This report was prepared by Westat using federal funding provided by the Bureau of Justice Statistics.

Document title:	Testing Questions to Measure Cybercrimes on Three Supplements to the National Crime Victimization Survey
Author(s):	David Cantor, PhD, Westat Pamela Giambo, Westat Sarah Bennett-Harper, Westat Willow Burns, Westat
BJS Project Manager(s):	Jennifer L. Truman, PhD, Statistician, Victimization Statistics Unit
Document No.:	NCJ 311862
Publication Date:	May 2026

Abstract:

In response to the Better Cybercrime Metrics Act (P.L. 117-116), the Bureau of Justice Statistics (BJS) is exploring how to measure cybercrime through the National Crime Victimization Survey (NCVS). This report describes research that considers which types of crimes are feasible to collect on the NCVS, the survey items designed to collect these data and the evaluation of these items using cognitive interviews and a web survey. In addition, in response to a U.S. Government Accountability Office request, the research also explored measuring bias-motivated crimes that occurred on the internet. The recommended changes involve modifying existing questions and adding items to three NCVS supplements – the Supplemental Victimization Survey (SVS; stalking supplement), Identity Theft Supplement (ITS) and Supplemental Fraud Survey (SFS). The report provides the rationale for survey changes, research methodology, test results and final recommendations.

This page is intentionally left blank.

Westat

Improving Lives Through Research®

Testing Questions to Measure Cybercrimes on Three Supplements to the National Crime Victimization Survey

National Victimization Statistical Support Program (NVSSP)
Contract: 15PBJS22F00000003

May 2026

Prepared For
Bureau of Justice Statistics
Washington D.C.

Prepared By
Westat
1600 Research Blvd.
Rockville, MD 20850-3129
301-251-1500

Authors
David Cantor
Pamela Giambo
Sarah Bennett-Harper
Willow Burns

Summary

In response to the Better Cybercrime Metrics Act (P.L. 117-116), the Bureau of Justice Statistics (BJS) is exploring how to measure cybercrime through the National Crime Victimization Survey (NCVS). This report describes research that considers which types of crimes are feasible to collect on the NCVS, the survey items designed to collect these data and the evaluation of these items using cognitive interviews and a web survey.

Background

The report begins with a discussion of the rationale for determining which types of cybercrimes should be collected and how this data collection fits within the NCVS. The recent NCVS Instrument Redesign considered several possibilities on how best to add crimes.[1] The Instrument Redesign concluded that given the breadth of crimes covered under the umbrella term "cybercrime" and in the interest of respondent burden, it was not possible to significantly add to the core of the NCVS. Adding other types of crimes to the survey requires adding more screening questions, covering much different content than the index crimes that are surveyed on the core NCVS. In the end, the Instrument Redesign recommended using supplements as a more practical way to expand the scope of the survey. Supplements provide more flexibility to develop specialized content to measure emerging types of crime, including cybercrimes.

Based on a review by Brinton et al (2023)[2], eleven different types of cybercrimes were considered for addition to the NCVS (Table ES-1). Among those recommended for further testing were cyberstalking, identity theft, cyber fraud, computer-related forgery, cyber harassment, cyber-enabled image-based abuse, illegal access (hacking), and phishing. Survey items are recommended for additions to the Supplemental Victimization Survey (SVS; stalking supplement), Identity Theft Supplement (ITS) and Supplemental Fraud Survey (SFS).

In response to a U.S. Government Accountability Office request,[3] the research also explored measuring bias-motivated crimes that occurred on the internet. The changes to these surveys involved modifying existing questions and adding questions on the three above-mentioned supplements. These modifications were developed after a review of the literature and statutes that cover the different cybercrimes of interest. Once the questions were developed, they were reviewed by experts familiar with the measurement of cybercrime. The final set of changes were then subject to cognitive testing.

---

[1] For more information on the NCVS Instrument Redesign, see https://bjs.ojp.gov/programs/ncvs/instrument-redesign.

[2] Brinton, J., Langton L, Krebs, C. and Casper, M. (2023) An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey. Bureau of Justice Statistics, NCJ 306766.

[3] Government Accountability Office (2024) Online Extremism: More Complete Information Needed about Hate Crimes that Occur on the Internet, U.S. Government Accountability Office, GAO-24-105553.

Table ES-1. Summary of recommendations and next steps			
Cybercrime type	**Currently captured by NCVS supplement**	**Next steps**	**NCVS supplement**
Cyberstalking	Yes	Update follow-ups on cyber-enabled incidents	SVS
Identity theft	Yes	Update cyber-related probes	ITS
Cyber fraud	Partially	Add follow-ups on cyber-enabled incidents	SFS
Computer-related forgery	Partially	Add a question on how personal information was used to open a new account or access an existing account	ITS
Cyber harassment	Partially	Modify the questions to collect data on cyber harassment	SVS
Extortion	No	Further research to assess feasibility	N/A
Cyber-enabled image-based abuse	Yes	Modify questions to measure image-based abuse	SVS
Cyber-enabled sextortion	No	Further research to assess feasibility	Consider for SVS
Illegal access (hacking)	Yes	Compile occurrences of hacking for each supplement	ITS, SFS
Phishing	Yes	Compile occurrences of phishing for each supplement	ITS, SFS
Cyberbullying	Yes, for ages 12-18	No change	School Crime Supplement (SCS)

Methodology

The testing involved recruiting 75 individuals (25 for each supplement) from a non-probability sample provided by a web survey vendor. A web survey was administered to screen for victims for each of the three different types of crimes (stalking, identity theft, and fraud). Each of the web surveys replicated a portion of the corresponding NCVS supplement to identify eligible respondents. A little more than 10,000 survey responses for each of the three crimes were collected. The rationale for such a large sample was the projected rarity of cybercrime victims. Those respondents to the web survey who reported incidents to at least one of the screening questions were included in a pool for recruiting cognitive testing respondents. The goal for recruiting was to have a mix of victimization types, racial/ethnic backgrounds, ages and sexes.

There were substantially more respondents reporting an experience with cybercrime than had been anticipated based on the results of prior NCVS supplements. Upon talking to respondents during the cognitive interviews, it became apparent that these higher rates were due to respondents reporting telemarketing, spam and other issues that might qualify as harassment or annoyances of some type but are not considered illegal.

A total of six experienced cognitive interviewers were trained on at least one of the three survey protocols. One person was assigned to take the lead for each of the three crimes. Respondents were scheduled for a video-Zoom interview by a recruiting team who confirmed the conditions of the study and set up appointment times. Respondents for the bias-motivated crime interviews were first reminded of the incidents they reported during the cybercrime interview. They were then asked the bias-motivated crime question and follow-up probes.

Results and Recommendations

A total of 94 cognitive interviews were conducted. Twenty-five each on stalking, identity theft and fraud. Among these 75 respondents, 19 were also administered the bias-motivated crime questions in a separate interview. Respondents generally understood the terminology added to existing questions, as well as the new questions that were added to each supplement. A summary of these recommendations is provided in Table 8 in the report.

Based on the results of the interviews, most of the suggested modifications and additions were recommended for adoption in the supplements. In several instances we recommend collecting a summary of the most recent incident. This recommendation should also be considered for all types of crimes. Summaries are helpful when editing the data, as illustrated by the process used on the core NCVS.

One area recommended for additional research is measurement of cyber harassment. The adjectives used to describe more serious consequences did not adequately distinguish between cyber harassment and non-harassment victims. It is recommended to conduct further testing, perhaps as part of the next SVS, to further refine the methods used to identify those who do not qualify as cyberstalking victims but qualify as victims of cyber harassment. It is also recommended to collect incident summaries as part of the collection to further assess the nature of the incidents that are reported on these supplements.

Table of Contents

Appendices

Tables

Introduction

The Better Cybercrime Metrics Act (P.L. 117-116), enacted in May 2022, directed the Bureau of Justice Statistics (BJS), in coordination with the Bureau of the Census, to include questions relating to cybercrime victimization in the National Crime Victimization Survey (NCVS).[4] In response, the Bureau of Justice Statistics (BJS) has reviewed different cybercrime typologies and their relevance to the NCVS.[5] Based on this review, BJS conducted additional research through a cooperative agreement with Westat to determine which types of crimes were feasible to collect on the NCVS, design questions to collect the data and conduct testing of the proposed questions. This report describes these activities, in five sections.

The first section provides the rationale for determining which types of cybercrimes should be collected and how this data collection fits within the NCVS. The second describes the modifications to the NCVS that were tested. The third section explains the project methodology and research design. Section four presents the results of the collection, and the fifth section summarizes the results along with recommendations for moving forward.

[4] Government Accountability Office (2023) Cybercrime: Reporting Mechanisms Vary, And Agencies Face Challenges in Developing Metrics, U.S. Government Accountability Office, GAO-23-106080

[5] Brinton, J., Langton L, Krebs, C. and Casper, M. (2023) An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey. Bureau of Justice Statistics, NCJ 306766.

1. Background

Brinton et al (2023)[6] enumerate different types of cybercrimes and cyber-enabled crimes using a typology developed by Phillips et al (2022).[7] Their review links each type of act to legal statutes. The review also points to where cybercrimes are already collected by the National Crime Victimization Survey (NCVS), which is primarily in the NCVS supplements, and makes recommendations on next steps to expand collection of these crimes.

1.1 What Types of Cybercrimes Should be Measured on the NCVS?

The typology by Phillips et al (2022)[8] identifies 53 different types of cybercrimes. Some may not be illegal according to state or federal statutes (e.g., grooming). Others might be illegal, but are not against a person (e.g., political interference, espionage). There are eleven types of cybercrimes that Brinton et al (2023)[9] recommended as within the scope of the NCVS because they are both illegal in most (or all) states and/or federal statutes, as well as occurring against an individual rather than a business or organization. These include cyberstalking, identity theft, cyber fraud, computer-related forgery, cyber harassment, extortion, cyber-enabled image-based abuse, cyber-enabled sextortion, illegal access (hacking), phishing, and cyberbullying.

As part of the recent NCVS Instrument Redesign, there were discussions related to how best to expand the content of the survey. As noted in a National Academies of Science, Engineering, and Medicine ("National Academies") report on the future of the NCVS, the survey needs to expand the types of crimes measured as technology and society change.[10] With that in mind, the NCVS Instrument Redesign considered several possibilities on how best to add crimes.[11] The Instrument Redesign concluded that given the breadth of crimes covered under the umbrella term "cybercrime" and in the interest of respondent burden, it was not possible to significantly add to the NCVS core instrument. Adding additional types of crimes to the survey requires adding more screening questions, potentially covering much different content than the index crimes that are surveyed on the core NCVS. In the end, the Instrument Redesign recommended using supplements as a more practical way to expand the scope of the survey. NCVS supplemental surveys provide more flexibility to measure emerging types of crime, including cybercrimes. This proposal is consistent with a recent National Academies report on the measurement of cybercrime.[12]

---

[6] Brinton, J., Langton L, Krebs, C. and Casper, M. (2023) An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey. Bureau of Justice Statistics, NCJ 306766.

[7] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., and Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 379-398 https://doi.org/10.3390/forensicsci2020028

[8] *Ibid.*

[9] Brinton, J., Langton L, Krebs, C. and Casper, M. (2023) An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey. Bureau of Justice Statistics, NCJ 306766.

[10] Groves, R.M. and Cork, D.L. (Eds) (2008) Surveying Victims: Options for Conducting the National Crime Victimization Survey, National Research Council: Washington D.C.

[11] For more information on the NCVS Instrument Redesign, see https://bjs.ojp.gov/programs/ncvs/instrument-redesign.

[12] National Academies of Sciences, Engineering, and Medicine (2025) Cybercrime Classification and Measurement. Washington, DC: The National Academies Press. https://doi.org/10.17226/29048

1.2 Cybercrimes Proposed for Inclusion on the NCVS

This section reviews each of the types of cybercrimes considered for addition to the NCVS as enumerated by Brinton et al (2023)[13] and describes the rationale for which crimes are most compatible for inclusion on the NCVS. Table 1 summarizes this information for each type of crime, including the recommended next steps and NCVS supplement that should capture these crimes.

Table 1. Summary of recommendations and next steps

Cybercrime type	Currently captured by NCVS supplement	Next steps	NCVS supplement
Cyberstalking	Yes	Update follow-ups on cyber-enabled incidents	SVS
Identity theft	Yes	Update cyber-related probes	ITS
Cyber fraud	Partially	Add follow-ups on cyber-enabled incidents	SFS
Computer-related forgery	Partially	Add a question on how personal information was used to open a new account or access an existing account	ITS
Cyber harassment	Partially	Modify the questions to collect data on cyber harassment	SVS
Extortion	No	Further research to assess feasibility	N/A
Cyber-enabled image-based abuse	Yes	Modify questions to measure image-based abuse	SVS
Cyber-enabled sextortion	No	Further research to assess feasibility	Consider for SVS
Illegal access (hacking)	Yes	Compile occurrences of hacking for each supplement	ITS, SFS
Phishing	Yes	Compile occurrences of phishing for each supplement	ITS, SFS
Cyberbullying	Yes, for ages 12-18	No change	School Crime Supplement (SCS)

Cyberstalking

The Supplemental Victimization Survey (SVS) asks persons age 16 or older who completed an NCVS interview about their experiences with stalking and provides a relatively comprehensive list of cyber-related methods to commit stalking. The NCVS currently publishes these estimates, which can be used as a national estimate for this type of cybercrime. For example, questions SQ1_h – SQ1_l of the supplement include:

SQ1_h. Has anyone spied on you or monitored your activities using technologies such as a listening device, camera, or computer or cell phone monitoring software?

