through ad hoc modules of questions included in the survey. However, it was not possible to incorporate these into the headline figures due to different data collection approaches and challenges around measuring fraud and cyber-crime.

ONS therefore established a project in early 2014 to explore the feasibility of covering fraud and cyber-crime in the main crime survey estimates. The National Centre for Social Research was commissioned to take the initial phase of this work forward.

2.1 Prior development work

The initial development work ran from June 2014 to January 2015. Findings from the desk research stage informed the development of a number of new screener questions, designed to identify victims who had experienced different types of fraud and cyber crime. It also informed modifications to some of the existing follow up questions, such as where the incident took place and the cost of incident. The next stage of development cognitively tested a series of questions by capturing people's thought processes and understanding as they respond to the questions. The testing therefore assessed participants' initial reaction to the new screening questions; and their understanding of the questions.

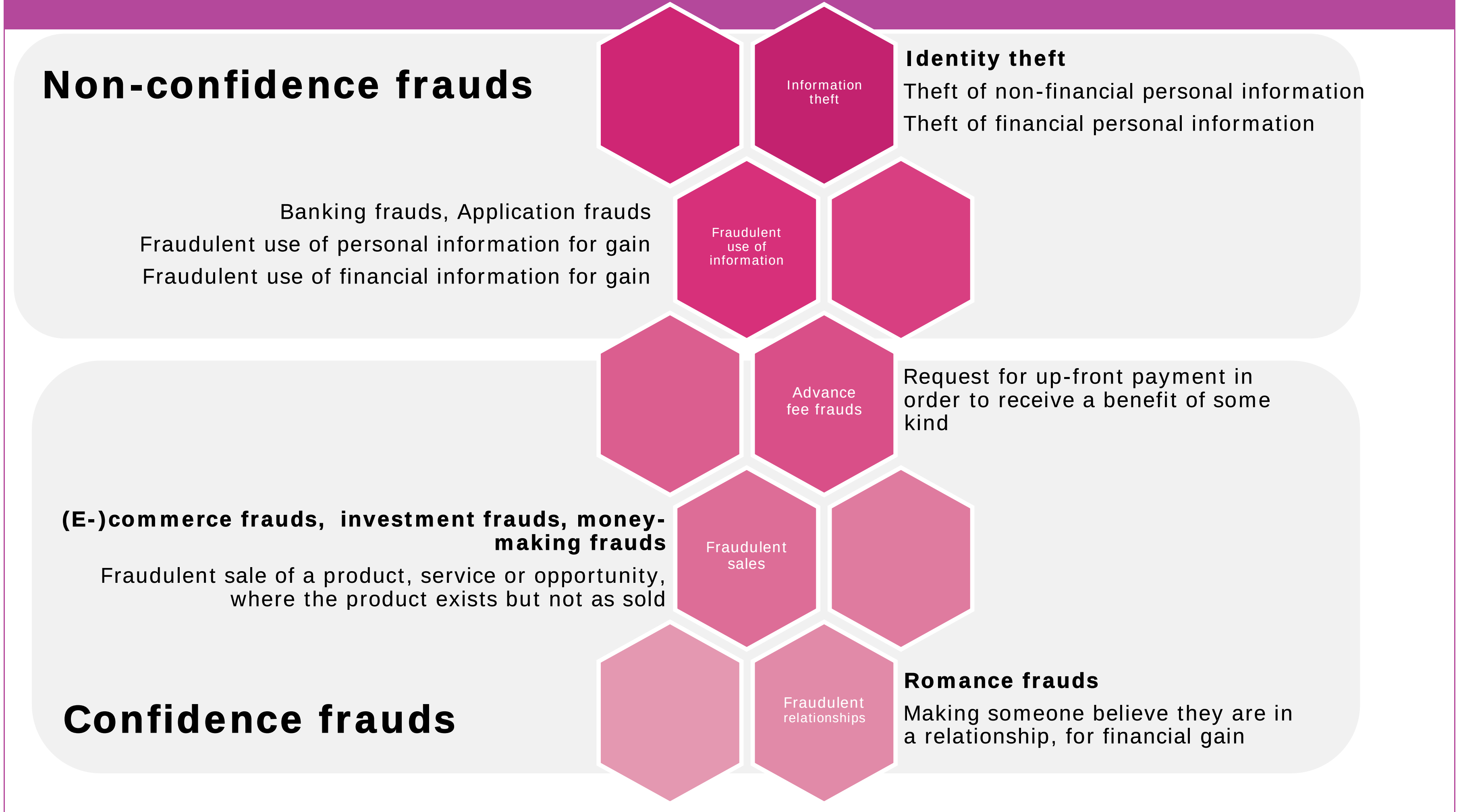
In addition, the testing explored any difficulties participants had in being able to answer the questions, such as recall of the event, and whether the new screener questions picked up the types of crimes they were designed to identify.

2.1.1 Fraud

The review identified five broad, potentially overlapping categories of fraud, comprising of eight ‘types’. In the vast majority of cases, it was found that these frauds can be perpetrated entirely offline, supported by online activity, or be perpetrated entirely online. For this reason, the screener questions developed on fraud were kept broad, focusing on the intrinsic characteristics of the different ways of committing fraud. This focus was also consistent with the aim of ‘future-proofing’, as far as possible, the new screener questions. This aim was concerned with minimising the need for changes to question wording to reflect changes in technology or the modus operandi of fraudsters. Two conceptual categories were identified - confidence and non-confidence frauds - which cover five sub-categories. Figure 1 shows the five categories and how they map onto the confidence/non-confidence classification.

Figure 1

Mapping of confidence and non confidence frauds to different crime types



Non-confidence frauds

Information theft

Identity theft

Theft of non-financial personal information

Theft of financial personal information

Banking frauds, Application frauds

Fraudulent use of personal information for gain

Fraudulent use of financial information for gain

Fraudulent use of information

Advance fee frauds

Request for up-front payment in order to receive a benefit of some kind

(E-)commerce frauds, investment frauds, money-making frauds

Fraudulent sale of a product, service or opportunity, where the product exists but not as sold

Fraudulent sales

Fraudulent relationships

Romance frauds

Making someone believe they are in a relationship, for financial gain

Confidence frauds

2.1.2 Theft of personal information

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

2.1.3 Interference with internet and computer access

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

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

2.2 Development stage recommendations

The initial development work was concluded in early 2015 making the following recommendations[2].

- Further testing of the new screener and victimisation module questions to assess whether revised and or new questions are being consistently understood as intended.

- A large-scale field test to assess the impact the new screener and victimisation questions have on the CSEW's: response rates; interview length; and data quality.

- It was also understood that the inclusion of a large scale field test would enable the process of coding incidents of fraud to be developed ahead of it, allowing the editing program and manual to be tested and further refined. Guidance for coders would also be developed in light of experience gained for the large scale field test.

The new screener questions developed at the end of the initial development period went through a further iteration of development which indicated that the screener questions (but not the victim module questions) could be included on the main CSEW. It was recommended that the questions should be asked of half the CSEW sample to test for any effect new screener questions may have on existing questions by comparing results across both arms of the experiment.

[2] http://www.ons.gov.uk/ons/guide-method/method-quality/specific/crime-statistics-methodology/methodological-notes/questions-on-fraud-and-cybercrime-for-the-csew---paper.pdf

3. Field test methodology

The methodology for the field trial was designed to mirror as closely as possible the standard CSEW fieldwork. A representative sample of 4,196 addresses across England and Wales was selected from the Royal Mail Postcode Address File (PAF). The data was weighted using design weights based on the address selection probability, the multi-dwelling unit count, and the number of adults count. There is no non-response element to the weighting, or calibration to populations estimates as there is on the existing survey data. This is unlikely to produce significant differences between estimates from the trial data and those that will be produced when the questions are live within the CSEW.

All selected addresses were sent a copy of the CSEW advance letter informing the household about the survey and that an interviewer would be calling. The letter was accompanied by an information leaflet and a book of 6 first class stamps, as in the main survey. Following receipt of the survey letter households were contacted by an interviewer to complete the interview in their home. Where there was more than one adult aged 16 or over living at the address the respondent was selected at random to take part in the survey. For the standard CSEW a second interview may be conducted with a 10-15 year old living in the household but this was not required for the trial. Overall a response rate of 53% was achieved. This is a lower response rate than that achieved for the standard CSEW (the 2014-15 CSEW response rate was 70%) reflecting the shorter fieldwork period available for the field trial[3].

The field trial questionnaire used a subset of the CSEW modules and the developed fraud and cyber-crime screener and victim form questions. The questionnaire included the following modules:

- Household box
- Perceptions of crime
- Screener questionnaire (including six new screener questions covering fraud and cyber-crime)
- Victimisation module – traditional crimes
- Victimisation module – fraud and cyber-crimes
- Demographics

There was no self-completion element included in the survey. The average length of the field trial survey was 28 minutes.

[3] Addresses in the core CSEW sample remain in field for up to six months while the field trial sample was only active for a maximum of 3 months.

4. Split sample test and field trial results

Screener questions (Split sample launch)

In addition to the field trial the new fraud screener questions were added to the core CSEW survey between April 2015 and October 2015. These new questions were added for respondents from two sub-samples (those answering follow up modules C and D) only. This split sample test was included to monitor whether the inclusion of the new screener questions had any impact on the existing questions (table 4.1). Overall there was no significant difference between the responses from those in follow up A and B (FUA and FUB - not asked the new questions) and those in follow up C and D (FUC and FUD - who were asked the new fraud and cyber screening questions). At the time of writing data was only available for the April-June 2015 quarter. The analysis will be repeated when the July-September data is available. Some small differences were observed that, while not statistically significant, suggest that further monitoring of the impact of adding the new fraud questions should be conducted.

It is therefore recommended that the split sample approach is continued between October 2015 and March 2016 to minimise the risk to the core estimates from any impact in adding these new questions.

Proportion of respondents completing a victim form

The proportion of respondents completing a victim form will have a significant impact on the interview length once the new fraud and cyber-crime questions are included in the live survey. Including new types of incidents will inevitably result in an increase in the numbers of victims identified.

In the 2014-15 CSEW 18% of all respondents completed a victim form. Between April and June 2015 17% of all respondents reported a traditional incident which was followed up in a victim form. In addition a quarter of respondents (25%) reported a potential fraud or cyber incident which was followed up in a separate victim form. Six per cent of respondents reported experiencing both a traditional crime and a possible fraud offence. These respondents who have experienced both traditional and fraud offences would be expected to complete a victim form for each incident (up to the point at which the limit of six forms is reached).