[13] Brinton, J., Langton L, Krebs, C. and Casper, M. (2023) An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey. Bureau of Justice Statistics, NCJ 306766.

Yes 01
No.....02

SQ1_i. Has anyone tracked your whereabouts with an electronic tracking device or application, such as GPS or an application on your cell phone?

Yes 01
No.....02

SQ1_j. Has anyone posted or threatened to post inappropriate, unwanted, or personal information about you on the Internet, including private photographs, videos, or spreading rumors?

Yes 01
No.....02

SQ1_k. Has anyone sent you unwanted e-mails or messages using the Internet, for example, using social media apps or websites like Instagram, Twitter, or Facebook?

Yes 01
No.....02

SQ1_l. Has anyone monitored your activities using social media apps like Instagram, Twitter, or Facebook?

Yes 01
No.....02

According to the 2019 SVS, 0.4 percent of the general population age 16 or older have been stalked by one or more of the above tactics.[14]

However, some technologies have evolved since the SVS was last revised. Social media continues to be among the most popular methods used by perpetrators to stalk others online.[15] The SVS specifically referenced social media apps like Instagram, Twitter, and Facebook, which continue to be among the most widely used in the United States according to an online survey conducted by Statista. [16]

Other apps, however, like TikTok and Snapchat, are also popular according to the same survey. Therefore, the questions should reference a broader range of social media apps on the next SVS.

[14] Morgan, R.E. and Truman, J.L. (2022) Stalking Victimization, 2019. Bureau of Justice Statistics, NCJ 301735.

[15] National Network to End Domestic Violence, (2021) Tech Abuse in the Pandemic & Beyond: Reflections from the field. National Network to End Domestic Violence. Tech Abuse in the Pandemic & Beyond (squarespace.com); Vogels, E.A. (2021) The State of Online Harassment. Pew Research Center. https://www.pewresearch.org/wp-content/uploads/sites/20/2021/01/PI_2021.01.13_Online-Harassment_FINAL-1.pdf

[16] Bashir, U. (2025) Social Network Usage by Brand in the U.S. 2025. Statista. https://www.statista.com/forecasts/997135/social-network-usage-by-brand-in-the-us

Research[17] indicates that electronic tracking devices and applications (e.g. "e-trackers" such as Apple AirTags, Tile Trackers) are not used as widely as social media and other technologies, but they remain significant. Other technologies have also evolved since the last iteration of the SVS that warrant inclusion on the next supplement, such as wireless headphones (e.g., AirPods) and smart watches (e.g., Apple Watch).

To account for these changes in technology, this research modified the SVS to include additional cyber-enabled methods that might be used in a stalking incident. Another update for consideration is whether particular technologies should be asked about separately so that estimates can be provided beyond the general categories on the SVS.

Identity Theft

A second cybercrime considered for collection is identity theft. The Identity Theft Supplement (ITS) is administered to persons age 16 or older who completed an NCVS interview and asks respondents if they had experienced identify theft during the past 12 months. As part of the supplement, victims are asked how they believe their identity was stolen:

How do you think your personal information was obtained?

I lost an item that included my personal information 01

My wallet, checkbook, or purse was stolen 02

My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash 03

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04

It was stolen during an online purchase/transaction 05

Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader 06

I responded to a scam email/phone call 07

My personal information was stolen from my personnel or human resources at my place of employment 08

It was stolen from an office/company such as a financial institution, retailer, service provider, or restaurant 09

Obtained in another way (specify) 10

Analysis of these data[18] indicate that 37.5 percent of the most recent identity theft incidents were cyber-enabled. The estimate is based on including online transactions (category 5 above), scam email or phone call (category 7 above), or electronic access to the victim's work or home computer, cell phone, tablet or other electronic device (category 4 above). This estimate could be made more precise by refining these categories. Category 7 combines scam email and phone calls and category

[17] *Ibid*; Hanson, E.J. and Finklea, K, (2022) Stalking Concerns Raised by Bluetooth Tracking Technologies: In Brief. Congressional Research Service, R47035.

[18] Harrell, E. and Thompson, A. (2023) Victims of Identity Theft, 2021. Bureau of Justice Statistics, NCJ 306474.

9 does not address whether the information was stolen from cyber (e.g., hacking a database) or non-cyber methods (e.g., stealing hardcopy files).

A second issue identified by Harrell and Thompson (2023)[19] was that only 21.2% of the victims of identity theft knew how the offender obtained their personal information. There are differences among the types of identity theft with respect to the extent a respondent could report how it happened. Those most likely to report how it occurred were victims who had just opened a new account (29.2%) and bank-related theft (25.6%). Those least likely to be able to report how the offender obtained their personal information are those who experienced email/social media misuse (14.6%) and other misuse of personal information (15.8%). Among those that knew how the offender obtained their personal information, about 38% reported it was done through cyber-enabled means.

This research considered modifications of the questions to more precisely narrow down incidents that were cyber-enabled. In particular, it tested disentangling phone and email, as well as the category related to cyber-enabled theft.

Cyber Fraud

As with identity theft and cyberstalking, there is a NCVS supplement that covers fraud. The Supplemental Fraud Survey (SFS) collects data on the experiences of persons age 16 or older who completed an NCVS interview across seven types of personal financial fraud during the preceding 12 months. The most recent survey on financial fraud was completed in 2017 and is based on a typology developed with input from other organizations that are interested in measuring this type of crime. According to that survey, [20] 1.25 percent of persons age 18 or older were victims of financial fraud. About two-thirds were victims of fraud when trying to obtain a consumer product or service. The other six types of fraud each constitute one to eleven percent of the victims.

Distinguishing between services or products that were not received because of intentional deception to defraud versus poor service is not straightforward. The SFS collects data that allows variance in the criteria used for defining fraud. These definitions largely affect fraud related to products and services. Unlike the SVS and ITS, the SFS questionnaire does not ask about the methods used to commit the fraud. Consequently, it is not possible to parse the fraud incidents into cyber-enabled and non-cyber-enabled victimizations.

According to the FBI's Internet Crime Complaint Center,[21] cyber fraud occurs in various ways with people of all ages and backgrounds. Victims of this crime may receive an email, text message or phone call to initiate the fraudulent scheme. Many incidents of cyber fraud are cross-platform. For example, the incident may be initiated through social media, but the perpetrator receives payment on a different platform.[22] Inserting questions on the SFS asking about the mode used to initiate the fraudulent transaction should be possible.

---

[19] *Ibid.*

[20] Morgan, R.E. (2021) Financial Fraud in the United States, 2017. Bureau of Justice Statistics, NCJ 255817.

[21] Federal Bureau of Investigation (undated) Elder Fraud Report 2022. Internet Crime Complaint Center, Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf

[22] Breen, C., Herley, C. and Redmiles, E.M. (2022) A Large-Scale Measurement of Cybercrime Against Individuals. Proceedings of the 2022 Cyber Harassment Conference on Human Factors in Computing Systems, April 2022, Article No.: 122, pp. 1-41. https://dl.acm.org/doi/10.1145/3491102.3517613

Following this recommendation, follow-up questions were developed that determine whether the fraud occurred using cyber-related medium. The SFS is currently divided into a set of screening questions and a detailed crime incident report (CIR). A respondent that reports fraud for one or more of the types of fraud is administered a CIR specific to the type of fraud reported. The new items should be added to the CIR to collect information on the mode used to initiate the fraudulent transaction. Placing these items on the CIR will allow for collecting these data for the most recent incident for each type of fraud reported by the respondent.

An initial review of the frequencies of the 2017 SFS indicates about 80 percent of victims report one incident.[23] Applying the different definitions used for fraud (e.g., Fraud 1, Fraud 2…) as specified and defined by Morgan (2021)[24] would likely increase the share of victims reporting more than one incident. However, this also creates structural challenges for the survey. Nonetheless, the SFS produces descriptive data for different types of fraud using the most recent incident. Producing data on cyber fraud using the same strategy would be consistent with this.

Adding items to the CIR assumes that victims that are subject to cyber fraud will think about these incidents when asked the more general SFS screening items. For example, someone who was targeted by a pop-up request on their computer may consider this as a scam related to the internet rather than one of the types of fraud described in the SFS. In principle, this can be solved by adding a screening item that asks about cyber fraud. However, the approach used on the SFS screener makes it difficult to insert a screening item that specifically asks about cyber fraud. The SFS asks respondents about seven specific types of fraud. Adding a screener item focusing on a characteristic of the event (i.e., cyber-enabled) will capture events that overlap with those covered in the other items. In addition, an entirely different detailed incident form will need to be developed to classify the incident into one of the seven types. An alternative, and less intrusive, change is to insert a reminder in the introduction to the screener to include incidents where the fraud occurred as a result of cyber-enabled contacts.

Computer-related Forgery

Forgery occurs when text, images or documents are altered to make it appear to originate from a legitimate source.[25] This is closely related to identity theft. The ITS includes questions on someone using the victim's personal information without permission to either use an existing account or to open new accounts. Collecting data on whether these instances of identity theft were completed using cyber-enabled methods will be collected as proposed above in the discussion of identity theft. This will measure computer-related forgery.

Cyber Harassment

Definitions of harassment and cyber harassment vary by state but generally involve engaging in an act or behavior that torments, annoys, terrorizes, offends or threatens an individual. One option to collect data on cyber harassment is through the SVS. In order to consider collecting these data on the SVS, it is important to understand how harassment and cyber harassment are defined in the states. To better understand which states have laws and what they cover, this research completed

---

[23] Morgan, R.E. (2021) Financial Fraud in the United States, 2017. Bureau of Justice Statistics, NCJ 255817.

[24] For definitions of fraud types, see *Measurement of personal financial fraud victimization* in Morgan, R.E. (2021) Financial Fraud in the United States, 2017. Bureau of Justice Statistics, NCJ 255817.

[25] Tsakalidis, G., and Vergidis, K. (2017) A Systematic Approach Toward Description and Classification of Cybercrime Incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(4), 710-729 https://ieeexplore.ieee.org/document/7936557

an environmental scan of statutes on harassment and cyber harassment in all 50 states and the District of Columbia (D.C.). The scan involved reviewing current harassment and cyber harassment laws through searches of the internet, as well as a review of the harassment and stalking laws enumerated by Hazelwood and Koon-Magnin (2013)[26] and Kaplun (2023)[27]. The review revealed that 45 states have laws that are labelled as 'harassment' or have 'harassment' in the title of the statute (Table 2).

In Florida and D.C., no harassment statutes were found, and the stalking statute did not address it. In the other four states without a harassment statute (Georgia, Mississippi, North Carolina, Wyoming), specific forms of harassing behavior are defined within the stalking statutes. While some of the harassment statutes do not mention cyber-enabled modes of contact, there are other laws that reference harassment by telephone and electronic communication. For example, in Michigan, there is a statute that prohibits posting:

> *"….a message through the use of any medium of communication, including the internet or a computer, computer program, computer system, or computer network, or other electronic medium of communication, without the victim's consent, if all of the following apply – posting message could cause 2 or more noncontinuous acts of nonconsensual contact with victim, posting the message would make the victim feel terrorized, frightened, intimidated, threatened, harassed, or molested, cause reasonable person to suffer emotional distress." (750.411s)*

A similar statute in Mississippi called "Posting of messages through electronic media for purpose of causing injury to any person" (97-45-17) covers harassing behavior using electronic media.

In many states the harassment statute relies on a 'reasonable person' criterion in their definition of law. For example, in Alabama, harassment is defined as a:

> *"…threat, verbal or nonverbal, made with the intent to carry out the threat that would cause a reasonable person …to fear for his or her safety." (13A-11-8).*

[26] Hazelwood, S.D. and Koon-Magnin, S. (2013) Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis. *International Journal of Cyber Criminology* 7(2): 155-168. https://www.proquest.com/docview/1492867427

[27] Kaplun, K. (2023) Tracking and Trailing Each Other: Tracing Stalking and Harassment Through Time and Technology. Dissertation submitted to the Graduate School-Newark, Rutgers University of New Jersey. https://rucore.libraries.rutgers.edu/rutgers-lib/72649/

Or in New Jersey:

> *"Harassment consists of …. conduct that is intended to annoy, seriously alarm or terrorize another person and that serves no lawful purpose. The conduct must be such that it would cause a reasonable person to suffer substantial emotional distress…" (30-3A-2).*

In some states, harassment is defined by specific acts that would serve 'no legitimate purpose', such as making calls that "harass, annoy, or alarm another person with no intent of legitimate communication" (e.g., Indiana, § 35-45-2-2).

The difference between harassment and stalking is not consistent across states. One distinction is the number of times the incident occurs. In most states, a single event can qualify as harassment, whereas stalking requires repeated events or a 'course of conduct.' However, there are a number of states (18) that list a 'course of conduct' in the harassment statute. In a few of these (5), the harassment specification is embedded in the stalking statue. In some others (3), only some of the behaviors require repeated events.

Another distinction between the two crimes are the consequences for the victim related to the offender's behavior. Just like stalking, the definition of harassment in many states (28) requires the behavior to lead to fear and/or emotional distress. In other states, there is language in harassment statutes that does not specifically mention fear or emotional distress but refers to other consequences. Twenty-two states, include reference taking actions that cause 'alarm.' In Arizona, for example, harassment is defined as conduct that "…would cause a reasonable person to be seriously alarmed, annoyed, humiliated or mentally distressed" (13-2921).

In those states that have both harassment and stalking laws, the stalking statute refers to more severe consequences for the victim. For example, the Alaska harassment statute references the "…intent to harass or annoy another person," (11.61.120) while the stalking statute "…places another person in fear of death or physical injury" (11.41.270). In Idaho, harassment is defined as: "…contact that would cause a reasonable person to suffer emotional distress…." (35-35-10-2), whereas stalking is defined as conduct that causes "…a reasonable person to feel terrorized, frightened, intimidated, or threatened…" (35-45-10-1). Similarly, Kentucky defines harassment as a series of acts intended to "…intimidate, harass, annoy, or alarm another person" for no legitimate purpose (525.070), whereas the stalking statute requires "…intent to place that person in a reasonable fear of sexual contact, physical injury or death" (508.114).

Table 2. Harassment and Cyber Harassment Laws by State and the District of Columbia		
State	**Statute title**	**Is cyber harassment included?**
Alabama	13A-11-8. Harassment or harassing communications	Yes
Alaska	11.61.120. Harassment in the second degree	Yes
Arizona	13-2921. Harassment	Yes
Arkansas	5-71-208. Harassment 5-71-209 Harassing communications	Yes
California	422. Criminal threats 653.2. Cyber harassment 527.6. Civil harassment order	Yes
Colorado	§ 18-9-111. Harassment	Yes
Connecticut	§ 53a-183. Harassment in the second degree § 53a-182b Harassment in the first degree	Yes
Delaware	§ 1311. Harassment	Yes
District of Columbia	No harassment statute. § 22–3133. Stalking	No
Florida	No harassment statute. 784.048. Stalking	No
Georgia	16-11-39.1. Harassing communications 15-5-90. Stalking	Yes
Hawaii	§711-1106 Harassment §711-1106.5 Harassment by stalking	Yes
Idaho	18-6710. Use of telecommunication to annoy, terrify, threaten, intimidate, harass or offend by lewd or profane language, requests, suggestions or proposals – threats of physical harm – disturbing the peace by repeated telecommunication	No
Illinois	26-5-1. Transmission of obscene messages 26-5-2. Harassment by telephone 26-53. Harassment through electronic communications	Yes
Indiana	§ 35-45-2-2. Harassment § 34-6-2-51.5. Harassment	Yes
Iowa	708.7. Harassment	Yes
Kansas	21-6206. Harassment by telecommunication device 31a. Protection from stalking	Yes

State	Statute title	Is cyber harassment included?
Kentucky	525.070. Harassment 525.080. Harassing communication	Yes
Louisiana	14: § 285 Unlawful communications; telephones and telecommunications devices; improper language; harassment 14: 40.3. Cyberstalking 14: 40.2. Stalking	Yes
Maine	§ 506. Harassment by telephone or electronic communication § 506-A Harassment	Yes
Massachusetts	Section 43A. Criminal harassments 14A. Annoying telephone calls or electronic communication	Yes
Maryland	§ 3-803. Harassment § 3-805 Misuse of electronic communication	Yes
Michigan	No separate harassment statute 750.411h. Stalking 750.411s. Posting message through electronic medium	Yes
Minnesota	609.749. Harassment, stalking, penalties 565.090. Harassment, first degree 609.795. Letter, telegram, or package; opening; harassment	Yes
Mississippi	Harassment is only mentioned in the stalking statute § 97-3-107. Stalking § 97-45-15. Cyberstalking § 97-45-17. Posting messages through electronic media for purpose of causing injury § 07-29-45. Obscene electronic communications	Yes
Missouri	565.090. Harassment, first degree 565.091 Harassment, second degree	No
Montana	45-5-221. Malicious intimidation or harassment relating to civil or human rights 45-8-213. Privacy in communications	Yes
Nebraska	28-311.02. Stalking and harassment 28-1310. Intimidation by telephone or electronic communication	Yes
Nevada	200.575. Stalking, includes cyber stalking 200.571 Harassment	No
New Hampshire	644:4. Harassment	Yes
New Jersey	2C:33-4. Harassment 2C:33-4.1. Cyber-harassment	Yes

State	Statute title	Is cyber harassment included?
New Mexico	12.1-17-07. Harassment	Yes
New York	240.30. Aggravated harassment in the second degree 240.31. Aggravated harassment in the first degree	Yes
North Carolina	§ 14-196. Using profane, indecent or threatening language to any person over telephone; annoying or harassing by repeated telephoning or making false statements over telephone §14-196.3. Cyberstalking § 14-277.3A. Stalking	Yes
North Dakota	12.1-17-07. Harassment	Yes
Ohio	2917.21. Telecommunications harassment 2903.211. Menacing by stalking	No
Oklahoma	§ 21-1172. Obscene, threatening or harassing telecommunication or other electronic communications	Yes
Oregon	166.065. Harassment	Yes
Pennsylvania	2709. Harassment 2709.1. Stalking	Yes
Rhode Island	§ 19-14.9-6. Harassment or abuse § 11-52-4.2. Cyberharassment and cyberstalking	Yes
South Carolina	16-3-1700 (A) and (B). 16-17-430 Unlawful communication	Yes
South Dakota	22-19A-1. Stalking 22-19A-4. Harassment	No
Tennessee	39-17-308. Harassment	Yes
Texas	§ 42.07. Harassment	Yes
Utah	76-5-106. Harassment. 76-9-201. Electronic communication harassment	Yes
Vermont	13 V.S.A. § 1027. Disturbing peace by use of telephone or other electronic communications	Yes
Virginia	18.2-186.4. Use of person's identity with intent to coerce, intimidate, or harass 18.2-427. Use of profane, threatening, or indecent language over public airways or by other methods 18.2-429(B). Causing a telephone, digital pager, or other device to ring or signal with intent to annoy 18.2-152.7:1. Harassment by computer	Yes
Washington	RCW 9A.46. Harassment	Yes

State	Statute title	Is cyber harassment included?
West Virginia	§61-2-9a. Stalking, harassment §61-2-9a. Obscene, anonymous, harassing and threatening communications by computer, cell phones and electronic communication devices;	Yes
Wisconsin	947.013. Harassment 947.0125. Unlawful use of computerized communication systems	Yes
Wyoming	§ 6-2-506. Stalking	Yes

The review found 44 of the 50 states and D.C. have cyber harassment laws.[28] This finding assumes that if the mode is not specifically mentioned in the harassment statute, then cyber contact is not covered. The cyber harassment laws are either embedded within the existing harassment law or a separate statute has been added. For example, in Connecticut, the harassment law specifies that it can occur when the offender:

> *"Communicates with a person by …. electronic mail or text message or any other electronically sent message, whether by digital media account, messaging program or application or otherwise by computer, computer service or computer network…." (53a-183).*

This contrasts with a state like Kentucky which has a separate statute "Harassing Communication" (525.080) that includes "…telephone, telegraph, mail, or any other form of electronic or written communication in a manner which causes annoyance or alarm and serves no purpose of legitimate communication."

In those states that have separate cyber harassment laws, the language does not consistently refer to the same consequences to the victim as the harassment law. For example, in Alabama, the "Harassing Communication" section refers to communication that is likely to "harass or cause alarm", which is different than the general harassment law which refers to "fear for safety". The more specific cyber harassment statutes also tend to refer to specific behaviors. In 19 states, the statutes specific to cyber harassment reference the use of 'coarse, lewd or obscene language'. Other statutes emphasize the sequencing of the communication, such as making repeated contacts for no legitimate purpose (e.g., to tie up the phone, at inconvenient hours).

With respect to collecting data on cyber harassment, the approach taken was to add a question to the SVS to measure reactions that are not as extreme as measured by the current fear (SQ3a) or distress items (SQ3b). Examples of this wording, suggested by the statutes refer to reactions such as: 'harass', 'annoy', 'cause alarm', 'intimidate', 'torment', or 'embarrass'.

The proposal is to define a victim of cyber harassment as anyone who: 1) reports two or more instances of stalking/harassment, 2) does not report consequences that define being stalked (fear, distress, personal victimization) and 3) reports reactions such as intimidation, harassment, torment. Two or more incidents is recommended to be consistent with the prevalent legal criteria defining harassment as a 'course of conduct'.

Extortion

Extortion related to cybercrime typically consists of planting malware on a computer which locks up critical data or makes the system inoperable. The offender then extorts money from the victim in order to regain access to their data or prevent their data's release to others. It isn't clear how often this type of crime happens to individuals as private citizens. For example, the FBI reports that they received 39,416 complaints from both businesses and private individuals in 2022 related to

[28] The states without cyber harassment laws are Florida, Idaho, Missouri, Nevada, Ohio, and South Dakota. Additionally, the District of Columbia does not have cyber harassment laws. Further work should be conducted to assess whether the harassment laws do not cover cyber-related communication.

extortion.[29] Breen et al (2022)[30] report seven different estimates of extortion, ranging from the FBI to survey estimates, including the authors' survey, the NCVS, and the Crime Survey of England and Wales (CSEW). These estimates are all well below one percent, with the authors' survey being 0.1 percent for a prevalence rate among identified internet users. The CSEW is somewhat higher (0.8%). However, it isn't clear how the CSEW estimate of 'computer misuse' corresponds specifically to extortion. To provide some perspective the 2022 estimates for rape and sexual assault had a prevalence rate of 0.1 percent.[31]

All of these studies are grounded in generally accepted statistical methodology and reasoning. However, there are reasons to be skeptical of the estimates. Breen et al (2022)[32] calculated estimates using an extrapolation method to convert the two-year reference period to a one-year estimate. They are based on an internet probability panel, rather than a probability sample, and the small sample size resulted in large confidence intervals and reduced precision in estimates. As noted above, it isn't clear how the CSEW estimates provided correspond to the definition of extortion. Given the very low prevalence, it is not recommended, at this time, to add extortion to any of the NCVS supplements. Further research on how often this occurs to private citizens is recommended before adding to the NCVS supplements.

Cyber-enabled Image-Based Abuse

Cyber-enabled image-based abuse consists of a perpetrator creating and/or distributing private sexual images.[33] The SVS includes a question that would cover both behaviors (SQ_POSTS). However, the question covers topics in addition to distributing images (e.g., personal information, spreading rumors). It is proposed to modify the SVS to be more specific to image-based abuse.

Cyber-enabled Sextortion

Sextortion refers to threatening to disseminate explicit, intimate or embarrassing images of a sexual nature without consent, usually for the purposes of something in return (money, sexual acts, etc.).[34] This is considered illegal; all states have an explicit statute or related clauses related to 'revenge porn'. There are also federal laws covering this type of crime.[35] As noted above, it is recommended that posting or threats to post indecent images on the internet will be added to the SVS. Once these results are compiled, it is recommended that further research be conducted to assess collecting data on sextortion. For example, it should be possible to add questions to the SVS detailed incident form that assesses if threats to extort money or sexual acts were experienced by those respondents

---

[29] Federal Bureau of Investigation (undated) Internet Crime Report 2022. Internet Crime Complaint Center, Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[30] Breen, C., Herley, C. and Redmiles, E.M. (2022) A Large-Scale Measurement of Cybercrime Against Individuals. Proceedings of the 2022 Cyber Harassment Conference on Human Factors in Computing Systems, April 2022, Article No.: 122, pp. 1-41. https://dl.acm.org/doi/10.1145/3491102.3517613

[31] Thompson, A. and Tapp, S.N. (2023) Criminal Victimization, 2022. Bureau of Justice Statistics, NCJ 307089.

[32] Breen, C., Herley, C. and Redmiles, E.M. (2022) A Large-Scale Measurement of Cybercrime Against Individuals. Proceedings of the 2022 Cyber Harassment Conference on Human Factors in Computing Systems, April 2022, Article No.: 122, pp. 1-41. https://dl.acm.org/doi/10.1145/3491102.3517613

[33] McGlynn, C., and Rackley, E. (2017). Image-Based Sexual Abuse. Oxford Journal of Legal Studies, 37(3), 534-561 https://www.jstor.org/stable/48561003

[34] Patchin, J. W., and Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. Sexual Abuse, 32(1), 30-54. https://journals.sagepub.com/doi/10.1177/1079063218800469

[35] *Ibid.*

who reported image-based stalking. However, at this time, it is not recommended to add this question to the SVS without additional research.