Table 4.1 Response to traditional screener questions CSEW April-June 2015

#	Screener question	% Victims (FUA and FUB)	Base	% Victims (FUC and FUD)	Base
1	mottheft	0.37	3,238	0.51	3,121
2	motstole	2.63	3,238	2.88	3,121
3	cardamag	4.85	3,238	4.87	3,121
4	biktheft	2.90	1,932	2.36	1,862
5	prevthef	1.03	390	0.75	399
6	prevdam	0.51	390	0.25	399
7	prevtry	0.77	390	0.50	399
8	prevstol	0.51	390	0.50	399
9	proside	3.85	390	3.26	399
10	prdeface	0.51	390	1.00	399
11	Homethef	0.00	390	0.75	399
12	yrhothef	0.82	3,668	0.94	3,517
13	yrhodam	0.12	4,059	0.08	3,918
14	yrhotry	0.96	4,059	0.94	3,918
15	Yrhostol	0.17	4,059	0.36	3,918
16	Yroside	2.46	4,059	3.09	3,918
17	Yrdeface	1.55	4,059	1.28	3,918
18	persthef	0.79	4,059	0.89	3,918
19	trypers	0.37	4,059	0.48	3,918
20	oththef	1.28	4,059	1.05	3,918
21	delibdam	0.27	4,059	0.48	3,918
22	delibvio	1.55	4,059	1.43	3,918
23	threviol	2.14	4,059	2.68	3,918
24	sexattak	0.10	4,059	0.15	3,918
25	hhldviol	0.18	2,837	0.22	2,725

Victim	16.09	4,059	17.53	3,918

Between April and June 2015 37% of respondents overall reported experiencing either a potential traditional or a fraud or cyber-crime incident. This is a significant increase from 18% of respondents who completed a victim form in 2014-15 and the implications for the interview length are discussed in chapter 9.

Table 4.2 shows the proportion of respondents who reported a potential traditional or fraud and cyber-crime between April and June 2015.

Table 4.2 Proportion of respondents reporting potential incidents (April-June 2015)

	Proportion of potential victims identified
Traditional	11
Fraud	19
Both	6
Total	37

Limiting the number of victim forms

During the fraud field trial the number of victim forms that could be completed by each respondent was increased to seven. This included up to six traditional victim forms and a seventh fraud and cyber-crime victim form. For example if a respondent reported three traditional crimes and eight incidents of fraud and cyber-crime they would have completed three traditional victim forms and four fraud and cyber-crime victim forms. Table 4.3 shows the number of victim forms completed by respondents. It was extremely rare for respondents to complete the maximum of seven victim forms with only 0.3% of respondents doing so. This suggests that the standard limit of six victim forms could be maintained with minimal loss of information.

Table 4.3 Number of victim forms completed (Fraud field trial 2015)

Number of victim forms	**n**	**%**
0	1403	67.7
1	437	21.1
2	130	6.3
3	66	3.2
4	15	0.7
5	8	0.4
6	7	0.3
7	6	0.3
Total	2,072	100

5. Recording cyber incidents

Part of the development work focussed on the recording of cyber incidents and how best to ensure that these can be identified in the data.

Throughout the initial question development stage it was decided not to focus on the method by which crimes occur at the screening stage but rather that the crime itself should be recorded and detail subsequently collected about how it was committed. This decision was based primarily on the need to future proof the questions, ensuring they would still be applicable in a number of years. This approach also mirrors how traditional crimes are recorded by the survey.

As part of the fraud field test a question was added to the victim form to record whether there was any cyber element to the offence. This was the only question added that clearly identifies whether the incident should be recorded as a cyber incident.

There does appear to have been some misunderstanding among respondents as to what would constitute any internet or online activity being involved in the offence and particularly around the extent to which this type of activity was involved to record a yes answer at this question (i.e. did the entire offence have to be committed online or whether just suspicion that details were obtained via the internet would be sufficient to record a yes here). As this is such a key variable for analysis it is recommended that a further question to check this is added. This is an approach taken by the core victim form – key points such as whether there was any theft, whether any violence was involved are asked at least twice.

Further recommendations include adding further clarification to the cyber question below (recommended revisions in text are in blue).

V88 SL **[ASK ALL]**

ASK OR RECORD

As far as you are aware, was the internet or any type of online activity related to any aspect of the offence?
INTERVIEWER NOTE: This includes cases where the internet may have been used to obtain the victim's details as well as online and cyber incidents.

1. Yes
2. No

WCYBER SL **[ASK ALL]**

Can I just check, was the internet, any type of online activity or internet-enabled device related to any aspect of the offence?
INTERVIEWER NOTE: This includes cases where the internet may have been used to obtain the victim's details as well as online and cyber incidents.

3. Yes
4. No

Following further discussions it was identified that a cyber flag should be applied to all incidents (both traditional and fraud incidents). This will enable the coding of cyber threats via the traditional victim form.

The recording of any cyber element to the offence will also form part of the offence coding task. Guidance will be added to the coding manual and coders will be expected to use the responses to questions V88 and WCYBER as well as all other information in the victim form to accurately classify whether an incident should be recorded as a cyber incident or not.

This was added to the coding for the field trial but following review it was found to require some further development to improve the accuracy of this classification. A number of steps are recommended to address this:

- An additional question added to the victim form to identify cyber-crime,
- Further guidance regarding the coding of the cyber flag to be incorporated into the coding manual
- Additional briefing for the coding team on coding the cyber flag
- Coding of the cyber flag to be added to the verification process

6. Offence classification

Part of the development work focussed on the criteria for including offences as in scope and the development of an appropriate classification system for fraud and cyber offences. Wherever possible this classification was based on the Home Office Counting Rules (HOCR) for fraud, which also include Computer Misuse Act Offences.

Early in the development it was envisaged that only those frauds resulting in loss would be included in the survey. However, it became apparent that this would not reflect a substantial number of incidents of fraud which would be recorded as offences by Action Fraud and where the victim may have been significantly affected, even if there was no actual loss incurred. It was therefore decided that incidents of fraud should be included as in scope in all cases where a specific intended victim can be identified. This reflects the HOCR criteria for inclusion.

The offence categories for coding of fraud and cyber-crime were as follows:

- Code 101 – Confidence fraud – with loss
- Code 102 – Attempted confidence Fraud – with no loss
- Code 103 – Unauthorised access to bank/credit accounts – with loss
- Code 104 - Unauthorised access to bank/credit accounts – no loss
- Code 105 – Unauthorised access to personal information - with loss
- Code 106 – Unauthorised access to personal information – no loss
- Code 107 – Attempted access to bank/personal information
- Code 108 – Computer virus
- Code 109 – Fraud falling outside the survey's coverage

It should be noted that in law there is no offence 'attempted fraud'. This category is used to refer to cases where a fraud has taken place but the victim has not lost anything as a result of the fraud.

Examples of incidents recorded for each code:

Code 101 – Confidence fraud with loss

This includes cases where the victim has somehow been tricked or deceived and this deception has resulted in a loss of money. Cases are included in this code even if the money is subsequently refunded by a bank, credit card company or someone else.

“The respondent ordered a hairdryer via the internet and it never arrived. She sent about 10 e-mails and found that the address wasn't active. She had paid by debit card and the credit card company restored the money”.

“The respondent wanted a toilet installed. The builder wanted a deposit, he handed over £400 and never saw the builder again”.

“I was at my allotment, a young man started talking to me. He seemed genuine and he said he had 40 bags of compost. I brought him to my house and paid him £30 and I never saw him again. I heard that he was caught conning elderly people in the area and he is now in prison”.

Code 102 - Attempted confidence Fraud – with no loss

This code covers cases where the victim has been tricked or deceived in some way but they have not lost any money as a result of the deception, possibly because the fraud is identified before they have a chance to lose any money.

“I received a phone call telling me I had won money and that if I sent £20 that would release the money they asked for my bank details and I started giving them but then stopped before I gave them. I told them I couldn’t afford it and hung up”.

“A phone call suggested that there was something wrong with the respondent’s computer. It was supposedly from Microsoft. He was asked to do something to correct the problem by them having direct control of the machine. A form came up on the screen asking him to give financial details and agree payment and at that point the respondent declined.”

“We were looking to buy a car off auto trader we emailed a man who emailed us back he said he worked for the army and wanted us to send money for a car he would put on a plane to us when he had the money. We did not do this and had no further contact”.

Code 103 – Unauthorised access to bank/credit accounts – with loss

This code includes cases where the victim’s accounts have been accessed without authorisation. In may cases the victim will not have had any contact with the offender. Cases are included here even when the money is subsequently refunded by the bank.

“I had a phone call from banks fraud dept to tell me I had unusual transactions in china of £200 plus purchases. respondent confirmed that she was not responsible for the transactions and the money was refunded.”

“The bank phoned me and asked if I'd used my credit card that day and I hadn't. They told me someone had tried to order something using my card. They stopped it and they issued me with a new card but when I got the bill there was a transaction that was not mine but they said they would remove it”.

“It was Sunday and we were off to do some shopping and I checked my account and I noticed there were strange transactions. There were 6 transactions made from one company that I hadn’t used”.

Code 104 - Unauthorised access to bank/credit accounts – no loss

This code includes cases where there has been an attempt to access the victim’s accounts but where the attempt has been unsuccessful. This includes cases where the financial institution stopped the transaction before it took place but not cases where the transaction took place but the money was subsequently refunded.

“Received a letter from my bank telling me that a number of direct debits had been set up to various payees without my knowledge. I believe this is my ex wife. I do not use this a/c and so there was no money and the bank would not pay them”

“I was out of the country in Turkey, on holiday. Trying to sort out an administrative problem, I left my credit card with the desk at a golf course. Subsequently on my return to UK I was contacted by the bank because an attempt had been made to withdraw £400 during that time.”

“Someone was trying to use my credit card details to charge a large hotel bill”.

Code 105 – Unauthorised access to personal information - with loss

This code includes access to the victim’s accounts (not including bank or credit card accounts) where there has been a loss of money or a loss of information. This includes unauthorised access to email and social media accounts.

“I had my social media hacked & had to change all my passwords. It also loaded a virus on my computer but I managed to clear it before it caused any damage.”

“Online – someone obtained personal details and opened and Experian account.”

Code 106 – Unauthorised access to personal information – no loss

This code includes access to the victim’s accounts (not including bank or credit card accounts) where there has been no loss of money or a loss of information.

“My ex partner hacked my Facebook, she obviously knew the password, she intimidated a 3rd party to stop speaking to her brother by private messaging him”.

“Somebody hacked into my email account & tried to access contact information. Hotmail sent a message to my phone asking if I was trying to log in from Thailand. It was obviously not me so I changed my password.”

“Someone set up a fake account on face book in my name with my full address etc.. stealing my entire identity, including family photos etc. They used the account to harass me & create a rift between members of my family.”

Code 107 – Attempted access to bank / personal information
This code covers unsuccessful attempts to access bank or other personal information. If the attempt to access the account is successful but no money is taken this should be recorded as either a code 104 or 106 depending on the account accessed. This code only includes cases where the attempt to access the account was unsuccessful.

"The bank got in touch with respondent as someone had tried to access his account to withdraw approx £3000 through the internet. no internet site was known."

Code 108 – Computer virus
This code includes all cases of computer misuse and computer viruses. Unsuccessful attempts are not included in this code.

"We got a virus on the computer which was spreading, making the computer more disabled by the hour. We used another computer to try and find out more and if there was a fix. We found some advice but people wanted paying for it, we then found some free advice and then we managed to work through and get it fixed"

"A bug came through an email from unknown source and infected my computer which has caused slowing of my computer and interference with using the internet. It cannot be eradicated."

"I opened an email and computer became infected with virus which shut down windows.I had to re install windows."

Code 109 – Fraud falling outside the survey's coverage
This code covers all cases of fraud falling outside the scope of the survey. This includes cases where there is no specific intended victim, for example receipt of generic spam e mails asking for personal information, non targeted phone scams etc. It also includes any cases where the fraud was committed against a business rather than a private individual.

Classification of incidents and lessons from the field trial

Incidents of fraud and cyber-crime recorded during the fraud field trial were coded by TNS coders and by ONS coders independently. This identified a number of discrepancies in the coding both within teams but also between the two teams. The most significant discrepancy was around the identification of the specific intended victim and therefore whether the case should be classified as in scope or out of scope. This discrepancy was due in part to insufficient information contained within the incident description to enable the coder to accurately assess whether or not the victim was a specific intended victim. It was also felt that additional guidance would be helpful for coders around this issue to facilitate more accurate classification.

Further briefing has been provided to interviewers regarding the information to be collected in the incident description which should help to improve the consistency of the coding. In addition the coding guidance is being reviewed and a number of scenarios have been referred back to Action Fraud to check how they should be classified. All cases from the field trial will be coded a second time to check the consistency of the coding before coding the cases recorded from the main CSEW.

7. Interview length

The average length of the 2015-16 CSEW is 47 minutes (based on interviews achieved to 4th August 2015).

Two modules will be removed from the survey in October, follow up D (currently asked to a quarter of all CSEW respondents) and the financial loss and fraud module (currently asked to three quarters of all CSEW respondents).

- Average length of follow up D module (for those who complete it) is 2.3 minutes.
- Average length of the financial loss and fraud module (for those who complete it) is 2.8 minutes

Overall, once we take into account the fact that module D is asked to only a quarter of respondents, we might expect that deleting follow up D would save 0.6 minutes and deleting the financial loss and fraud module would save 2.1 minutes of interview length. This would result in a reduction of c. 2.7 minutes to the survey length and an estimated survey length of 44.3 minutes from October BEFORE the inclusion of victim forms for fraud and cyber offences.

The length of the CSEW interview increases with the number of victim forms. Overall, if more victim forms are completed on average by victims then the average length of the interview for victims of crime will increase. Based on the estimates from the April-June 2015 survey interviews we would expect the average length of interview for victims of crime to increase from 64 minutes to 67 minutes. Overall this would result in an overall questionnaire length of **52 minutes**. However should the new questions be added for half sample only we estimate this will result in an overall interview length of **49 minutes**.

One important consideration for the survey development is the balance of interview length and the maximum interview length experienced by respondents. The average interview length for the CSEW for a victim who has experienced four or more incidents is 98 minutes. This is a significant time commitment required from respondents and far above the average length. Including the fraud and cyber-crime questions is likely to push more respondents into this 4+ bracket of those experiencing extremely long interviews. We do not believe that this maximum length should be increased as this would be likely to have an impact on the quality of the data and may also impact on the response rate.

8. Field trial - Initial estimates of fraud and cyber-crime

Following the initial development work new screener questions were launched on the main CSEW in April 2015 as a split sample experiment alongside a large scale field trial of the survey. This took place between 20th May and 9th August 2015 and was designed to replicate the existing CSEW with the addition of the new fraud and cyber-crime screener questions and victimisation modules alongside the screener and victimisation modules for traditional crimes.

The purpose of the field trial was to test the questions in the context of a live survey. The trial also aimed to assess the impact the new questions would be likely to have on the standard CSEW survey when integrated onto the survey. This included an assessment of any impact the questions may have on reporting of traditional incidents of crime and the extent to which the interview length would be extended by the inclusion of the new questions.

Overall the split sample test and field trial aimed to:

- Provide an initial estimate of the extent of victimisation of fraud and cyber-crimes
- Establish an understanding of the degree of overlap between these offences and traditional crimes
- Estimate the impact of adding these new questions on questionnaire length
- Assess whether adding the new screener questions would have any impact on existing estimates

The field trial included 2,072 interviews with households.

Being based on a reasonably large and representative sample, the field trial enables the production of an indicative set of estimates. However, as the estimates are based on field trial data and coded using a developmental coding procedure the results may vary from future estimates produced by the CSEW as systems and processes develop and bed-in.

Fraud

Data from the field trial was aggregated into two fraud categories; fraud with loss, and fraud without loss. It should be noted that the fraud with loss category includes some victims who later were reimbursed by the bank or financial institution and therefore suffered no personal loss (although the bank or other institution may have).

The total number incidents of fraud estimated by the field trail were just over 5.1 million (table 8.1), this includes a wide range of frauds including:

- confidence frauds including attempts where the intended victim engaged with the fraudster but suffered no loss
- Unauthorised access to bank/credit accounts with or without loss
- Unauthorised access to other personal information (e.g. social media or email accounts) with loss
- Attempted access to bank/personal information

The estimates provided cover a broader coverage of fraud than previously attempted by the CSEW modules on banking and plastic card fraud.

Table 8.1 Fraud and Computer Misuse - Incident and number of victims

Offence group	Number of incidents (000s):	Incidence Rate per 1,000 adults:	Number of victims (000s):	Victim Rate per 1,000 adults:
Fraud	5,110	112	3,757	82
Fraud with loss (including those reimbursed)	2,648	58	2,079	46
Fraud no loss	2,462	54	1,856	41
Computer misuse	2,460	54	2,113	46
Unauthorised access to personal information (including hacking)	404	9	404	9
Computer virus	2,057	45	1,741	38
Total	7,571			

The total number of victims of fraud in the 12 months prior to interview estimated by the field trial was 3.8 million. Just over half of these incidents (2.1 million) were the victims of fraud with loss although this includes some who were later reimbursed by the bank or financial institution.

Of those incidents where a loss was initially reported, victims received financial compensation in three quarters (78%) of cases, with well over half reimbursed in full 62%.

The Field Trial went on to ask victims how much money was taken, although the trial data did contain a large volume of missing data, it was clear that in most incidents victims lost between £50 and £500 (Table 8.2).

Table 8.2 Financial loss – all victims

	Percent
Less than £20	14.3
£20 - £49	4.0
£50 - £99	23.0
£100 - £249	18.6
£250 - £499	18.4
£500 - £999	9.2
£1,000 - £2,499	5.9
£2,500 - £4,999	6.3
£10,000 - £19,999	0.3
Total	**100**
Unweighted base	68*

Unweighted base excludes 25 missing cases

Of those who did not receive compensation, the majority lost less than £100 although in one case the loss which was not refunded was between £2,500 and £5,000 (Table 8.3).

Table 8.3 Financial loss – without compensation

	Percent
Less than £20	18.5
£20 - £49	17.1
£50 - £99	23.5
£100 - £249	8.9
£250 - £499	18.7
£1000 - £2,499	8.6
£2,500 - £4,999	4.8
Total	100
unweighted base	15

Computer misuse

The number of incidents of computer misuse estimated by the field trial in the 12 months prior to interview was 2.5 million (Table 8.1) .Computer misuse falls into two categories; unauthorised access to personal information (including hacking); and cases of a computer virus where the computer or internet enabled device became infected. Unsuccessful attempts at installing a computer virus which were, for example blocked by anti-virus software, were not included. Estimated incidents of computer viruses infecting internet enabled devices far outweighed unauthorised access to personal information (2.1 million incidents compared with 400,000 respectively).

Whilst some of these incidents are at the more serious end of crime harm spectrum, by nature they also include a large number of minor incidents. It is recommended that further consideration be given as to how the wide range of such incidents should be included alongside existing CSEW incidents. It should also be noted that consideration should be given to the inclusion of other cyber related events such as online harassment which are also not currently included in the main CSEW.

It is also recommended that further consideration given to the classifications of fraud and cyber crime incidents to be used in the published statistics to ensure they are clear and understandable to users. This should inform any possible changes to the coding classifications that underpin it.

9. Summary and Recommendations

Overall the field trial showed that the structure and format of the questionnaire worked well in the live environment. The screener questions, placed at the end of the existing screener questionnaire, had no impact on the recording of traditional crimes suggesting that the adding fraud and cyber-crime would not impact on the core survey estimates.

The incident descriptions and follow up questions recorded in the victim form generally provided sufficient information for the accurate classification of offences. However it was identified that some further detail would be useful in the incident descriptions, particularly information about what the victim did as a result of any fraudulent activity. Questions within the victim form were also amended slightly to add further clarity around this.

Following the field trial the offence classification and its guidance documentation will be reviewed to ensure that all scenarios identified by the trial are covered by the coding guidance. This review will also include the classification of cyber offences and further guidance about how these incidents should be recorded.

- In order to minimise the risk of any disruption to the time series data and the risk of significantly extending the interview length the new fraud and cyber-crime screeners and victimisation module should be added for half sample only between October 2015 and March 2016. These questions should continue to be asked for modules C and D only.

- In order to avoid excessive interview lengths the cap on the number of victim forms completed by a single respondent should remain at six victim forms.

- Clearly define a series of incidents – a slightly amended definition of a ‘series’ is required for fraud incidents to deal with multiple amounts of money taken in a single incident.

- Cyber incidents will be identified by a flag in the data from (F)V88 rather than by separate offence codes. As this will be a key measure we recommend adding a further check question to record any cyber element to the offence. This question will be added to the victim form for both traditional and cyber-crimes.

    - In addition coders will be asked to record whether or not the incident was a cyber-incident during the offence coding.

- Minimise the burden on respondents by ensuring that the length of the fraud victim form is kept to a minimum by deleting any questions not essential for offence coding.

- It is recommended that further consideration be given as to how the wide range of such incidents should be included alongside existing CSEW incidents.

- Consideration should be given to the inclusion of other cyber related events such as online harassment which are also not currently included in the main CSEW.