Hacking and Phishing

Hacking and phishing are, in many cases, used to commit other types of cybercrime. For example, in the ITS, hacking is referenced as one of the ways used to carry out the crime. Some surveys do collect data on hacking and phishing as stand-alone incidents.[36] Since hacking and phishing are methods to commit other types of crimes, the proposed revisions sought to gather this information when collecting data on more specific types of cybercrime (e.g., identity theft, fraud). Separate estimates of hacking and phishing can be published within the other types of crimes (e.g., fraud, stalking). Otherwise, it would be necessary to create a separate supplement to collect these data or add questions to the core NCVS, as some European surveys have done.[37] However, as noted in the introduction, adding to the NCVS core survey is not practical, given the survey has just been redesigned and BJS has fully transitioned to the redesigned NCVS instrument in 2025.

Cyberbullying

Cyberbullying is defined as "…willful and repeated harm inflicted through the medium of electronic text".[38] The School Crime Supplement (SCS) collects data on cyberbullying for minors (Q28v1, 30v2). For adults, the distinction between this and different forms of harassment or stalking is not clear-cut. Furthermore, cyberbullying among adults is not against the law in most states or in federal law. For purposes of the present research, it is recommended to maintain the collection of cyberbullying in the SCS. Given this type of act does not rise to the level of a crime for adults in most states, it is not recommended that a measure of cyberbullying should be added to the NCVS or any NCVS supplements besides the SCS.

[36] For a summary of national surveys collecting these data, see Reep-van den Bergh, C.M.M. and Junger, M. (2018) Victims of Cybercrime in Europe: A Review of Victim Surveys. Crime Science 7:5 https://doi.org/10.1186/s40163-018-0079-3

[37] Reep-van den Bergh, C.M.M. and Junger, M. (2018) Victims of Cybercrime in Europe: A Review of Victim Surveys. Crime Science 7:5 https://doi.org/10.1186/s40163-018-0079-3

[38] Patchin, J. W., and Hinduja, S. (2006). Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. Youth Violence and Juvenile Justice, 4(2), 148–169 https://doi.org/10.1177/1541204006286288

2. Changes Tested

The proposed changes to the NCVS supplements to measure cybercrime are a combination of new and modified questions. These changes were initially drafted by the Westat research team in collaboration with BJS and then reviewed by a group of outside experts on cybercrime. Modifications were made in light of the expert review and then tested as part of the research. Appendix I provides the list of experts who reviewed the initial draft.

2.1 Stalking

The changes to the SVS were made in the primary screening items, as well as an additional question on the consequences of stalking. This would allow analysts to estimate prevalence for any crimes occurring in the last 12 months. If the item were placed on the detailed incident form, the estimates would be restricted to the most recent incident.

The changes tested are described below. The variable names correspond to those on the current SVS questionnaire, [39] when a modification was made. New variable names were created for questions proposed for addition to the instrument. The changes include:

1. **Separating phone calls from text messages.** The current question asks about both phone calls and text messages. Because these two mediums are related to cybercrimes in different ways, they were separated into two questions (SQ_TELEPHONE, SQ_TEXTMESSAGES).
2. **Adding additional information covering social media and websites.** The question on social media apps was supplemented with additional examples and applications. Two questions were tested, one with general reference to cyber platforms (e.g., 'dating apps'; SQ_WEBSITES) the other with more specific examples (e.g., TikTok; SQ_WEBSITES_1).
3. **Separating spying technologies.** The question on monitoring and spying was separated into direct observation (e.g., listening devices; SQ_TECHNOLOGY_DIRECT) and indirect (e.g., cell phone; SQ_TECHNOLOGY_INDIRECT).
4. **Adding 'e-tracker' as an example to the electronic tracking question.** Updated the electronic tracking question with 'e-tracker' as an example (SQ_APPLICATION).
5. **Updating the question on use of social media to monitor behavior.** The question on tracking with social media was updated with additional examples. Two alternatives were tested. One with specific examples (e.g., Facebook; SQ_SOCIALMEDIA) and the other with more general examples (e.g., 'discussion forum'; SQ_SOCIALMEDIA_1).
6. **Adding a question on image-based sexual abuse**. A question was added on image-based sexual abuse (SQ_IMAGE_BASED_SEXUAL_ABUSE).
7. **Supplementing the question on posting inappropriate material.** The question on posting inappropriate material was supplemented with additional examples, including indecent and personal information. Alternative questions were tested. One had all of the examples in a single question (SQ_POSTS). The second separated the question into two

[39] For more information about the SVS and to see the most recent questionnaire, see: https://bjs.ojp.gov/data-collection/supplemental-victimization-survey-svs

parts, one that asked specifically about inappropriate or untrue information (SQ_POSTS_1) and the other about personal information (SQ_POSTS_2).

8. **Adding a question on other reactions to repeated incidents to measure harassment.** Respondents who reported some type of repeated incident on the screener, but did not meet the stalking criteria, were asked if they experienced other types of emotions (e.g., alarmed, intimidated; SQ_OTHERREACTIONS).

2.2 Identity Theft

The changes to the ITS were also made in the screening portion of the survey for reasons similar to the SVS. The survey screens for seven different types of identity theft and if one is identified, a detailed incident form is administered for the most recent incident.

The changes tested are described below. The variable names correspond to those on the current ITS questionnaire[40] when a modification was made. New variable names were created for questions proposed for addition to the instrument. The changes include:

1. **Adding a question on how the information was used for five types of identity theft.** A question was added to the screener for five types of identity theft (P1, P3, P6, P8, P10). Adding this to the screener allows analysts to estimate prevalence for all incidents that occurred in the last 12 months.
2. **Modifying the question on how the information was obtained.** The current question on how the information was obtained includes both cyber and non-cyber methods (THINK_PI_OBTAINED) and has been used to estimate cyber identity theft for the most recent incident. For six types of identity theft, the test moved this question to the screener and supplemented the categories to get more specific information on cyber-related items (P2, P4, P5, P7, P9, P11). Moving this to the screener allows analysts to estimate prevalence for all incidents that occurred in the last 12 months.
3. **Adding examples to the question on having an email or social media account.** Specific examples added included YouTube, Reddit and Pinterest. (EMAIL_SOCIAL_EVER).
4. **Adding examples to question on the type of social media account used without permission.** The corresponding social media examples of YouTube, Reddit and Pinterest were added when asking about social media (SOCIAL_MEDIA_USED).
5. **Adding a question on opening an email or social media account while pretending to be the respondent.** This question was added to collect data on forgery and identity theft (9bb).
6. **Adding examples for the types of accounts ever used without permission.** The examples expanded on what is meant by telephone and internet accounts (EXISTING_ACCTS_USED_PASTYR).
7. **Adding the new examples for the type of account used**. The corresponding examples were carried through to all questions which listed the accounts used (EX_PHONE, 13aa).

[40] For more information about the ITS and to see the most recent questionnaire, see: https://bjs.ojp.gov/data-collection/identity-theft-supplement-its

8. **Adding examples for the types of new accounts opened.** Added more examples to the social media account (YouTube, Reddit and Pinterest) and separated telephone and internet accounts (OPEN_NEWACCT_EVER).
9. **Adding the new examples for the type of account opened.** The corresponding examples were carried through to all questions which listed the new accounts opened (NEW_SOCIAMEDIA, NEW_PHONE, 17aa).
10. **Adding a question on whether someone else has obtained their personal information using different cyber and non-cyber methods.** A question was added to collect data on hacking and phishing for those who did not already report such instances in prior questions (P12).
11. **Checking if the hacking and phishing has occurred in the last 12 months.** This allows analysts to estimate of prevalence for all incidents of hacking and phishing in the last 12 months (P13).

2.3 Fraud

The SFS has a series of screening questions for seven types of personal financial fraud. For respondents who report experiencing fraud, an incident form is administered about the one incident or the most recent incident. Changes to the SFS were made on the detailed incident form. Because of the ambiguous nature of measuring fraud, BJS allowed for users to examine different operational definitions of this type of crime. The detailed incident form was used to apply these definitions. For this reason, the changes were made to each of the incident forms that asked about the characteristics of different types of fraud.

The changes tested are described below. The variable names correspond to those on the current SFS questionnaire[41] when a modification was made. New variable names were created for questions proposed for addition to the instrument. The changes include:

1. **Adding a question on how the victim first found out about the fraud**. This question was added on the incident forms for each type of fraud (P1, P2, P3, P4, P5, P6, S7B3).
2. **Modifying the existing question for relationship or trust fraud regarding how the victim was contacted**. This question includes different types of cyber methods. The change enhanced the categories to be consistent with the changes made to other questions (TRUST_CONTACT).
3. **Adding questions and response categories on the use of cryptocurrency for each type of fraud**. This addition recognized that use of this type of currency could be related to cyber methods for committing fraud (S1B31, S2B21, S3B21, S3B31, S4B41, S5B21, S6B61, S7B41; added response category to INVEST_TYPE).

2.4 Bias-Motivated Crimes

While the Better Cybercrime Metrics Act (P.L. 117-116) does not explicitly mandate BJS capture bias-motivated crime that occurs on the internet, the U.S. Government Accountability Office recommended that BJS explore opportunities to do so either through the core NCVS or an

[41] For more information about the SFS and to see the most recent questionnaire, see: https://bjs.ojp.gov/data-collection/supplemental-fraud-survey-sfs

appropriate supplement. [42] The core NCVS currently measures bias-motivated criminal victimization, however, further research was needed to determine how the survey might effectively measure these crimes if they occur online. As this research was testing cybercrime-related modifications to NCVS supplements, it provided an appropriate opportunity to assess the inclusion of bias-motivated cybercrime questions.

While bias-motived criminal victimization is asked through a series of questions on the core NCVS, this series was abbreviated to a single item to reduce the burden of the cognitive interviews. The question used in the interviews was:

> *The next question is about why the offender may have targeted you. The reason may have been prejudice or bigotry toward those with your characteristics or religious beliefs, even if the offender mistakenly thought you had those characteristics or beliefs. This kind of reason is different from just being angry or wanting to get something from you.*
>
> **Do you think the offender was targeting you because of prejudice or bigotry toward your race/ethnic background, your religion, your disability, your sexual orientation, your sex or any other of your personal characteristic?**
>
> Yes 01
> No 02

The main question of interest for the cognitive interviews was whether asking about bias-motivated crimes was feasible: Are victims of the different types of crimes able to report on these crimes? Are there certain types of crimes that are better suited to asking about bias-motivated crimes?

It was anticipated that the SVS would be the best fit because victims of stalking are likely to know the offender[43] and, perhaps, their motivation. Victims of fraud and identity theft are less likely to have this information available and make a determination on the motivation of the offense.

[42] Government Accountability Office (2024) Online Extremism: More Complete Information Needed about Hate Crimes that Occur on the Internet, U.S. Government Accountability Office, GAO-24-105553.

[43] Morgan, R.E. and Truman, J.L. (2022) Stalking Victimization, 2019. Bureau of Justice Statistics, NCJ 301735.

3. Methodology

The proposed questions were tested primarily using cognitive interviews, with some supplementation from questions that were asked as part of the web survey used to recruit the participants. This section describes the methods used to recruit the participants and the protocols to conduct and analyze the cognitive interviews.

3.1 Recruitment

The pool of recruits for the cognitive testing of the three cybercrime instruments came from a non-probability sample provided by the web survey vendor CloudResearch. Their web panel includes approximately 25 million members in the U.S. and is continuously updated. CloudResearch directed its panel members to Westat's web surveys and a little more than 10,000 survey responses for each of the three cybercrime surveys: stalking, identity theft, and fraud. The rationale for such a large sample was the projected rarity of cybercrime victims.

The web surveys were tailored to collect information on prior experiences for each of the three types of crime (Appendices A-C). The stalking screener replicated the questions on the SVS along with the proposed revisions for testing. The items included in the cognitive tests were those that involve telephone and other cyber-related methods. Follow-up questions were administered that asked about fear and victimizations that are used to define an individual as a stalking victim. In addition, the question on other emotional consequences was also asked. This survey also included testing alternative versions of various questions (see points 2, 5 and 7 for changes to be tested in section 2.1 above). The identity theft web survey administered the screening questions for each of the different types of thefts, incorporating the changes proposed for measuring cybercrime. The fraud survey included the screener questions on the current SFS. Follow-up questions were administered that asked how the victim first found out about the fraud and whether they provided the money using cryptocurrency. Each of the web surveys included a debriefing section, which asked a subset of respondents for feedback on different parts of the web survey.

The respondents recruited by CloudResearch who reported incidents to at least one of the screening questions were included in a pool for recruiting the cybercrime cognitive testing respondents. The goal for recruiting was to have a mix of victimization types, racial/ethnic backgrounds, ages and sexes. Table 3 provide details on the characteristics of the web survey respondents who formed the pool of potential recruits for the cognitive interviewing. Tables 4-6 provide information on the screening questions that were answered in the affirmative, along with the percent of respondents who reported 'yes' to at least one of the screeners for each cybercrime.

There were substantially more respondents reporting an experience with cybercrime than had been anticipated based on prior administrations of the SVS. For example, the most recent SVS found that approximately one percent of the adult population were classified as a stalking victim.[44] In contrast, approximately 78 percent of web respondents reported 'yes' to at least one of the screener items. Around 30 percent of web respondents met the definition of a stalking victim.

[44] Morgan, R.E. and Truman, J.L. (2022) Stalking Victimization, 2019. Bureau of Justice Statistics, NCJ 301735.