- It is also recommended that further consideration given to the classifications of fraud and cyber crime incidents to be used in the published statistics to ensure they are clear and understandable to users. This should inform any possible changes to the coding classifications that underpin it.

Appendix A - Screener questions

[ASK ALL MODULE C AND D]

INTRO1

The next set of questions relate to fraud; including being tricked out of money or goods, misuse of your personal details, unauthorised access to your bank, email or social media accounts, computer viruses and so on.

FININC **[READ OUT IF ANY TRADITIONAL SCREENERS =1]**

26

Sometimes following a crime, stolen items such as bank cards or computers or internet enabled devices may be used to gain access to a person's accounts or personal information.

Looking at this card, in the time [since the first of ^DATE^] did any of these things happen as A DIRECT RESULT of [the incident/any of the incidents] you have just told me about?

SHOWCARD M9

1. Your personal information or account details were used or tried to be used to obtain money, or buy goods or services
2. You were tricked or deceived out of money or goods (in person, by telephone or online)
3. Someone TRIED to trick or deceive you out of money or goods,(in person by telephone or online)
4. Your personal information or details were accessed or used without your permission
5. An internet-enabled device of yours was infected or interfered with, for example, by a virus

1. Yes
2. No

NFININC **[ASK IF FININC=1]**

As far as you are aware, how many times has this happened as a DIRECT RESULT of an incident you have already told me about? Please tell me how many separate incidents there were.

INTERVIEWER: WE WANT TO RECORD HERE THE NUMBER OF TIMES THIS TYPE OF INCIDENT HAS OCCURRED. WE DO NOT WANT TO RECORD HOW MANY TIMES WITHIN EACH INCIDENT THE PARTICIPANT'S INFORMATION WAS USED.

ENTER NUMBER_________

96 More than 95

97 Too many to remember

NONCON 27 **[ASK ALL]** ***[USE OF PERSONAL DETAILS]***

[Apart from anything you have already mentioned], in the time [since the first of ^DATE^] has your personal information or account details been used to obtain money, or buy goods or services without your permission or knowledge?

1. Yes – ASK **NNONCON**
2. No – GO TO **CON**

NNONCON **[ASK IF NONCON=YES]**

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

INTERVIEWER: RECORD NUMBER OF **SEPARATE** INCIDENTS. MULTIPLE THEFTS DISCOVERED AT THE SAME POINT FROM THE SAME ACCOUNT WOULD BE A SINGLE INCIDENT (E.G. MULTIPLE USE OF A STOLEN CARD COUNTS AS A SINGLE INCIDENT). ENTER NUMBER_________

96 More than 95

97 Too many to remember

CON 28 **[ASK ALL]** ***[TRICKED OUT OF MONEY OR GOODS]***

[Apart from anything you have already mentioned] In that time has anyone tricked or deceived you out of money or goods, in person, by telephone or on-line?'

INTERVIEWER NOTE: ONLY INCLUDE CASES WHERE PARTICIPANT LOST MONEY OR GOODS AS A RESULT OF BEING TRICKED OR DECEIVED. DO NOT INCLUDE ATTEMPTS WHERE PARTICIPANT DID NOT LOSE ANYTHING.

1. Yes – ASK **NCON**
2. No – GO TO **CMACT**

NCON **[ASK IF CON=YES]**

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

ENTER NUMBER_________

96 More than 95

97 Too many to remember

TRYCON **[ASK ALL]** ***[ATTEMPT TO TRICK OUT OF MONEY OR GOODS]***

29

[Apart from anything you have already mentioned] In that time has anyone TRIED to trick you or deceive you out of money or goods, in person, by telephone or on-line?'

1. Yes – ASK **NCON**
2. No – GO TO **CMACT**

NTRYCON **[ASK IF TRYCON=YES]**

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

ENTER NUMBER_________

96 More than 95

97 Too many to remember

CMACT [ASK ALL] ***[UNAUTHORISED ACCESS TO PERSONAL INFORMATION]***

30

[Apart from anything you have already mentioned], in that time has anyone stolen your personal information or details held on your computer or in on-line accounts (e.g. email, social media)?

1. Yes – ASK **NCMACT**
2. No – GO TO **VIRUS**

NCMACT **[ASK IF CMACT=YES]**

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

ENTER NUMBER_________

96 More than 95

97 Too many to remember

VIRUS **[ASK ALL]** ***[COMPUTER VIRUS]***

31

[Apart from anything you have already mentioned], in that time…has a computer or other internet-enabled device of yours been infected or interfered with, for example by a virus?

DO NOT INCLUDE VIRUSES WHICH WERE BLOCKED BY ANTI VIRUS SOFTWARE BEFORE INFECTING THE DEVICE

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

1. Yes – ASK **NVIRUS**
2. No – GO TO **PROBES**

TOTNVIR **[ASK IF VIRUS=YES]**

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

ENTER NUMBER_________

96 More than 95

97 Too many to remember

VIRUSCHK **[ASK IF NVIRUS >1]**

Can I check how many, if any, of these incidents were blocked by anti-virus software?

ENTER NUMBER_________

97 More/too many to remember

CAPI CHECK – CHECK THAT VIRUSCHK<TOTNVIR

INTERVIEWER: You have coded more incidents of computer virus stopped by anti-virus software than experienced in total. Please go back and amend your coding.

NVIRUS **[ASK IF VIRUS=1] – DERIVED VARIABLE**

COMPUTE NVIRUS = TOTNVIR-VIRUSCHK

TFRAUDCK [ASK IF NFININC>0 OR NNONCON>0 OR NCON>0 OR NTRYCON>0 OR NCMACT>0 OR NVIRUS>0]

INTERVIEWER: THE NEXT SET OF QUESTIONS CHECK INSTANCES OF DOUBLE COUNTING ACROSS SCREENERS.

+SCRNCHK [ASK IF NFININC>0 OR NNONCON>0 OR NCON>0 OR NTRYCON>0 OR NCMACT>0 OR NVIRUS>0]

INTERVIEWER: BELOW IS A CHECK LIST OF INCIDENTS OF FRAUD COMMITTED AGAINST THE RESPONDENT IN THE PAST YEAR

You mentioned the following incidents:

PLEASE CONFIRM THE LIST WITH THE RESPONDENT - CHECK THAT EVERYTHING HAS BEEN MENTIONED AND **NOTHING COUNTED TWICE**

Incident	**Number of incidents**
Fraud/Virus following other crime	**NFININC**
Personal details used to obtain money or goods	**NNONCON**
Tricked out of money or goods	**NCON**
Attempt to trick out of money or goods	**NTRYCON**
Stolen Personal Information	**NCMACT**
Computer Virus	**NVIRUS**

Can I just check were any of these incidents related?

INTERVIEWER: FOR RELATED INCIDENTS CODE ONE INCIDENT ONLY, CODE AT FIRST INCIDENT RECORDED.

FOR EXAMPLE: IF PERSONAL DETAILS STOLEN AS A RESULT OF A COMPUTER VIRUS CODE ONE INCIDENT OF “PERSONAL DETAILS USED TO OBTAIN MONEY OR GOODS” ONLY.

RECODE NUMBER OF INCIDENTS HERE IF NECESSARY.

Incident	**Number of incidents**	**Number of non-related incidents**
Fraud following other crime	**NFININC**	
Personal details used to obtain money or goods	**NNONCON**	
Tricked out of money or goods	**NCON**	
Attempt to trick out of money or goods	**NTRYCON**	
Stolen Personal Information	**NCMACT**	
Computer Virus	**NVIRUS**	

Appendix B- Field test fraud victimisation module

VICTIMISATION MODULE – FRAUD OFFENCES

S ***{INDICATES THAT THE QUESTION IS ASKED ON SHORT VICTIM FORMS}***

L ***{INDICATES THAT THE QUESTION IS ASKED ON LONG VICTIM FORMS}***

SL ***{INDICATES THAT THE QUESTION IS ASKED ON BOTH LONG AND SHORT VICTIM FORMS}***

ASK IF NFININC>0 OR NNONCON>0 OR NCON>0 OR NTRYCON OR NCMACT>0 OR NVIRUS>0

PRIORITY ORDER:

FROM HIGHEST TO LOWEST

- **NFININC**
- **NNONCON**
- **NCON**
- **NTRYCON**
- **NCMACT**
- **NVIRUS**

TIMING POINT

+DISPLAY [ASK ALL]

SL

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 (E.G. BIRTHDAYS, ANNIVERSARIES, ETC.) IF RESPONDENT UNAWARE WHEN INCIDENT TOOK PLACE RECORD WHEN THEY DISCOVERED THE INCIDENT (FOR EXAMPLE WHEN THE BANK CONTACTED THEM ABOUT A LOSS)

FVINTRO [ASK ALL]

SL

Now I want to ask you some more about the [incident] you reported of [crime type]

[INTERVIEWER: IF SOMEONE ELSE IS PRESENT, IT MAY BE BETTER TO

RETURN ON ANOTHER OCCASION TO COMPLETE THIS VICTIM FORM]

0 [Suspend this Victim Form for now]
1 Continue

{IN INCIDENTS OF DOMESTIC VIOLENCE OR SEXUAL ASSAULT, THE INTERVIEWER IS ALLOWED TO SKIP THE VICTIM FORM IF NECESSARY (E.G. BECAUSE OTHERS WERE PRESENT)}

FWHYSKIP [ASK IF FVINTRO = SUSPEND]

SL

INTERVIEWER: PLEASE EXPLAIN WHY YOU ARE SKIPPING THIS VICTIM

FORM.

Text: Maximum 50 characters

DATE OF INCIDENT (FOR A SERIES OF INCIDENTS)

{DATESER-QTRRECIN ARE ASKED OF THOSE REPORTING A SERIES OF SIMILAR INCIDENTS}

FDATESERA-

FDATESERH [ASK IF SERIES OF SIMILAR INCIDENTS]

SL

You mentioned a series of [NUMBER] similar incidents of [CRIME TYPE] since [the first

Of ^DATE^]. When did these incidents happen? CODE ALL THAT APPLY

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

{IF ALL THE INCIDENTS IN THE SERIES OCCURED MORE THAN 12 MONTHS AGO (i.e. CODE 1) THE RESPONDENT DOES NOT GET ASKED A VICTIM FORM FOR THIS INCIDENT}

FNQUART1 [ASK IF FDATESER = 2]

SL

How many incidents of this kind happened between [^QUARTER^]?

1..97

FNQUART2 [ASK IF FDATESER = 3]

SL

How many incidents of this kind happened between [^QUARTER^]?

1..97

FNQUART3 [ASK IF FDATESER = 4]

SL

How many incidents of this kind happened between [^QUARTER^]?

1..97

FNQUART4 [ASK IF FDATESER = 5]

SL

How many incidents of this kind happened between [^QUARTER^]?