Upon talking to respondents during the cognitive interviews, it became apparent that these higher rates were due to respondents reporting telemarketing, spam and other issues that might qualify as harassment or annoyances of some type but are not considered illegal. For the stalking survey, a large percentage of the 'yes' responses were for unwanted phone calls, texts and emails. There were instructions to the questions to exclude these types of experiences, similar to the SVS. Some respondents may not have read these instructions, as can be common for a web survey. Even after accounting for solely those who reported the consequences to the victim that are used to define a stalking incident, there remained a very large percentage of individuals who met the stalking criteria (30%).

Table 3. Characteristics of the web survey respondents – percent			
	Stalking	Fraud	Identity theft
Sex			
Female	65.5%	62.7%	65.4%
Male	34.5%	37.3%	34.6%
Age			
Age 18-29	26.6%	13.6%	15.2%
Age 30-45	31.1%	26.3%	26.7%
Age 46-54	13.0%	13.3%	13.9%
Age 55-64	12.7%	15.7%	16.3%
Age 65-74	11.1%	20.7%	19.2%
Age 75+	5.4%	10.4%	8.7%
Race and ethnicity			
White	63.5%	72.2%	71.8%
Hispanic	6.5%	4.5%	4.7%
Black	18.1%	13.1%	13.8%
Asian	2.9%	2.9%	2.6%
American Indian or Alaska Native	0.8%	0.8%	0.6%
Middle Eastern or North African	0.2%	0.1%	0.2%
Native Hawaiian or Pacific Islander	0.2%	0.1%	0.1%
Multiple – Hispanic	4.8%	3.6%	3.5%
Multiple – non-Hispanic	2.9%	2.6%	2.6%
Education			
Some high school or less	5.7%	4.3%	4.6%
High school graduate	30.4%	23.4%	23.9%
Other post high school vocational training	4.3%	4.1%	3.9%
Some college	20.0%	19.9%	19.5%
Associate's degree	11.8%	12.6%	12.6%
Bachelor's degree	17.9%	22.0%	22.8%
Master's or professional degree	8.4%	11.7%	10.9%
Doctorate degree	1.4%	2.0%	1.8%
Census Region			
Midwest	21.1%	21.2%	21.1%
Northeast	17.4%	18.8%	18.1%
South	44.0%	40.1%	42.9%
West	17.5%	19.9%	17.9%
Total Number	**10,164**	**11,014**	**10,178**

Note: Sex, age and race/ethnicity were asked in the web survey. Education and Region were supplied by CloudResearch.

Table 4. Responses to the stalking web survey screening questions		
	Number of respondents answering 'Yes'	Percent of respondents
Unwanted phone calls [SQ_TELEPHONE]	6,417	63.5
Unwanted texts [SQ_TEXTMESSAGES]	5,778	57.2
Unwanted contact via email, dating apps, social media, or other online platforms [SQ_WEBSITES_1, SQ_WEBSITES]	5,846	60.3
Spied on (e.g., camera, listening device) [SQ_TECHNOLOGY_DIRECT]	1,523	15.1
Computer or phone monitoring [SQ_TECHNOLOGY_INDIRECT]	1,399	13.9
E-tracking device [SQ_APPLICATION]	2,621	25.9
Monitored on social media [SQ_SOCIALMEDIA, SQ_SOCIALMEDIA_1]	2,998	31.2
Posted intimate images (or threats) [SQ_IMAGE_BASED_SEXUAL_ABUSE]	966	9.6
Posted untrue and/or personal information (or threats) [SQ_POSTS, SQ_POSTS_1, SQ_POST_2]	1,563	16.1
Reported at least one type of incident	7,963	78.4

Note: Denominator for percents include valid responses only. Respondents could select more than one response. Text in brackets are the questions from the web survey used to generate the frequency.

Table 5. Responses to the fraud web survey screening questions		
	Number of respondents answering 'Yes'	Percent of respondents
Paid for a prize et al.	2,475	22.5
Tricked into paying for fake debt/taxes	1,192	10.9
Donated to a fake charity	1,414	12.9
Tricked into paying money to get a job/business op	1,104	10.1
Tricked into paying for false investment	1,214	11.0
Paid for products/services not received	2,350	21.4
Sent money to someone pretending to be family/friend	1,096	10.0
Reported at least one type of incident	3,971	36.1

Note: Denominator for percents include valid responses only. Respondents could select more than one response.

Table 6. Responses to the identity theft web survey questions		
	Number of respondents answering 'Yes'	Percent of respondents
Accessed checking/savings accounts	2,331	22.9
Accessed credit card	1,726	17.0
Accessed email/social media or created new account	1,672	16.4
Accessed other accounts	1,220	12.0
Created new accounts	922	9.1
Other fraud	782	7.7
Accessed personal information	1,211	11.9
Reported at least one type of incident	5,008	49.2

Note: Denominator for percents include valid responses only. Respondents could select more than one response.

There were a total of 75 individuals recruited for the cybercrime cognitive interviews, 25 for each of the three types of cybercrime. There was a wide distribution of respondents across age, race and ethnicity, education and census region (Table 7). For fraud and identity theft, the goal was to also have equal representation by sex. This goal was not included in the stalking recruiting because stalking victims are significantly more likely to be female than male[45]. The recruiting team was sent contact information for approximately 600 individuals (approximately 200 for each of the three groups).

[45] Morgan, R.E. and Truman, J.L. (2022) Stalking Victimization, 2019. Bureau of Justice Statistics, NCJ 301735.

Table 7. Characteristics of cognitive interview respondents by topic of interview				
	Stalking	Fraud	Identity theft	Bias-motivated crime
Sex				
Female	16	13	12	11
Male	9	12	13	8
Age				
Age 18-29	4	2	3	2
Age 30-45	5	6	6	3
Age 46-54	6	5	5	6
Age 55-64	6	8	6	4
Age 65-74	3	3	4	4
Age 75+	1	1	1	0
Race and ethnicity				
White	13	12	13	9
Hispanic	1	3	1	2
Black	6	7	8	7
Asian	1	1	2	0
American Indian or Alaska Native	0	2	0	0
Middle Eastern or North African	0	0	0	0
Native Hawaiian or Pacific Islander	0	0	0	0
Multiple – Hispanic	3	0	1	1
Multiple – non-Hispanic	0	0	0	0
Missing	1	0	0	0
Education				
Some high school or less	2	2	2	0
High school graduate	3	1	1	3
Other post high school vocational training	1	1	1	0
Some college	7	7	5	5
Associate's degree	4	4	6	3
Bachelor's degree	7	5	5	3
Master's or professional degree	3	5	4	4
Doctorate degree	4	0	1	0
Missing	0	0	0	1

	Stalking	Fraud	Identity theft	Bias-motivated crime
Census Region				
Midwest	7	7	6	5
Northeast	4	4	1	3
South	9	6	9	7
West	5	8	9	4
Total Number	**25**	**25**	**25**	**19**

The respondents for the bias-motivated crime interviews were recruited in a separate effort. The pool of potential recruits came from the existing cognitive testing respondents for the three cybercrime instruments. Thirty participants were selected to recontact. Of the 30, 19 agreed to be reinterviewed. Five were from the fraud interview, thirteen the stalking interview, and one originally participated in an identity theft interview. The demographic breakout is provided in Table 7.

3.2 Cognitive Interview Protocols and Analysis

The cognitive interview protocols are provided in Appendices D-G. A total of 6 experienced cognitive interviewers were trained on at least one of the protocols. One person was assigned to take the lead for each of the three crimes. Respondents were scheduled for a video-Zoom interview by a recruiting team who confirmed the conditions of the study and set up appointment times.

Respondents for the bias-motivated crime interviews were first reminded of the incidents they reported during the cybercrime interview. They were then asked the bias-motivated crime question and follow-up probes.

The analysis was conducted in two steps. First, each interviewer filled out a template that provided the details of how respondents answered the questions and the probing. Once these were compiled, an analyst summarized the results for each of the relevant questions (Appendix H). A senior analyst then summarized the main points for each of the surveys.

4. Results

The cognitive testing results are summarized below for each of the different crimes. They are organized by each of the questionnaire items that were added or modified to collect data on cybercrimes (see Section 2 above). The results below repeat the targeted item(s). In a few cases, the original item is repeated for clarity. **The revision to the item is highlighted in blue. Items that are brand new are highlighted in all blue.** Observations from the interviews are then provided, along with recommendations based on the results.

4.1 Stalking

1. *Split questions on phone calls/voice messages and text messages*

The original question was:

> *Now I want to ask about unwanted contacts or behaviors using various technologies, such as your phone, the Internet, or social media apps. Again, please DO NOT include bill collectors, solicitors, or other salespeople.*

SQ1g. **Has anyone made unwanted phone calls to you, left voice messages, sent text messages, or used the phone excessively to contact you?**

Yes 01
No 02

For this test, the question was split to separately measure phone calls and voice messages from text messages. The latter is most clearly a cybercrime, while the former is more ambiguous across legislation in different states.

SQ_TELEPHONE

SQ1g. **Has anyone made unwanted phone calls or left voice messages excessively to contact you?**

Yes 01
No 02

Yes	14
No	11

- Respondents did concentrate on telephone calls or voice mail messages. They did not seem to confuse this with other types of messages (e.g., text, email).
- 'Excessive' was interpreted in different ways. Some defined it as more than what was expected, while others gave a quantitative answer (4 or 5).
- About half of the 'yes' responses were for ex-partners or unrequited interest.
- A number of the 'yes' responses were for spam, telemarketing, robocalls or attempts at ID theft.

Recommendation: With respect to focusing on phone calls, the question worked as intended.

A significant number of respondents reported telemarketing, robocalls, etc. even though the introduction instructs to exclude these. This issue was apparent in prior administrations of the SVS and were screened out when asked the questions on the consequences defining stalking. However, it would be more efficient to screen these out at this point, rather than later. Note, the issue of respondents reporting contacts like spam or robocalls. is not a function of the revised wording, since the cognitive interviews included the same introduction as on the actual supplement to exclude these types of incidents. Additional wording to exclude these calls should be considered. For example, using words like 'spam' or 'phishing' may bring these types of incidents out more readily. Consider including the exclusionary condition as part of the question:

"Excluding calls from bill collectors, solicitors, spam or robocalls, …."

BJS should also review prior administrations to see if this was an issue on the survey and how it was handled.

SQ_TEXTMESSAGES

SQ1g1. Has anyone sent excessive unwanted text messages to contact you?

Yes 01
No 02

Yes	13
No	12

- Interpretation of excessive was similar to SQ1g.
- One 'yes' respondent reported a Facebook message, rather than one sent SMS.
- Same issues with inclusion of spam, telemarketing as noted in SQ1g.

Recommendation: Most people understood what text messages meant, but there was one person who confused it with a Facebook message. Consider using 'SMS text messages' or 'Text messages on your phone'.

2. *Update the question on unwanted emails or messages*

The current question is:

SQ1k. Has anyone sent you unwanted messages using e-mail or messages using the Internet, for example, using social media apps or websites like Instagram, Twitter, or Facebook?

Yes 01
No 02

Alternative questions were proposed to replace this. Updated examples were used in both alternatives. One alternative listed several examples and used 'other internet platforms and applications' as a summary of other relevant methods. The second option listed out more specific examples.

SQ_WEBSITES

SQ1h. **Has anyone sent you unwanted messages using email, social media apps, dating apps or other internet platforms and applications?**

Yes 01
No 02

Yes	8
No	4

SQ_WEBSITES_1

SQ1h1. **Has anyone sent you unwanted messages using email, social media apps, or other internet applications like WhatsApp, SnapChat, Instagram, Twitter (X), YouTube, Facebook or TikTok?**

Yes 01
No 02

Yes	7
No	5

- Respondents interpreted 'unwanted messages' as something they had communicated to stop and it didn't.
- Respondents correctly interpreted 'dating apps'.
- Most respondents to the first version were able to give relevant examples of 'other internet platforms and applications' (e.g., Facebook, Instagram, TikTok). Very few of the respondents to the second version could come up with other examples.

These two questions were also administered as part of the web survey used to recruit respondents for the cognitive interviews. A random half of the sample was administered the first question, and the other random half was administered the second question. Significantly more respondents reported an unwanted message for the first question, which did not list out as many examples as the alternative version (54.5% vs. 50.5%; $p<.0001$).

Recommendation: The first question that used dating apps or other internet platforms was understood by respondents. Virtually all of the respondents to the first version provided examples that were included in the second version. Furthermore, the results from the web survey indicated more respondents said 'yes' to the first version of the survey. It is notable that the first version includes 'dating apps' in the question, while the second version does not. This may be why the first version had more respondents saying 'yes'. The cognitive interview results seemed to suggest that 'other internet platforms and applications' did a good job summarizing the relevant applications.

For these reasons, it is recommended the first version be used. It is shorter and may not need to be updated as new applications emerge in the future.

3. *Can the question on monitoring activities be broken up into direct and indirect monitoring methods?*

The current question is:

h. Has anyone spied on you or monitored your activities using technologies such as a listening device, camera, or computer or cell phone monitoring software?

The revised questions are:

SQ_TECHNOLOGY_DIRECT

SQ1i. Has anyone spied on you using technologies such as a listening device, camera, or video recorder?

Yes 01
No 02

Yes	6
No	17
Don't Know	2

SQ_TECHNOLOGY_INDIRECT

SQ1i1. Has anyone spied on you using computer or cell phone monitoring software?

Yes 01
No 02

Yes	2
No	20
Don't Know	3

Results for SQ_TECHNOLOGY_DIRECT:

- Respondents generally understood the types of devices being asked about. One exception was a single respondent who thought the question was asking about hidden devices.
- Respondents generally understood what 'spying' meant, giving examples that fit within the definition.
- Respondents that said 'yes' to this question had varying levels of knowledge on how they knew about the surveillance.
  - One mentioned being recorded by Facebook. Another believed their phone was tapped but couldn't provide any information of how they knew (this respondent reported a number of unlikely events). Another reported being tapped because they heard beeping sounds on the line.
  - Several said they were aware of being recorded by boyfriends and landlords.

Results for SQ_TECHNOLOGY_INDIRECT:

- Respondents generally understood what computer or cell phone monitoring software meant.
- Respondents were asked to compare this to the prior question. Many had a hard time understanding this probe. Of the several that did make the comparison, they generally described this question as spying with software through the computer or cell phone.

Recommendation: The primary question was whether it was possible to break up the question to get more specific information on the type of spying. From a comprehension point of view, respondents generally understood the specific type of spying that each question was asking about. Based on this, it is recommended that the proposed questions be adopted. On a separate note, there are likely to be some false positives for this question because of respondent's suspicions (or even paranoia) that are not grounded in direct knowledge.

4. *Should 'e-tracker' be added to the question about electronic tracking?*

The revised question is:

SQ1j. **Has anyone tracked your whereabouts with an electronic tracking device or application, such as GPS, an e-tracker, or an application on your cell phone?**

Yes 01
No 02

Yes	5
No	20

- Several respondents reported being tracked with their consent. One of these individuals answered 'yes' to the question.
- A number of respondents did not know what an e-tracker was.
- Others did not know but took an educated guess that it had something to do with being able to keep track of a person.
  - "I don't really have an answer for that, because I would assume it might be something like a sim that you could use to test another phone service provider. And that would imply. maybe software. But that one's not clear to me at all, I would not know."
- Several respondents said that they would not necessarily know if they had been tracked.

Recommendation: The addition of this term did not seem to add to the meaning of the question for most respondents. Many respondents could not define what it was, but inferred it had something to do with tracking them. Based on this, we recommend not adding 'e-tracker' to the question. It may confuse some respondents and since it doesn't seem to add meaning to the question, it doesn't seem necessary.

Several respondents reported that they were tracked willingly, with at least one person answering 'yes' to this question. The introduction to this section does instruct to only include unwanted incidents. But this may get lost after the first few questions in this section are asked. BJS should assess whether this was an issue in the last administration of the survey. If so, it should consider adding a phrase such as:

"Has anyone tracked your whereabouts, without your permission…"

This change may help to avoid possible false positives related to willingly being tracked.

5. *How should the question on monitoring activities with social media apps be changed?*

The testing asked about two alternative versions of the question:

SQ_SOCIALMEDIA

SQ1k. **Has anyone monitored or observed your activities on social media apps like Facebook, TikTok, YouTube, Instagram, Twitter (X), or LinkedIn?**

Yes 01
No 02

Yes	8
No	4

SQ_SOCIALMEDIA_1

SQ1k1. **Has anyone monitored or observed your activities on social media apps, discussion forums, or other social networking platforms or apps?**

Yes 01
No 02

Yes	5
No	8

- Most respondents understood what 'monitoring or observed your activities' meant.
- Most respondents understood what 'social media apps' meant. They generally gave examples that were part of the first alternative (SQ1k).
- Some respondents interpreted the question of being monitored by a third party but not in a nefarious way. For example, other family members, friends or companies that track for business reasons (e.g., marketing particular products).

These two questions were also administered as part of the web survey used to recruit respondents for the cognitive interviews. A random half of the sample was administered the first question and the other random half was administered the second question. Significantly more respondents reported being monitored to the first question (SQ1k) than the second question (SQ1k1) (28.4% vs. 24.1%; p<.0001).

Recommendation: The question with examples is recommended. The examples covered most of those that respondents reported when asked the more general question (SQ1k1) and there were more individuals reporting 'yes' to the question with examples in both the web survey and the cognitive interviews. Based on this, the examples seem to be providing additional memory cues that the general question does not.

This question also had several respondents report being followed but in a friendly or non-nefarious way. This issue is not due to any changes that were tested as part of the current testing. BJS should assess whether this was an issue in the last administration of the survey. If so, it should consider modifying the question by adding a qualifying phrase like:

> *"Please do not include monitoring by people who you want to stay in touch with or companies that would like to sell you something."*

However, since following someone on social media is done by a wide variety of entities, such as family, friends, or companies and permission is not always required, it isn't clear what phrase would capture the appropriate universe. It may be best to capture these in the follow-up questions that ultimately classify the incident as stalking.

6. *Add a question on posting sexually explicit images or videos*

The new question tested was:

SQ_IMAGE_BASED_SEXUAL_ABUSE

SQ1X. Has anyone posted nude, intimate, or sexually explicit images or videos of you on the internet without your consent or threatened to post this content on the internet?

Yes 01
No 02

Yes	1
No	24

- Respondents understood this question.
- The one respondent who said 'yes' described a relevant incident:
  - "It was like an escort site, and I wasn't on it. He posted it, I guess, to see who would respond and who would give him money, pretending to be me once again, using my pictures and stuff."

Recommendation: Adopt this question as worded.

7. *Revise current question on others posting respondent's information to be more specific to posting non-image related personal information.*

Two alternatives were tested. The first revised the wording as noted below:

SQ_POSTS

SQ1I. **Has anyone posted or threatened to post inappropriate, unwanted, indecent, or personal information about you on the Internet including your name, address, email, spreading rumors or other information about you?**

Yes 01
No 02

Yes	4
No	8

The second broke up the question into two. One asking about inappropriate information, while the other was on personal information such as name, address or other details.

SQ_POSTS_1

SQ1I1. **Has anyone posted or threatened to post inappropriate, unwanted, indecent, or untrue information about you on the Internet?**

Yes 01
No 02

Yes	4
No	9

SQ_POSTS_2

SQ1I2. **Has anyone posted or threatened to post your personal information, including name, address, email, or other details about you on the Internet?**

Yes 01
No 02

Yes	3
No	10

Yes to either SQ1I1 or SQ1I2	3
Yes to both SQ1I1 and SQ1I2	2
No to both SQ1I1 and SQ1I2	8

- People generally had reasonable definition of 'inappropriate, unwanted, indecent or personal information':
  - "Anything that's derogatory or threatening."
  - "Telling you lies about yourself, what you what you do, and then maybe showing places your body in areas that you don't approve like you know what I said."
- There were mixed interpretations of the first, combined, question. Of the four who said 'yes', only one seemed to definitively meet the intention of the question:
  - "I've had my ex-husband post on social media, my name, my date of birth, my social security number, my checking account number, my balance of the account, the withdrawals."
- One of the four 'yes' responses seemed to be a case of identity theft, another was a scam.
- When answering the two alternative questions (SQ1I1, SQ1I2), respondents seemed to get the distinction. They did not say anything about potential redundancies. Of the five people who answered 'yes' to at least one of these questions, the types of incidents reported were consistent with the intent of the question (slanderous material for SQ1I1 and personal information for SQ1I2).

These two questions were also administered as part of the web survey used to recruit respondents for the cognitive interviews. A random half of the sample was administered the first question, and the other random half was administered the other two questions. Significantly more respondents reported unwanted posts across the two alternative questions (SQ1I1 and SQ1I2) than for the single question (SQ1I) (15.7% vs. 11.7%; p<.0001).

Recommendation: Use the two, more detailed, questions (SQ1I1, SQ1I2). Respondents understood the difference between the two. Separating personal information from inappropriate or untrue information is more straightforward than in a single question. This version also produced the most reports of unwanted posts on both the cognitive interviews and the web survey.

8. *Add a question that asks about reactions to the incident for those that report multiple incidents but do not meet the formal stalking definition.*

SQ_OTHERREACTIONS

How did you feel when any of these unwanted contacts or behaviors occurred? (MARK ALL THAT APPLY)

Alarmed 01
Intimidated 02
Harassed 03
Seriously annoyed 04
None of the above 05

Alarmed	12
Intimidated	7
Harassed	17
Seriously annoyed	14
None of the above	1

As noted above, this question would be asked of those individuals who experienced more than one incident but did not express the consequences of the incident that make up the definition of stalking. However, for purposes of the cognitive interviews, all respondents who reported at least one incident were asked this question. This plan maximized the number of people who could provide feedback for this question.

- Many respondents selected more than one response. The most serious, judging by respondent comments on the type of feelings and how long they lasted, selected the categories of 'alarmed' and 'intimidated'. Examples of respondent comments include:
  - "I'm still fighting it to this day, like you might hear me get a little shaky. You might hear me stutter a little bit like. PTSD is no joke."
  - "I'm scared. I mean, I guess you could say annoyed, but that was like low on the list of my feelings."
  - "It did a little bit not for a long time. I kind of cried and got upset because I had started, you know, to really feel that this was somebody that I could, you know, possibly have a relationship down the way"
- All of those reporting serious consequences (i.e., alarmed and/or intimidated) also reported experiencing fear or distress in the prior questions. Under the definition used in the SVS, they would have skipped this question (see note above).
- There were a number of people who selected 'harassed' and 'seriously annoyed' that did not express significant consequences. These were primarily individuals who reported telemarketing and spam incidents.
- A few respondents suggested adding to the list 'fear' and 'anger'.

Recommendation: All respondents, except one, selected at least one of the emotions for this question. There were clearly respondents who did express serious consequences. The best indicator of this was the selection of 'alarmed' and, to a lesser extent, 'intimidated'. As noted above, all of these individuals would have qualified as a stalking victim because they said 'yes' to the prior fear and distress question. On the one hand, this is evidence that the 'alarmed' and 'intimidated' categories are candidates for defining respondents as harassment victims. The other two adjectives 'harassed', and 'seriously annoyed' seemed to apply to incidents that were bothersome, but did not rise to the level of illegal behavior.

It is not recommended to adopt this question to define harassment. The sample may not have been diverse enough to distinguish between stalking victims and those who were harassed in ways that could be considered illegal. Several respondents were victims of telemarketing and spam. Presumably these would be screened out as part of the SVS. Their reactions to the adjectives on the list may not reflect how a sample of victims of incidents that are not spam or telemarketing would react. It is recommended that further testing of this question be conducted, perhaps in conjunction with the next SVS. As part of the test, summaries of the incidents should be collected and used to assess whether the scale is able to identify victims of harassment that rise to the level of being illegal.

4.2 Identity Theft

1. *Add a question on whether the theft occurred when someone used cyber methods to use the person's identity.*

For five different types of identity theft, a new question was asked on how the offender used the stolen information. This question was asked for ID theft related to: checking/savings accounts (P1), credit card accounts (P3), telephone/utility/medical insurance accounts (P6), opening checking or other accounts (P8), and misuse of personal information (P10). The example from P1 shows the revised wording for the questions:

P1. For the incidents occurring in the last 12 months, how did someone use your checking or savings account or to do other things?

It was done online 01
It was done in some other way (e.g., in-person, over the telephone, by mail, something else) 02
Both 03

Results were compiled across all five questions that were asked of the respondent. Respondents got to this question if they said they had experienced the particular type of identity theft at the screening question.

Online	8
Other	1
Both	3

- Most respondents understood this question as asking how the personal information was used. However, there were a few respondents who reported how the personal information was obtained, rather than used. In one instance, the respondent used the 'both' response category to report how it was used and how it was obtained.
- When asked about what 'in some other way' meant, respondents gave examples of non-cyber transactions (telemarketers, in-person transactions).
- Most respondents knew how the information was used. In a number of cases, the respondent got the information from statements they received from their vendors or transaction history. However, there were a few (3) that were taking educated guesses. One respondent said they did not know.

Recommendation: Respondents did understand the distinction between online and other methods. On the other hand, there was some confusion among a few respondents between the medium by which the account was used and how the information was obtained (see details below). It is recommended to keep this question, as worded. It might work better if it is asked after the question on how the information was obtained, which may be more salient to the respondent.

2. *Add additional options to the current question asking how the information was obtained.*

The ITS currently has a question that asks how the personal information was obtained. It includes some options related to cyber sources. This was expanded to include more cyber-enabled options. This question was asked across six of the different types of ID theft: checking/savings accounts (P2), credit card accounts (P4), social media accounts (P5), telephone/utility/medical insurance

accounts (P7), opening checking or other accounts (P9), and misuse of personal information (P11). The example from P2 shows the revised wording for the questions:

P2. **How do you think your personal information was obtained to access your checking or savings account?**
(MARK ALL THAT APPLY)

I lost an item that included my personal information 01
My wallet, checkbook, or purse was stolen 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash 03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader 06
I responded to a scam email or clicked on a link in the email 07
I responded to a scam phone call 08
I responded to a scam text message or clicked on a link in the message 09
I responded to a social media post 10
My personal information was stolen from my personnel or Human resources electronic records at my place of employment 11
My electronic records containing personal information were stolen from a company or other organization 12
Obtained in another way (specify)_____ 13

A total of 14 people answered this question across all types of identity theft.