1..97

FNQUART5 [ASK IF FDATESER = 6]

SL

How many incidents of this kind happened between [^DATE^] and the present?

1..97

FMTHRECIN [ASK IF FDATESER IN (2..6)]

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.

{CODE FRAME ON SCREEN SHOWS THE PREVIOUS 12 CALENDAR MONTHS (PLUS THE CURRENT MONTH) FROM THE DATE OF INTERVIEW}

FQTRRECIN [ASK IF FMTHRECIN= DK]

SL

INTERVIEWER: ASK OR RECORD

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

1. Before [the first of ^DATE^] *Don't get asked VF*
2. Between [^QUARTER^]

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

FCHKRECIN [ASK IF FQTRRECIN = DK/REF]

SL

And can I just check, did the most recent incident happen before or after the first of [^DATE^]?

1. Before the first of [^DATE^] *Don't get asked VF*
2. After the first of [^DATE^]

DATE OF INCIDENT (FOR SINGLE INCIDENTS)

FMTHINC2 [ASK IF SINGLE INCIDENT]

SL

You said that, since [the first of ^DATE^], you had an incident of [CRIME TYPE]. In which month did that happen?

{CODE FRAME ON SCREEN SHOWS THE PREVIOUS 12 CALENDAR MONTHS (PLUS THE CURRENT MONTH) FROM THE DATE OF INTERVIEW}

FQTRINCID [ASK IF FMTHINC2= DK]

SL

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

1. Before [the first of ^DATE^] - *Don't get asked VF*
2. *Between [^QUARTER^]
3. Between [^QUARTER^]
4. Between [^QUARTER^]
5. Between [^QUARTER^]
6. Between [the first of ^DATE^] and the present?

**NOTE: in certain months because of the breakdown of quarters there will be an additional code before the existing code 2, ‘In [MONTH]’*

FCHKRECI2 [ASK IF FQTRINCID = DK/REF]

SL

And can I just check, did the incident happen before or after the first of [^DATE^]?

1. Before the first of [^DATE^] *Don't get asked VF*
2. After the first of [^DATE^]

FYRINCIB [ASK IF FMTHINC2= DK AND FQTRINCID = DK]

SL

ASK OR RECORD

Can I just check, did the (most recent) incident take place before or after the first of [^DATE^]?

1. before first of [^DATE^] - *Don't get asked VF*
2. after first of [^DATE^]

DERIVED VARIABLE – CRIMTYPE (Type of Crime recorded at screener)

FININCTYP IF CRIMTYPE=FINIINC

You mentioned that you experienced an incident of fraud or computer misuse following another crime. Thinking about the [most recent/second most recent] incident can you tell me which type of incident it followed:

ADD LIST FROM TRADITIONAL SCREENERS

DESCRIPTION OF INCIDENT

FDESCRINC [ASK ALL]

SL

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, HOW DID IT HAPPEN, WHERE DID IT HAPPEN, WHAT DID THEY DO, WHO WAS THE OFFENDER,?)

FOR COMPUTER VIRUS PROBE FOR TYPE/DESCRIPTION OF VIRUS, HOW WAS THE PROBLEM IDENTIFIED AND RECTIFIED.

Text: Maximum 220 characters

INCIDENT CHECKLIST

{INTERVIEWER TO CHECK (ASK OR RECORD) THE FOLLOWING QUESTIONS. INTERVIEWER TO QUESTION UNLESS CLEAR FROM DESCRIPTION}

FV71 **[ASK ALL]**

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Did the victim lose any money or property, even if they later got it

back?

1. Yes
2. No

FV72A-

FV72I **[ASK IF FV71 = YES]**

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE RESPONDENT

Was the money or property that was lost ... CODE ALL THAT APPLY

1. Personal information (including bank statements, credit cards, passport etc)
2. Money (include cash, money from bank accounts etc)
3. Computer, laptop/tablet, smartphone or other internet enabled device
4. or something else?

FV75 **[ASK ALL]**

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE RESPONDENT

[Was/Apart from what was actually stolen, was] an attempt made to steal anything [else] that belonged to the victim or any other member of the household?

1. Yes
2. No

FV77 **[ASK ALL]**

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE RESPONDENT.

Was any property damaged (i.e. buildings, vehicles, and/or other property)?

DO NOT INCLUDE DAMAGE TO COMPUTERS ETC CAUSED BY A VIRUS/MALWARE

1. Yes
2. No

FV78 **[ASK ALL]**

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE RESPONDENT

Did the victim (or someone in the household) have any contact with the offender(s), or any information about them, such as how many there were?

1. Yes
2. No

FV710 **[ASK ALL]**

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE RESPONDENT

Did the person/(any of the people) who did it actually use force or violence on anyone in any way, even if this resulted in no injury?

1. Yes
2. No

FV711 **[ASK ALL]**

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Did the person/(any of the people) who did it threaten anyone?

1. Yes
2. No

FV712 **[ASK ALL]**

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Was there any sexual element in the offence (e.g. indecent assault, touching, indecent images)?

1. Yes
2. No

FV81 [ASK ALL]

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Did the person/(any of the people) who did it use (or attempt to use) the victim's personal details to purchase goods or make payments without his/her permission?

1. Yes
2. No

FV82 [ASK ALL]

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Did the person/(any of the people) who did it use (or attempt to use) the victim's personal details to make an application (e.g. for a mortgage, loan or credit card or to apply for state benefits)?

1. Yes
2. No

FV83 [ASK ALL]

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Was the victim tricked or deceived into making an investment that they later discovered was mis-sold or had never actually existed?

1. Yes
2. No

FV84 [ASK ALL]

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Was the victim tricked or deceived into sending or transferring money to someone who turned out to be not who they said they were?

1. Yes
2. No

FV85 [ASK ALL]

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Did the victim pay for goods or services that either did not arrive, were false/fake, were substandard or never actually existed?

1. Yes
2. No

FV86 [ASK ALL]

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Did the person (or people who did it) steal the victim’s personal information or details by hacking into their computer or on-line accounts (e.g. social media, e-mail)?

INTERVIEWER NOTE: Hacking refers to unauthorised access to computer material.

1. Yes
2. No

FV87 [ASK ALL]

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE

DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE

RESPONDENT

Was a computer or other internet-enabled device infected or interfered with, for example by a virus?

1. Yes
2. No

FV88 [ASK ALL]

SL

ASK OR RECORD

INTERVIEWER: ONLY RECORD THE ANSWER IF YOU ARE CERTAIN FROM THE DESCRIPTION ALREADY GIVEN. IF IN ANY DOUBT YOU MUST ASK THE RESPONDENT

Was the internet or any type of online activity related to any aspect of the offence?

5. Yes
6. No

FREFCHK [ASK IF ALL QUESTIONS FROM FV71 TO FV87 ARE DK OR REF]

SL

INTERVIEWER: DO YOU WANT TO SKIP THE REST OF THE VICTIM FORM?

1. Yes
2. No

FWHYSKI2 **[ASK IF FREFCHK = YES]**

SL

INTERVIEWER: PLEASE EXPLAIN WHY YOU ARE SKIPPING THE REST OF THIS VICTIM FORM

Text: Maximum 200 characters

TIMING POINT

CIRCUMSTANCES OF INCIDENT

FFRHWA-

FFRHWL **[ASK IF FV81- FV88=YES]**

GREY SHOWCARD F1

As far as you are aware did the incident happen as a result of any of the things on this card?

CODE ALL THAT APPLY

1. Theft of your credit or bank card
2. Theft of your personal documents (e.g. cheque book, bank statements, pass book)
3. Theft of a computer, laptop, tablet, smart phone, or another internet enabled device
4. Unauthorised access to online banking information (e.g. online banking or credit/debit card)
5. Unauthorised access to other personal information
6. Your card details being stolen/cloned (e.g. at a cash machine, a restaurant or petrol station)
7. An email that you received or a link that you opened into a fake website.
8. A phone call /text message that you received asking you for money or personal information or to access files on your computer
9. Someone visiting your address and trying to get access to your money or personal information
10. Something else (Please specify)
11. Not sure
12. None of these

FFrCont **[ASK ALL]**

Did you (or anyone else in your household) have any contact with the people who did it? This might have been in person, by telephone, by text message, by email or online.

1. Yes
2. No

FFrCont2 [ASK IF FFrCont=YES AND MORE THAN 1 PERSON IN HOUSEHOLD]

Was the contact with you or with someone else in the household?

1. Respondent
2. Someone else in the household
3. No contact

FHowCont [ASK IF FFrCont =1 OR 2]

SCRIPTING NOTE: Text fill below: IF FFrCont=1 AND ONLY 1 PERSON IN HOUSEHOLD “you”. IF FFrCont2=1 “you” IF FFrCont2=2 “someone else in your household”. IF FFrCont2=1 AND 2 “you and someone else in your household”.

In which of the following ways did you [or someone else in your household] have contact with them?

CODE ALL THAT APPLY

1. In person
2. By Telephone
3. By text message
4. By e mail or online
5. By post/letter
6. Some other way (specify)
7. No contact

FMFrdTyp [ASK IF FFrCont=1]

Was the contact related to any of the things on this card? CODE ALL THAT APPLY

GREY SHOWCARD F2

INTERVIEWER: THIS INCLUDES INTERNET POP UPS (new web browser windows that are often used to display advertisements)

1. A. A big win in a lottery, prize draw, sweepstake or competition that you had not entered

2. B. The chance to make an investment with a **guaranteed** high return (e.g. shares, art, fine wine, carbon credit etc.)
3. C. Someone inviting you to get to know them with a view to a possible friendship or relationship (this may be via a website) and then requesting money
4. D. Help in moving large sums of money from abroad
5. E. Help in releasing an inheritance
6. F. An urgent request to help someone (possibly claiming to be one of your friends) get out of financial trouble
7. G. A job offer, a franchise offer or other business opportunity such as paying for training
8. H. A loan on very attractive terms
9. I. Help to recover money lost from a previous scam
10. J. Releasing your pension savings early (e.g. for cash incentives, better returns, tax free advances or pension loans) without warning you of the tax implication
11. K. Paying an urgent debt
12. L. Unsolicited help to repair your computer/laptop (for example to deal with viruses)
13. M. Some other type of similar request
14. SPONTANEOUS ONLY: None of these
15. N. None of these

FRespond **[ASK IF FFRCONT=1AND FHowCont NOT 1]**

Did you actually reply or respond to any of the communication you received in any way

1. Yes
2. No

FHwRspnd1 **[ASK IF FRESPOND=2 OR DK OR FHowCont=1]**

GREY SHOWCARD F3

Can I just check, did you respond in any of the ways mentioned on this card?

CODE ALL THAT APPLY

1. Contacted the sender or someone else (e.g. by calling a number, sending an e-mail, webchat)
2. Requested further information to be sent to you
3. Provided bank details
4. Provided any other personal information (e.g. address, passport number)
5. Provided any other financial details (e.g. credit card number, Paypal account)
6. Provided device login details/ allowed access to your device
7. Sent or transferred money (e.g. by Western Union, Moneygram, Ukash)
8. Contacted the sender to complain
9. SPONTANEOUS ONLY: Didn’t read/listen to the communication(s) in enough detail to know/remember
10. None of these

FHwRspnd2 [ASK IF FRESPOND=1]

GREY SHOWCARD F3

Looking at this card, in which of these way did you respond?

CODE ALL THAT APPLY

1. Contacted the sender or someone else (e.g. by calling a number or sending an e-mail, webchat)
2. Requested further information to be sent to you
3. Provided bank details
4. Provided any other personal information (e.g. address, passport number)
5. Provided any other financial details (e.g. credit card number, Paypal account)
6. Provided device login details/ allowed access to your device
7. Sent or transferred money (e.g. by Western Union, Moneygram, Ukash)
8. Contacted the sender to complain
9. SPONTANEOUS ONLY: Didn't read/listen to the communication(s) in enough detail to know/remember
10. None of these

FContAt [ASK IF FFrCont=2(NO)]

Did you **attempt** to make any contact with the people who did it?

1. Yes
2. No

FLegit [ASK IF (FV83 OR FV84 OR FV85 = 1) AND FContAt=1]

As far as you were aware were the people who did it acting on behalf of a company or organisation that is still contactable now?

1. Yes
2. No

ID THEFT

FID2AA- **[ASK IF FV82=1]**

FID2AM

GREY SHOWCARD F4

Were any of your personal details used WITHOUT YOUR PERMISSION toapply for or obtain any of the things on this card?

CODE ALL THAT APPLY

1. A credit or debit card
2. A store card
3. Abank or building society account
4. A mobile phone account
5. A loan
6. A mortgage
7. Another credit agreement
8. State benefits such as child benefit, tax credits, housing benefit, etc.
9. A passport
10. Other (SPECIFY)
11. None of these

FIDPROBA-

FIDPROBK **[ASK IF ASK IF FV82=1]**

GREY SHOWCARD F5

Have you experienced any of the problems shown on this card as a DIRECT result of having your personal details used without your permission or prior knowledge?

1. Your identity used to commit a crime
2. Letters from debt collection agencies
3. Visits from bailiffs
4. Not being able to obtain a loan
5. Not being able to obtain a credit card
6. Not being able to open a bank account
7. Delays at the border when coming back into the country
8. Other (SPECIFY)
9. None of these

COMPUTER VIRUS

FEEXPVIR [ASK IF FV87=1]

You said that you had experienced a computer virus (or other computer infection). Did this infect your computer as a direct result of opening an email, attachment or a web link that was sent to you?

1. Yes
2. No
3. Don't know

FDEVICE [ASK IF FV87=1]

Was the internet enabled device that was affected…

1. A desktop PC
2. A laptop/netbook computer
3. A handheld computer (eg tablet, ipad, palmtop)
4. A mobile phone or smartphone
5. Smart TV
6. Games console
7. Smart Watch
8. Some other device (other specify)

FNODEVICE [ASK IF FV87=1]

In total how many different devices belonging to anyone in the household were infected by this virus?

ENTER NUMBER

ADD CAPI CHECK IF FNODEVICE>10

"Can I just check, you said that [INSERT NODEVICE] different devices belonging to members of your household were infected by the virus. Is that correct? Yes/No – IF No amend coding.

FDBELONG [ASK IF FV87=1]

Who did the infected device belong to?

CODE ALL THAT APPLY

INTERVIEWER: 'BELONG' = WOULD HAVE HAD TO PAY TO REPLACE IT

NOTE: IF RESPONDENT IS SELF-EMPLOYED, CODE DEVICES

AS BELONGING TO HIM/HER

1. Respondent
2. Other adult household member
3. Child under 16 in household
4. Employer/ work
5. Friend
6. Other

FAWARE [ASK IF FV714=1]

How did you first become aware that your computer or internet enabled device had become infected or had been attacked?

SINGLE CODE. PROMPT IF NECESSARY

1. The virus was detected by anti-virus software BEFORE infecting your device
2. The virus was detected by anti-virus software AFTER infecting your device
3. Pop ups constantly appearing on screen that victim could not remove
4. Computer was performing badly/stopped working
5. Spontaneous – Unsure - Identified by someone else in the household
6. Some other way – specify

DETAILS OF THE OFFENDERS

FDESCROFF [ASK IF FV78 = NO OR FV78 = DK/REF]

SL

Can I check, are you able to say anything at all about the people who did it - how many there were, or whether they were male or female?

1. Yes
2. No

FNUMOFF [ASK IF FV78 = YES OR FDESCROFF = YES]

SL

[You mentioned earlier that you might have some information about the offender(s).] How many were there?

1. One
2. Two
3. Three
4. Four or more

FOFFSEX1 [ASK IF FNUMOFF = 1]

SL

Was the person who did it male or female?

1. Male
2. Female

FAGEOFF2 [ASK IF FNUMOFF = 1]

SL

How old was the person who did it? Would you say [he/she] was...READ OUT

1. a child aged under 10
2. a child aged between 10 and 15
3. aged between 16 and 24
4. aged between 25 and 39
5. or aged 40 or over?

FRACEOFF3 [ASK IF FNUMOFF = 1]

SL

As far as you know was the person who did it...READ OUT

1. White
2. Black
3. Asian
4. Chinese
5. *Mixed ethnic group*
6. Or from another ethnic group? (SPECIFY)

FKNEWOFF1 [ASK IF FNUMOFF = 1]

SL

Was [he/she] someone you/(the victim) knew before it happened or was [he/she] a

stranger?

1. Someone known
2. Stranger
3. Don't Know

FSEENOFF1 [ASK IF FKNEWOFF1 = 2 OR 3 OR DK/REF]

SL

Had you/(the victim) had contact with [him/her] before?

1. Yes
2. No

FHOWKNOW1 [ASK IF FKNEWOFF1 = 1 OR FSEENOFF1 = 1]

SL

How well did you/(the victim) know [him/her]? Just online, by sight, just to speak to casually, or did you/(the victim) know [him/her] well?

1. Just online contact
2. Just by sight
3. Just to speak to casually
4. Known well

FOFFREL3 [FKNEWOFF1 = 1 OR FSEENOFF1 = 1]

SL

What was [his/her] relationship to you/(the victim)?

INTERVIEWER: PRIORITY CODE

1. Husband/ wife/ partner
2. Son/daughter (in law)
3. Other household member
4. Current boyfriend/girlfriend
5. Former husband/wife/partner
6. Former boyfriend/girlfriend
7. Other relative
8. Workmate/colleague
9. Client/members of public contacted through work
10. Friend/acquaintance
11. Online friend/acquaintance
12. Neighbour
13. Young person from local area
14. Tradesman/ builder/ contractor
15. (Ex) husband/(ex) wife/(ex) partner/(ex) boyfriend/(ex) girlfriend of someone else in household
16. Other (SPECIFY)

FSTGANG [ASK IF FKNEWOFF = 1 OR FSEENOFF = 1]

SL

To the best of your knowledge, do you think the person who did it was part of an organised crime gang.

1. Yes
2. No

FOFFSEX [ASK IF FNUMOFF IN (2..4) OR DK/REF]

SL

Were the people who did it male or female?

1. Male
2. Female
3. People of both sexes

FAGEOFF2A-

FAGEOFF2G [ASK IF FNUMOFF IN (2..4) OR DK/REF]

SL

How old were the people who did it? Would you say they were...READ OUT CODE ALL THAT APPLY

1. children aged under 10
2. children aged between 10 and 15
3. people aged between 16 and 24
4. people aged between 25 and 39
5. or people aged over 40?

FRACEOF3A-

FRACEOF3H [ASK IF FNUMOFF IN (2..4) OR DK/REF]

SL

As far as you know were the people who did it...READ OUT CODE ALL THAT APPLY

1. White
2. Black
3. Asian
4. Chinese
5. *Mixed ethnic group*
6. or from another ethnic group? (SPECIFY)

FKNEWOFF [ASK IF NUMOFF IN (2..4)]

SL

Were any of them people you/(the victim) knew before it happened or were they

strangers?

1. All known
2. Some known, some not known
3. None known
4. Don’t Know

FSEENOFF [ASK IF KNEWOFF = 3 OR 4 OR DK/REF]

SL

Had you/(the victim) had contact with any of them before?

1. Yes
2. No

FHOWKNOWA-

FHOWKNOWE [ASK IF (FKNEWOFF=1 OR 2) OR FSEENOFF=1]

SL

How well did you/(the victim) know them? Just online, by sight, just to speak to casually, or did you/(the victim) know any of them well? CODE ALL THAT APPLY SET OF [3]

1. At least one known only online
2. At least one known just by sight
3. At least one known to speak to casually
4. At least one known well

FWELLKNOW [ASK IF FV78 = YES]

SL

You mentioned earlier that (the victim/someone in the household) had some contact with, or knew something about the offenders. Can I just check, before the incident happened, were the offenders...READ OUT

1. Well known to you
2. Known by sight
3. Known just to speak to casually
4. or were they strangers?

FOFFREL3A- [ASK IF (FKNEWOFF= 1 OR 2) OR (FSEENOFF = 1) OR FWELLKNOW IN

FOFFREL3Q (1..3)]

SL

What was their relationship to you/(the victim)? CODE ALL THAT APPLY

1. Husband/ wife/ partner
2. Son/daughter (in law)
3. Other household member
4. Current boyfriend/girlfriend
5. Former husband/wife/partner
6. Former boyfriend/girlfriend
7. Other relative
8. Workmate/colleague
9. Client/members of public contacted through work
10. Friend/acquaintance
11. Neighbour
12. Young people from local area
13. Tradesman/ builder/ contractor
14. (Ex)Husband/(ex)wife/(ex)partner/(ex)boyfriend/(ex)girlfriend of someone else in household
15. Other (SPECIFY)

FSTGANG2 [ASK IF (FKNEWOFF = 1 OR 2) OR (FSEENOFF = 1) OR FWELLKNOW IN

SL (1..3]

To the best of your knowledge, were ANY of the people who did it members of an organised crime gang.?

1. Yes
2. No

DETAILS OF WHAT WAS STOLEN

FSTOLMON [ASK IF FV71 = NO OR FV71 = DK/REF]

SL

Can I check, was any money stolen, or taken from bank or credit accounts , even if you later got it back?