- All respondents understood the question to be asking how the personal information was obtained.
- There were a significant number of respondents who were either not sure or did not know how the information was obtained (10 out of 14 respondents). The extent of certainty varied across respondents, with most basing on some suspicions of how the breach might have been possible.
- Interpretation of 'I responded to a scam email or clicked on a link in the email' had a few respondents (2 out of 8) who confused text messages with email.
- Respondents understood the option 'I responded to a scam text message or clicked on a link in the message'.
- Respondents understood the category 'I responded to a social media post'. There was one exception where the respondent was not sure what that meant because they did not use social media.
- Respondents all understood 'My personal information was stolen from my personnel or human resources electronic records at my place of employment'. They interpreted it as data breaches as well as individuals stealing information from HR/payroll.
- Respondents all understood 'My electronic records containing personal information were stolen from a company or other organization'.

Recommendation: This question generally worked as intended. Respondents understood it was asking for how the information was obtained, rather than used. They also seemed to understand the enhanced response options and the distinctions that were made. The one exception to this was some confusion between email and text messages. The response option related to emails had a few respondents who interpreted this as including text messages. One possible fix to this is to add a probe to the email response (when selected) to verify that it is email and not text. The second issue is that many of the respondents were not entirely confident that they knew how their information was obtained. Many took educated guesses. This is consistent with the last administration of the ITS, which had a high rate of missing data. The ITS currently screens these out by first asking if the respondent knows how their information was obtained. This practice should continue with the revised question.

3. Supplement the question on having cyber accounts with additional examples.

The revised question added YouTube, Reddit or Pinterest as additional examples.

Q9a. **Have you ever had at least one email account, such as Gmail or Outlook, or social media account such as Facebook, Instagram, YouTube, Reddit or Pinterest?**

Yes 01
No 02

Yes	23
No	2

- For several (5) of the respondents there was confusion that this question was asking if someone had misused their account, not just whether they have had an account.
- Most respondents interpreted 'social media accounts' to be online platforms where someone can connect and interact with other people. Examples provided were Facebook, WhatsApp, TikTok, Twitter/X and Instagram.
- About three-quarters of the respondents thought the added examples (YouTube, Reddit, Pinterest) were social media, although some thought they are used differently (less interaction) than other types of social media (e.g., YouTube, Pinterest). Four respondents did not think YouTube was social media, three Pinterest and one Reddit.
- Among the new examples, YouTube was the most widely recognized application, followed by Pinterest and Reddit.

Recommendation: The first issue of respondents not understanding the question is partly a function of the probing in the cognitive interviews with some respondents losing the flow of the conversation. But it also may be the transition just before the question, which states "The next questions focus on the possible misuse of your existing email or social media accounts". Some respondents were expecting a question about misuse of accounts. We suspect this may have also been a problem in the current survey. Adding to the transition might help:

"…But first I want to find out if you have any email or social media accounts".

Respondents generally interpreted social media as accounts that involve interactions with other people. While most respondents thought the new examples were social media accounts, some viewed them a bit differently. For this reason, it is recommended that the examples be included in the question. It seems to expand the definition of social media beyond what some respondents may think of.

4. *Add a question on whether anyone has ever created fake email or social media account using the respondent's identity.*

Q9bb. Has anyone EVER created an email or social media account for you without your permission to pretend to be you?

Yes 01
No 02

Yes	8
No	16

- Several of the 'yes' responses were misuse of existing accounts. For example, one respondent described where someone hacked into their account and took it over. Another described both creating a new account and using an existing account.
- The remaining 'yes' responses said they found out because family and/or friends alerted them to the fake account.
- A number of respondents (8) said they did not know for sure if anyone created an account pretending to be them.

Recommendation: This question seemed to work as intended and it is recommended to adopt the current wording. However, two out of eight respondents falsely reported misuse of an existing

account. They may have confused impersonating when using an existing account versus impersonating with a new account. The prior question does ask about impersonating with an existing account. One possible way to check answers is to probe when a respondent answer's 'yes' to this second question to verify that someone impersonated them using a new account.

5. *Add examples to question asking about using existing telephone, utility, or other accounts.*

Q11. **Has anyone EVER used any of your other existing accounts, without your permission, such as…**

- Telephone account such as for cell phone or landline telephone;
- Internet account such as for internet or wireless Wi-Fi;
- Utilities accounts, such as cable, gas, or electric;
- Medical insurance accounts, such as Medicare or a health spending account;
- Entertainment accounts, such as for music, movies, or games;
- Online payment accounts, such as PayPal or Venmo; or
- Some other type of accounts?

Only include times when someone successfully posted charges to, took money from, or otherwise misused your account.

Yes 01
No 02

Yes	13
No	12

- Two of the 13 'yes' responses were not in scope. One described an incident with their social media account. One described her personal information being stolen from hospital records, but no theft occurred as a result of stealing that information.
- Several others described incidents that did not qualify, but also described incidents that did qualify.

Recommendation: The changes to this question were minor. At least one of the incidents reported included the victim's cell phone (e.g., spoofing their number), which is consistent with the examples added to the list. There may be some confusion by respondents on what should be included in this question. One respondent thought of misuse of a social media account and the other reported stealing their personal information, but no subsequent use of that theft to impersonate them. The ITS questionnaire has several instructions on what should be included (e.g., *"…aside from your bank, credit card, email or social media accounts*"). There are also several follow-up questions that ask for the specific type of account that was misused. If the account is not in scope, these should catch the mistake. If further verification is desired, consider asking for a summary of the most recent incidents.

6. *Add additional examples for follow-up questions to Q11.*

Q13a. **Telephone accounts such as cell phones or landline?**

Yes 01
No 02

Yes	2
No	3

- The two 'yes' responses fell within scope of the question. One was using the phone number to make spam calls to other people. The other was an ex-partner cutting off their service.

Q13aa. **Internet accounts such as wireless or Wi-Fi?**

Yes 01
No 02

Yes	0
No	5

- Respondents did not report any of these types of incidents.

Recommendation: These responses were consistent with the types of incidents the respondents reported in the initial question. The splitting of the question into two categories should be adopted.

7. *Add examples to question asking about using personal information open new accounts.*

Q15. **Has anyone EVER, without your permission, used your personal information to successfully open any NEW accounts, such as…**

- Checking or savings accounts;
- Credit card accounts;
- Email accounts, such as Gmail or Outlook;
- Social media accounts, such as Facebook, Instagram, YouTube, Reddit or Pinterest;
- Telephone or
- Internet accounts;
- Utilities accounts, such as cable, gas, or electric;
- Entertainment accounts, such as for music, movies, or games;
- Loans or mortgages;
- Insurance policies;
- Online payment accounts, such as PayPal or Venmo; or
- Some other type of new account?

Please include times when someone successfully opened a new account, even if you did not lose any money or were reimbursed later.

Yes 01
No 02

Yes	7
No	18

- Most respondents who said 'yes' to this question reported in-scope events. These included opening utility accounts, telephone accounts, checking accounts, internet accounts, a health insurance policy and a Facebook account.
- There were several people who reported changes to existing accounts, including opening new phone lines to an existing account.
- Those who said 'no' generally understood this was asking about opening new accounts, with two exceptions.

Recommendation: Respondents generally understood this question and it is recommended to adopt with the expanded examples. As with Q11, some respondents may include other types of identity theft that involve existing accounts. Asking for a summary would allow some check on this.

8. *Add a question at the end of the survey asking whether anyone obtained personal information, regardless if it was ever used.*

P12. **I've asked you about different ways someone may have used your personal information. This next question concerns whether someone ever obtained your personal information using any of the following methods.**
(MARK ALL THAT APPLY)

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 01
It was stolen during an online purchase/transaction 02
Someone stole it during an in-person purchase/transaction, including using a skimmer card 03
I responded to a scam email or clicked on a link in the email 04
I responded to a scam phone call 05
I responded to a scam text message or clicked on a link in the message 06
I responded to a social media post 07
My personal information was stolen from my personnel or Human resources electronic records at my place of employment 08
My electronic records containing personal information were stolen from a company or other organization 09
None of the above 10

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device	0
It was stolen during an online purchase/transaction	1
Someone stole it during an in-person purchase/transaction, including using a skimmer card	2
I responded to a scam email or clicked on a link in the email	1
I responded to a scam phone call	0
I responded to a scam text message or clicked on a link in the message	1
I responded to a social media post	1
My personal information was stolen from my personnel or human resources electronic records at my place of employment	0
My electronic records containing personal information were stolen from a company or other organization	2
None of the above	2

A total of 10 people answered this question. The intent was to ask this of those who did not report any type of cyber theft in the prior questions. But some who reported prior identity theft incidents were mistakenly asked this question.

- Most (7) of the respondents reported in the appropriate category.
- A few did confuse the different categories. One respondent reported an incident in option 3 ('Someone stole something during an in-person purchase/transaction, including using a skimmer card') but it actually belonged in option 6 ('I responded to a scam text message or clicked on a link in the message'). The respondent seemed confused about several different incidents that occurred around the same time 15 years ago. Another respondent reported a data breach at her doctor's office, but selected it being accessed electronically from work or home.

Recommendation: While a few respondents had some difficulty finding the appropriate category, the question worked well overall and it recommended for adoption in the survey. Some consideration should be given to asking the question for a 12-month reference period, rather than asking about lifetime and then following up with the past 12 months. These types of incidents are relatively common and recall for a lifetime reference period is burdensome.

9. *Add a follow-up question to P12 asking if the incident occurred within the past 12 months.*

P13. Has this happened during the past 12 months, that is from [AUOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

Yes 01
No 02

Yes	3
No	5

- Respondents did seem to be able to date when the events took place. They used their own records, landmark events and their memory to date events within the last 12 months.

- *"Anybody that call or text me, it's on here. I don't care if it's over 2 years ago. It's saved in my phone – Not only that I take screenshots and print them out. And I keep records. One thing with my training and my professional background—we are taught to keep a paper trail."*
- *"I mean, it's recent in my memory, so I'm sure it's in the last year."*
- *"Because it was [this past] Christmas."*

- Those saying 'no' referred to events as happening 'years ago' or a long time ago.

Recommendation: Adopt as worded. No changes recommended for this question.

4.3 Fraud

1. *For each type of fraud with a question on how victim first found out about the fraud.*

To assess whether the fraud was initiated through a cyber or non-cyber-enabled source, a follow-up question addressing how the respondent first found out about the fraud was added for all seven types of fraud. The question was preceded by an item asking if the respondent had ever experienced the specific type of fraud. Question language for six of the types of fraud were replicative: prize or grant fraud (P1), phantom debt (P2), charity fraud (P3), employment fraud (P4), consumer Investment fraud (P5), and consumer products or services fraud (P6). The example from P2 shows this wording:

P2. How did you first find out about the money or prize?

Someone told me on a phone call 01
A text message 02
The TV, radio or a newspaper 03
Social media such as Facebook, TikTok, Instagram, or LinkedIn..... 04
Website 05
Chat application, such as WhatsApp, Telegram or Signal..... 06
Someone told me in-person..... 07
From an email I received..... 08
From material I received in the mail or delivery to my home or business 09
Some other way (Specify: _____)..... 10

Someone told me on a phone call	3
A text message	0
The TV, radio or a newspaper	1
Social media	8
Website	5
Chat application, such as WhatsApp, Telegram or Signal	2
Someone told me in-person	9
From an email I received	10
From material I received in the mail or delivery to my home or business	0
Some other way (Specify: _____)	2

A total of 40 respondents answered these questions. One additional type of fraud, relationship or trust fraud, had a similar, but slightly different follow-up question (S7B3) on how the respondent first found out about the offer. See objective 2: "*For relationship or trust fraud, ask a question on how the respondent was first contacted*", below.

There was some misinterpretation of the initial screening items. For example, when asked about paying for products that were never re-imbursed (consumer investment fraud), the respondent reported a loan to a friend that was never paid back. Another reported clicking on an advertisement to receive pet treats and never receiving anything, even though no money was exchanged (consumer products or services fraud).

- The response categories generally worked as intended. Most (about 30 of 40) responses selected the appropriate response categories.
    - *(in person) "A business associate from… work… had a startup opportunity and was soliciting angel investor funds for the startup… I gave him a little bit of money, kind of risk versus reward, if you will. And then I found out that there was nothing behind the start up."*
    - *(email) "Email that followed closely on a purchase from a brick-and-mortar business. and an email from the same business showed up. It turned out to be a scam. It looked very real."*
- One source of confusion stemmed from how to classify events that occurred in several stages. Examples included: receiving a link in an email; seeing a product on social media that directed viewers to a website; and a friend directing them to a website.
- A few respondents reported the how they found out it was a scam, rather than how they first found out about the request to participate in the scam.
- Several people reported hearing about the scam over a Zoom call. They didn't feel there was a place to put that.
- Respondents were asked what their interpretation of 'social media' was on the list. There was a general understanding, although the specific responses differed to some degree. Many named specific sites, such as Myspace, Facebook, TikTok, Twitter/X, LinkedIn, Instagram, YouTube, Instagram and Snapchat. Some characterized it as a place where people can meet.
- Respondents had a harder time distinguishing 'social media' from other internet applications (such as 'websites'). About half distinguished it from 'websites' as being more interactive and not focused on a particular topic or product. Others focused more on who ran the site (e.g., company vs. individuals) and more interactive.
- When asked what a 'chat application' was, many respondents named specific applications, such as WhatsApp, Gemini, ChatGPT and Facebook Messenger (among others). It was described by a number of people as an app where people (or AI) have direct conversations.