1. Yes
2. No

FSTOLITEM [ASK IF FV71 = NO OR FV71 = DK/REF]

SL

Was anything else stolen, even if you later got it back?

1. Yes
2. No

FBELONGA–

FBELONGH [ASK IF FSTOLMON = YES OR FSTOLITEM = YES OR FV71 = YES]

SL

[You mentioned earlier that property was stolen.] Who did the stolen property belong to? CODE ALL THAT APPLY

INTERVIEWER: 'BELONG' = WOULD HAVE HAD TO PAY TO REPLACE IT

NOTE: IF RESPONDENT IS SELF-EMPLOYED, CODE TOOLS, EQUIPMENT, ETC AS BELONGING TO HIM/HER

1. Respondent
2. Other adult household member
3. Child under 16 in household
4. Employer/ work
5. Friend
6. Other

FWHAST10A–

FWHAST10SS [ASK IF FV71 = YES OR FSTOLITEM = YES]

SL

Could you tell me what was actually stolen, even if you later got it back? CODE ALL

THAT APPLY

PROBE FULLY: Anything else?

1. Money from bank account, credit card, store card
2. Cash (not including money taken from account)
3. Credit card/switch card/debit card/store card/cheque card
4. Documents (e.g. savings account book, cheque book, passport)
5. Personal information (passwords, PIN numbers, login details etc)
6. Mobile phone or smartphone (inc iPhone, Blackberry)
7. Laptops or other portable electronic devices (e.g. netbook, iPad, tablet, Kindle)
8. Computers and computer equipment (e.g. PC, Mac, printers, scanners)
9. Handheld games consoles (e.g. PSP, Nintendo DS)
10. Games consoles (e.g. Playstation 3, XBox 360, Nintendo Wii)
11. Car/van
12. Motorcycle/motorised scooter/moped
13. Vehicle parts/fittings/accessories (inc. car music system, satellite navigation system)
14. Briefcase/handbag/shopping bag
15. Purse/wallet
16. Jewellery
17. Watches
18. Clothes
19. Camera (inc. video camera/camcorder)
20. Portable audio or video device (e.g. MP3 player, iPod, DVD player)
21. DVD players/recorders (inc. Blu-ray)
22. Television
23. Stereo/Hi-fi equipment (inc. other home audio equipment)
24. CDs/tapes/videos/DVDs/computer games
25. House keys
26. Car keys
27. Tools
28. Bicycle
29. Garden furniture, ornaments, plants, or equipment (e.g. lawnmowers, spades, wheel barrows, BBQ)
30. Bins (wheelie bin, dustbin, recycling bins)
31. Glasses, sunglasses
32. Children’s toys
33. Sports equipment (e.g. golf clubs, horse riding equipment)
34. Food/drink/alcohol/cigarettes/groceries/shopping
35. Various household items/gadgets (e.g. small electrical appliances, torch, penknife)
36. *Toiletries/make up/perfume/medication*
37. *Furniture or white goods items*
38. *Doors/windows/door furniture/exterior fittings*
39. *Books*
40. *Bicycle parts*
41. *Fuel (petrol, diesel, oil)*
42. *Scrap metal (e.g. copper pipes, lead, iron, tin, etc.)*
43. *Building materials (e.g. timber, brick, paving stones)*
44. *Electricity/energy*
45. Other (SPECIFY)

COSTS OF CRIME

FQLOSS4 [ASK IF FSTOLMON =1 OR FWHAST10A=6 (MONEY)]

How much money, if any, was taken - whether or not it was refunded?

Please include any money that was subsequently refunded by your bank, building society or credit card company but DO NOT include any additional charges or costs that you incurred as a result of the incident.

INTERVIEWER: IF RESPONDENT SAYS THEY DON'T KNOW ASK: Approximately how much money would you say was taken?

1. Less than £20
2. £20-£49
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 - £9,999
10. £10,000 - £19,999
11. £20,000 - £39,999
12. £40,000 - £59,999
13. £60,000 - £79,999
14. £80,000 - £99,999
15. £100,000 or more
16. Not yet resolved

DK

REF

FQLOSS4b [ASK IF FQLOSS4 = 1]

You mentioned that the amount taken was less than £20, was this…

1. Less than £1
2. £1 - £4.99
3. £5 - £9.99
4. £10 - £19.99
5. No money taken (DO NOT READ OUT)

FQLOSS6 [ASK IF FQLOSS4>0]

Was the money that was taken…

1. Refunded in full
2. Partially refunded
3. Not refunded at all
4. SPONTANEOUS – not yet resolved

FQLOSS2A [ASK IF FQLOSS6=2]

How much of this money, if any, did you get back? Please include any money that was subsequently refunded by your bank, building society or credit card company.

INTERVIEWER: IF RESPONDENT SAYS THEY DON'T KNOW ASK: APPROXIMATELY HOW MUCH MONEY WOULD YOU SAY WAS REFUNDED?

1. Less than £20
2. £20-£49
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 - £9,999
10. £10,000 - £19,999
11. £20,000 - £39,999
12. £40,000 - £59,999
13. £60,000 - £79,999
14. £80,000 - £99,999
15. £100,000 or more
16. Not yet resolved

DK

REF

FQLOSS4b [ASK IF FQLOSS4 = 1]

You mentioned that the amount refunded was less than £20, was this…

1. Less than £1
2. £1 - £4.99
3. £5 - £9.99
4. £10 - £19.99
5. No money taken (DO NOT READ OUT)

CAPI CHECK THAT FQLOSS2A < FQLOSS4

FCHARGES [ASK IF FMONEY=1]

In addition to any money taken did you incur any additional charges or costs as a result of the incident? Additional charges might include bank charges, overdraft fees, costs of repair work required etc.

1. Yes
2. No

FCMLOSS2 [ASK IF FMONEY=NO OR DK/NA OR (FMONEY =YES AND FCHARGES=YES)]

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

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

FFRLOSS3 [ASK IF FFRLOSS2=5 (LOST £1000 OR MORE)]

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

ENTER AMOUNT TO NEAREST £1k £_________

FQKNOW [ASK IF FSTOLMON =1 OR FWHAST10A=6 (MONEY)]

How did you **first** find out that money had been taken from your bank, building society, or credit card account? CODE ONE ONLY. PROMPT IF NECESSARY.

1. By yourself – saw unrecognised transaction on statement or found money missing from account
2. By yourself – card was refused/declined
3. By yourself - other
4. Contacted/told by a financial institution (bank, building society or credit card company)
5. Contacted/told by the police
6. Another way (SPECIFY)

FACCNO [ASK IF FSTOLMON =1 OR FWHAST10A=6 (MONEY)]

Can I check was the money taken from just one account or from a number of different accounts that belonged to you (or anyone else in your household?

1. One account
2. More than one account

FACCNO2 [ASK IF FACCNO=2]

How many of your accounts had money taken from them?

ENTER NUMBER

CAPI check if FACCKNO2>10

ATTEMPTED THEFT

FTRYSTMO [ASK ALL]

[Apart from any money that was actually stolen] Can I just check, to the best of your knowledge, did the people who did it TRY to obtain any money from you?

1. Yes
2. No

FTRYSTOTH [ASK IF FV75 = NO OR FV75 = DK/REF]

SL

[Apart from what was actually stolen] Can I just check, to the best of your knowledge, did the people who did it TRY to steal anything [else] that belonged to you or any other member of your household?

1. Yes
2. No

FBELONGAA-

FBELONGAH [ASK IF FV75 = YES OR FTRYSTMO = YES OR FTRYSTOTH = YES]

SL

[You mentioned earlier that the people tried to steal something.] Who did the property that the person tried to steal belong to? CODE ALL THAT APPLY

NOTE: IF RESPONDENT IS SELF-EMPLOYED, CODE TOOLS, EQUIPMENT ETC

AS BELONGING TO HIM/HER

1. Respondent
2. Other adult household member
3. Child under 16 in household
4. Employer/work
5. Friend
6. Other

FWHTRS9A–

FWHTRS9RR [ASK IF FV75 = YES OR FTRYSTOTH = YES]

L

What did they try to steal? CODE ALL THAT APPLY

1. Car/van
2. Motorcycle/motorised scooter/moped
3. Vehicle parts/fittings/accessories (inc. car music system, satellite navigation system)
4. Briefcase/handbag/shopping bag
5. Purse/wallet
6. Money from bank account, credit card, store card
7. Cash (not from meter) (inc. foreign currency)
8. Credit card/switch card/debit card/store card/cheque card
9. Jewellery
10. Watches
11. Clothes
12. Documents (e.g. savings account book, cheque book, passport)
13. Personal information (passwords, PIN numbers, login details etc)
14. Mobile phone or smartphone (inc iPhone, Blackberry)
15. Camera (inc. video camera/camcorder)
16. Portable audio or video device (e.g. MP3 player, iPod, DVD player)
17. DVD players/recorders (inc. Blu-ray)
18. Television
19. Stereo/Hi-fi equipment (inc. other home audio equipment)
20. Laptops or other portable electronic devices (e.g. netbook, iPad,tablet, Kindle)
21. Computers and computer equipment (e.g. PC, Mac, printers, scanners)
22. Handheld games consoles (e.g. PSP, Nintendo DS)
23. Games consoles (e.g. Playstation 3, XBox 360, Nintendo Wii)
24. CDs/tapes/videos/DVDs/computer games
25. House keys
26. Car keys
27. Tools
28. Bicycle
29. Garden furniture, ornaments, plants, or equipment (e.g. lawnmowers, spades, wheel barrows, BBQ)
30. Bins (wheelie bin, dustbin, recycling bins)
31. Glasses, sunglasses
32. Children’s toys
33. Sports equipment (e.g. golf clubs, horse riding equipment)
34. Food/drink/alcohol/cigarettes/groceries/shopping
35. Various household items/gadgets (e.g. small electrical appliances, torch, penknife)
36. *Toiletries/make up/perfume/medication*
37. *Furniture or white goods items*
38. *Doors/windows/door furniture/exterior fittings*
39. *Books*
40. *Bicycle parts*
41. *Fuel (petrol, diesel, oil)*
42. *Scrap metal (e.g. copper pipes, lead, iron, tin, etc.)*
43. *Building materials (e.g. timber, brick, paving stones)*
44. Other (SPECIFY)

FEMOTREAC [ASK ALL]

L

GREY SHOWCARD F13

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
2. No

FWHEMOTA–
FWHEMOTL [ASK IF FEMOTREAC = YES]

L

GREY SHOWCARD F13

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)

FHOWAFF1 [ASK IF FEMOTREAC = YES]

L

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

1. Very much
2. Quite a lot
3. A little,
4. not at all?

FIMPACT2A-

FIMPACT2P [ASK ALL]

L

GREY SHOWCARD F14

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. Stop using specific internet sites
7. *Inconvenience*
8. *Moved house*
9. *Took additional security precautions (e.g. installing a burglar alarm)*
10. *Loss of trust in other people/the public*
11. *Time off from school/college/university*
12. *Impact on health*
13. *Effect on personal confidence*
14. Other (SPECIFY)
15. No impact

CONTACT WITH ACTION FRAUD AND POLICE ABOUT THE INCIDENT

FBANK [ASK IF FV81 TO FV86=1]

As far as you know, did your bank, building society or credit company know about the incident?

1. Yes
2. No

FBANK2 [ASK IF FBANK=YES]

How did your bank, building society or credit company find out about the incident?

1. Respondent reported incident to bank/building society/credit company
2. Someone else reported incident to bank/building society/credit company
3. Bank/building society/credit company notified respondent (after noticing suspicious transactions)
4. Other (specify)

FAFKNOW [ASK ALL]

ActionFraud is the UK's national fraud and internet crime reporting centre, providing a central point of contact for information about fraud and financially motivated internet crime.

Did you report the incident to Action Fraud?

1. Yes
2. No

FYAFNO2A-

YAFNO2U [ASK IF AFKNOW = NO]

SL

Why did you not report the incident to Action Fraud?

CODE ALL THAT APPLY

1. Never heard of Action Fraud
2. Thought incident would be reported by other authority (eg the bank/financial institution)
3. Reported to the Police
4. Private / personal / family matter
5. Dealt with matter myself/ourselves
6. Reported to other authorities (eg superiors, company security staff, etc)
7. Action Fraud could have done nothing
8. Action Fraud would not have bothered/not been interested
9. Inconvenient/too much trouble
10. No loss/damage
11. Attempt at offence was unsuccessful
12. Too trivial/not worth reporting
13. Previous bad experience of Action Fraud
14. It is a common event/just one of those thing/just something that happens
15. It is something that happens as part of my job
16. It was partly my/a relative's/a friend's fault
17. Did not want to report it because offender(s) was not responsible for their actions (e.g. children, person with mental health problems, etc)
18. (Thought) Someone else had already reported incident / or similar incidents
19. Tried to report it but was not able to contact Action Fraud/theywere not interested
20. Other (SPECIFY)

FCRIMEREF [ASK IF AFKNOW =YES]

SL

Did Action Fraud give you [he/she] a crime reference number for this matter?

INTERVIEWER: if respondent unsure, explain that crime reference numbers are typically issued over the phone, or through a letter, and should be received within several days of being reported to Action Fraud.

INTERVIEWER: If respondent leaves to find a letter or record of the number, discourage them from doing so – only interested in whether one was received, no details are required

1. Yes
2. No
3. Can't remember

FSATAF [ASK IF AFKNOW = YES]

SL

Overall, were you/(the victim) satisfied or dissatisfied with the way Action Fraud handled this matter?

INTERVIEWER: IF SATISFIED ASK: Very satisfied or just fairly satisfied?

IF DISSATISFIED ASK: A bit dissatisfied or very dissatisfied?

1. Very satisfied
2. Fairly satisfied
3. A bit dissatisfied
4. Very dissatisfied
5. Too early to say

COPSKNOW [ASK ALL]

SL

Did the police come to know about the matter?

1. Yes
2. No

ACTFR **[ASK ALL]**

GREY SHOWCARD F15

Did you report this to anyone else? CODE ALL THAT APPLY

INTERVIEWER NOTE: IF EXPERIENCED MORE THAN ONE COMPUTER VIRUS, THINK ABOUT THE LAST OCCASION

A. Anti-virus software company
B. Internet service provider
C. Other government agency
D. Website administrator (e.g. Facebook, eBay, Amazon)
E. Someone else
F. No-one

FFINDOFF **[ASK IF AFKNOW = YES OR COPSKNOW = YES]**

SL

Did Action Fraud or the police find out or know who did it?

1. Yes
2. No
3. Not yet
4. Don't Know

FCONTVS **[ASK ALL]**

SL

Victims' services are organisations which have staff and volunteers trained to offer information, practical help and emotional support to the victims of crime. Victim Support is an example of a victims' service. Thinking about the incident we have been discussing, did you or anyone else in the household have any type of contact with victims' services?

1. Yes
2. No

FTYCONVSA-

FTYCONVSF [ASK IF FCONTVS = YES]

SL

What type of contact did you have with victims' services? Did you.... CODE ALL THAT APPLY

1. Receive a leaflet or letter
2. Receive a phone call
3. Have face-to-face contact
4. or have some other type of contact?

FVSSAT [ASK IF FCONTVS = YES]

SL

Overall, were you (the victim/the household) satisfied or dissatisfied with the contact you had with victims' services?

INTERVIEWER: IF SATISFIED ASK: Very satisfied or just fairly satisfied?

IF DISSATISFIED ASK: A bit dissatisfied or very dissatisfied?

1. Very satisfied
2. Fairly satisfied
3. A bit dissatisfied
4. Very dissatisfied
5. Too early to say

FVSRECA-

FVSRECM [ASK ALL]

SL

GREY SHOWCARD F16

This card lists some of the types of information, advice or support that people sometimes need after being the victim of a crime. What types of information, advice or support, if any, did you (or anyone else in your household) RECEIVE following the incident? CODE ALL THAT APPLY

1. A. Did not receive any information, advice or support
2. B. Chance to talk to someone either formally or informally
3. C. Help with reporting the incident/dealing with the police
4. D. Help with insurance or compensation claims
5. E. Help related to the case going through the Criminal Justice System (e.g. attending court, giving evidence, etc.)
6. F. Financial support
7. G. Other practical help (e.g. clearing up, making a list of what was stolen, fitting locks)
8. H. Help accessing other services (e.g. health care, housing, refuge)
9. I. Information on the progress of the case or how the Criminal Justice System works
10. J. Information on preventing further crime
11. K. Something else (SPECIFY)

FVSLIK1A-

FVSLIK1M [ASK IF FVSREC=1 (NO INFORMATION RECEIVED)]

SL

GREY SHOWCARD F17

Even though you didn't receive any information, advice or support following the incident, would you have LIKED to receive any of the things listed on this card? CODE ALL THAT APPLY

1. A. Would not have liked to receive any (more) information, advice or support
2. B. Chance to talk to someone either formally or informally
3. C. Help with reporting the incident/dealing with the police
4. D. Help with insurance or compensation claims
5. E. Help related to the case going through the Criminal Justice System (e.g. attending court, giving evidence, etc.)
6. F. Financial support
7. G. Other practical help (e.g. clearing up, making a list of what was stolen, fitting locks)
8. H. Help accessing other services (e.g. health care, housing, refuge)
9. I. Information on the progress of the case or how the Criminal Justice System works
10. J. Information on preventing further crime
11. K. Something else (SPECIFY)

FVSLIK2A-

FVSLIK2M [ASK IF FVSREC IN (2..11)]

SL

GREY SHOWCARD F17

Apart from what you have already mentioned, would you have LIKED to receive any other types of information, advice or support?

1. A. Would not have liked to receive any (more) information, advice or support
2. B. Chance to talk to someone either formally or informally
3. C. Help with reporting the incident/dealing with the police
4. D. Help with insurance or compensation claims
5. E. Help related to the case going through the Criminal Justice System (e.g. attending court, (e.g. attending court, giving evidence, etc.)
6. F. Financial support
7. G. Other practical help (e.g. clearing up, making a list of what was stolen, fitting locks)
8. H. Help accessing other services (e.g. health care, housing, refuge)
9. I. Information on the progress of the case or how the Criminal Justice System works
10. J. Information on preventing further crime
11. K. Something else (SPECIFY)

{Show only codes NOT mentioned at VSREC – except code 11 always appears}

FSCORCRM2 [ASK ALL]

SL

I would now like to ask you how serious a crime you personally think this was. On a scale of 1 to 20 with 1 being a very minor crime like theft of milk bottles from a doorstep, to 20 being the most serious crime of murder.

How would you rate this crime on the scale from 1 to 20?

1..20

FCRIME [ASK ALL]

SL

Did you think that what happened was...READ OUT

1. A crime
2. wrong, but not a crime
3. or just something that happens?

REVIEW OF INCIDENTS

FREVDESC [ASK ALL]

SL

INTERVIEWER: YOU RECORDED THE DESCRIPTION OF THE INCIDENT AS: [answer from DESCRINC].

INTERVIEWER – BELOW IS A SUMMARY OF THE INFORMATION COLLECTED IN THIS VICTIM FORM. PLEASE CONFIRM WITH THE RESPONDENT THAT ALL THE INFORMATION IS CORRECT AND IS CONSISTENT WITH THE DESCRIPTION.

IF THERE IS ANYTHING YOU NEED TO ADD, CORRECT OR CLARIFY DO THIS AT THE NEXT QUESTION. **YOU SHOULD NOT GO BACK AND AMEND ANYTHING.**

YOU HAVE RECORDED THAT:

[(NOTHING/SOMETHING) WAS STOLEN] (taken from FV71)

[(*LIST OF WHAT WAS STOLEN, IF ANYTHING)*] (taken from FV72)

[(AN/ NO) ATTEMPT WAS MADE TO STEAL SOMETHING (ELSE)]

[FORCE OR VIOLENCE WAS (NOT) USED]

[THE OFFENDER(s) (DID NOT THREATEN ANYONE/THREATENED SOMEONE)]

[PERSONAL DETAILS WERE (NOT) USED TO MAKE A PURCHASE WITHOUT PERMISSION (taken from FV81)

[PERSONAL DETAILS WERE (NOT) USED TO MAKE AN APPLICATION WITHOUT PERMISSION (taken from FV82)

[VICTIM WAS (NOT) TRICKED INTO MAKING INVESTMENT] (taken from FV83)

[VICTIM WAS (NOT) TRICKED INTO TRANSFERRING ANY MONEY] (taken from FV84)

[PAYMENT (NOT) MADE FOR GOODS THAT DID NOT EXIST/SUBSTANDARD (taken from FV85)

[OFFENDER (DID NOT) ACCESS(ED) PERSONALINFORMATION (taken from FV86)

[INTERNET ENABLED DEVICE (NOT) INFECTED BY VIRUS OR MALWARE] (taken from FV87)

[THIS WAS (NOT) A CYBER OFFENCE] (taken from FV88)

Is there anything you would like to add or clarify?

1. Yes
2. No

FCHKDESCR [IF FREVDESC = YES]

PLEASE TYPE IN ANY ADDITIONAL INFORMATION OR CLARIFICATION HERE.

Text: Maximum 100 character