Recommendation: The question generally worked. There were a few people who confused how they were first approached about the scam and how they found out it was a scam. Since this only happened twice (out of 40 answers), it is not clear the question needs changing. Interviewers could be given the option to probe with:

"Is this where you first heard about the (FILL WITH TYPE OF FRAUD)?"

A larger issue is how to report a series of communications that lead to the fraud. For example, a few respondents were not clear how to report a series of communications that led to learning about the transaction (e.g., a friend pointed the victim to a website). Theoretically, any transaction that involved a cyber method should be included in the count of a cyber fraud. On the other hand, it is difficult to fully enumerate a chain of communications on a structured questionnaire.

One possibility is to allow respondents to select more than one response, and the answer can be coded appropriately. However, this may lead to complicating the question for respondents, who may think of all possible methods used in the transaction and possibly confuse how it occurred and how they found out. If this option is taken, then further pre-testing will be needed to assess this change. Another possibility is to take the first communication as the answer. In this case, we recommend altering the question to further emphasize the word 'first' in the question (e.g., all caps) and take the first contact as determining the classification as a cybercrime. The cyber-related question on the ITS takes this approach. While this may miss some crimes that have a cyber component, it is the simplest one to implement on the survey.

A third issue that was brought up was how to handle initial communications that used Zoom or other video software. We assume this type of communication is similar to telephone communications, rather than one using the internet or other cyber methods. But this should be investigated further by reviewing legal and conceptual definitions of cybercrime. If it is considered more like a telephone call, it is recommended to add this to the telephone category:

"Someone told me on a phone or video call"

Combining it into the telephone category also does not lengthen to the list, which is already very long.

2. *For relationship or trust fraud, modify the question on how the respondent was first contacted.*

S7B3. **Which ONE of the following BEST DESCRIBES how you were first contacted by this person?**

Through a chat application such as WhatsApp, Telegram, or Signal 01
Through a dating app 02
Through social media such as Facebook, TikTok, Instagram, or LinkedIn 03
Through a website 04
In an email 05
By a text message 06
By a phone call, or 07
Some other way (Specify: _____) 08

- One respondent reported being a victim of this type of fraud. They responded that they were initially contacted by email. The email asked for money for what appeared to be the nonprofit hospice provider for the respondent's mother. The money actually went to another organization.

Recommendation: Adopt this question but ensure the changes are consistent with the previously discussed question asked for the other six types of fraud. Add video call to the option for phone calls. Emphasize 'first' with capital letters in the question stem.

3. *Add a question on Cryptocurrency*

For all seven types of fraud, a question was added to the questionnaire about whether the respondent provided the money with cryptocurrency (S1B31, S2B21, S3B21, S3B31, S4B41, S5B21, S6B61, S7b41).

Did you provide the money using cryptocurrency?

Yes 01
No 02

Yes	2
No	21

- Across the types of fraud, two respondents reported providing the money using cryptocurrency. The two 'yes' responses described different features of using cryptocurrency, including the ability to see all transactions and transmitting a digital form of money.
- Of the respondents who did not use cryptocurrency, six had heard of it, but could not describe it in any detail:
  - *"For the wealthy."*
  - *"A trendy way to manage money."*
  - *"I think a fake money, but I mean, I guess people can use it."*

- Others who did not use it described it as some form of digital currency or specified particular types:
  - *"To me, it's electronic value, it's difficult to measure."*
  - *"Digital money that I'm afraid of."*
  - *"It's another form of cash, but it's different … Bitcoin."*
  - *"It's usually a numerical value placed on a blockchain algorithm that it's not physical currency. It's a digital type of currency."*

Recommendation: Adopt the question as worded. While there were many that could not define what cryptocurrency is, almost everyone had heard of it. Those that do not understand it are not likely to say 'yes' to the question. Those who did use it, are likely to know what it is. The latter is supported by the two people who reported using it.

4.4 Bias-Motivated Crime

The bias-motivated crime question was administered as a follow-up interview for 19 respondents who previously completed the interviews on cybercrime. The bias-motivated crime question was adapted from the core NCVS questionnaire. The question administered for the cognitive interviews was:

> *The next question is about why the offender may have targeted you. The reason may have been prejudice or bigotry toward those with your characteristics or religious beliefs, even if the offender mistakenly thought you had those characteristics or beliefs. This kind of reason is different from just being angry or wanting to get something from you.*
>
> **Do you think the offender was targeting you because of prejudice or bigotry toward your race/ethnic background, your religion, your disability, your sexual orientation, your sex or any other of your personal characteristic?**
>
> Yes 01
> No 02

Yes	7
No	12

- Of the seven who answered 'yes' to the question, three described incidents that fit the definition of a bias-motivated crime as indicated by the respondents saying they were targeted because of their religion, race/ethnicity, sex, etc. The other four were focused on the "reason targeted" rather than on prejudice or bigotry. These respondents believed they were targeted because the offender thought their attributes meant that they were part of a vulnerable subpopulation, as such they were an "easy target."
  - *"I tend to be targeted for these kind of scams or MLMs [multi-level marketing scam], for example. I guess it's because of the economic disparity that they see. And they think, you know, we tend to be easier targets."*
  - *"I would say, because I am a Christian and I think that he I think he like kind of fed off of that meaning in the sense of like me being very nice and welcoming and so I think he, I think he thought that I was naive, maybe and that I just would kind of go with the flow."*

- *"I just think it was because religion…because we were going to the same church before, and he quit going there and then he keeps calling me witch and stuff."*

- The respondents who answered 'no' to this question generally had a rationale for not thinking they were targeted due to prejudice or bigotry. The majority of these respondents (10 out of the 12) were victims of scams (or attempted scams) and while some thought they may have been targeted due to their demographics, it was because they belong to a group thought to be vulnerable/easy targets. Some examples of respondent comments include:
  - *"I just feel like at that time I was just an easy target, meaning that I'm not a naive person. I can pick up on things pretty quickly. But I think that during that time I had gotten an email. It looked legitimate."*
  - *"I was preyed upon because, I was a family friend. This individual preyed on friends and family predominantly for his Ponzi scheme to embezzle other people's money."*
  - *"No, unless they thought I was just stupid. You know that maybe they thought they had the edge over somebody, but outside of that no, I don't think it was because of race my sex orientation I think they just blanket everybody, and who they can get is who they can get."*

- When those who said 'no' were asked to explain what types of incidents this question was asking about, their explanations were generally in line with the intent of the question.
  - *"If it had anything to do with my race who I am, what I'm about. The color of my skin."*
  - *"An aspect of my identity, or you know, like a belief of mine, whether that be like I don't know, like religious or political."*
  - *"Targeted against someone of a particular race like Asian or African American or Latino or Caucasian maybe even possibly an income bracket."*
  - *"Asking about were you targeted because of your beliefs or religion or your disability."*
- Similarly, those who said 'no' thought the phrase 'prejudice or bigotry' said things like punishing a certain group and nationality.
- Respondents generally interpreted the meaning of 'sex' to refer to sexual orientation and/or gender. Although some also mentioned females being targeted.
  - *"If we're talking about targeting somebody, I think of females. And I would also throw in there the probably gays as well, not males, but because, again, if it's a prejudiced response, then they're going to be targeting somebody they believe is going against their norm."*
  - *"That means if you target somebody because they're either homosexual or transgender or you know, heterosexual. You target a particular person who is of that particular sexual orientation because you did not like them or believe what they're doing like you don't believe that gays should be married and you target them."*
- Most respondents were able to come up with examples of other personal characteristics that might spur prejudice or bigotry. Examples included:

- Appearance including weight, tattoos, piercings, eye color, hair color.
- Socio economic/ income status.
- Age (elderly).
- Speech impediments.
- Low Intelligence.
- Behaviors such as smoking or drug use.

Recommendation: There were a number of false positives to this question. The false positives were due to respondents thinking about individual vulnerabilities, rather than bigotry or prejudice (i.e., person was viewed as an easy or vulnerable target). This perception may be related to the abbreviation of the bias-motivated crime question that is currently on the NCVS. The introductory statement is:

> *"The next question is about why the offender may have targeted you. The reason may have been prejudice or bigotry toward those with your characteristics or religious beliefs, even if the offender mistakenly thought you had those characteristics or beliefs."*

The conditional language (i.e., "The reason may have been….") could have left the impression that the question is interested in more general reasons that relate to the person's vulnerabilities, not just those related to bigotry and prejudice

The NCVS item has seven sub-questions that ask about each characteristic (e.g., race, religion, disability, sexual orientation). This provides the respondent with a very concrete idea of the domain of the item. By asking about specific types of bigotry and hate, respondents will be much less likely to falsely report being a bias-motivated crime victim.

The false positives may also be related to the types of incidents that screened into the stalking and fraud surveys. Both had subjects reporting on spam and telemarketing that do not meet the standard of an offense. This was especially the case for the fraud cases. The fraud cases had the additional issue that respondents may be less likely to know anything about the motivations of the offender. For stalking, victims were more likely to have some knowledge of who the offender was[46] and why they chose the individual as a target. For this reason, we recommend the question be added to the SVS.

Additionally, it is recommended that the SVS administer the full bias-motivated crime question that asks about each characteristic instead of the abbreviated version that was tested. This should minimize the extent respondents will misinterpret the question in ways that lead to false positive.

[46] Morgan, R.E. and Truman, J.L. (2022) Stalking Victimization, 2019. Bureau of Justice Statistics, NCJ 301735.

5. Summary

A total of 94 cognitive interviews were conducted. Twenty-five each on stalking, identity theft and fraud. Among these 75 respondents, 19 were also administered the bias-motivated crime questions in a separate interview. A summary of the recommendations is shown in Table 8. Most questions are recommended to be adopted, some after making modifications.

The web screening instruments yielded very high prevalence rates for stalking, identity theft and fraud. In many cases these were reports of telemarketing and other sales-related contacts. BJS should review prior surveys to assess whether this was a problem with the last administration of each survey. A relatively simple fix is to remind respondents more often that these incidents should be excluded.

In several instances we recommend collecting a summary of the most recent incident. This recommendation should also be considered for all types of crimes. Summaries are helpful when editing the data, as illustrated by the process used on the core NCVS.

Table 8. Summary of recommendations	
Change considered	**Recommendation**
Stalking	
1. Ask separate questions on phone calls/voice messages from text messages.	Adopt as worded. Consider adding preamble "Excluding calls from bill collectors, solicitors, spam or robocalls."
2. Update the examples related to unwanted emails and messages.	Adopt the question with general descriptions of apps and platforms. Do not adopt the question with more specific examples.
3. Separate the question on monitoring activities into direct and indirect monitoring methods.	Adopt the separated questions.
4. Add 'e-tracker' to the question about electronic tracking.	Do not adopt modified e-tracker question.
5. Modify the question on monitoring activities with social media apps	Adopt the question with examples. Consider adding a qualifier to not include monitoring by people that respondent wants to stay in touch with or companies that would like to sell you something.
6. Add a question on posting sexually explicit images or videos.	Adopt the question.
7. Modify current question on others posting respondent's information to be more specific to posting non-image related personal information.	Adopt the two more detailed questions.
8. Add a question that asks about reactions to the incident for those that report multiple incidents but do not meet the formal stalking definition.	Do not adopt the question as written. Consider testing the question on the next supplement to further analyze the appropriate adjectives to use, as well as the types of incidents that qualify as harassment.
Identity Theft	
1. Add a question on whether someone used cyber methods to use the person's identity.	Adopt this question. Consider switching the order of this and the next question on how the information was obtained.
2. Add additional options to the current question about how the information was obtained.	Probe 'yes' responses to the email option to verify it is not a text message.
3. Modify the question on ever having cyber accounts with additional examples.	Adopt question with examples. Add to the transition before this question with: "…But first I want to find out if you have any email or social media accounts."
4. Add a question on whether anyone has ever created fake email or social media account using the respondent's identity.	Adopt as worded. Probe 'yes' responses to verify that someone impersonated them with a new account.
5. Add examples to question asking about using existing telephone, utility, and other accounts.	Adopt the question with examples. Consider asking for a summary of the incident to verify it is in scope.
6. Add additional examples for follow-up questions to Q11.	Adopt with additional examples.

Change considered	Recommendation
7. Add examples to question asking about using personal information open new accounts.	Adopt the question with examples. Consider asking for a summary of the incident to verify it is in scope.
8. Add a question at the end of the survey asking whether anyone obtained personal information, regardless of if it was ever used.	Adopt the question. Consider asking for a 12-month reference period to reduce burden.
9. Add a follow-up question to P12 asking if the incident occurred within the past 12 months.	Adopt the question.
Fraud	
1. For each type of fraud, add a question on how victim first found out about the fraud.	Consider adding a probe "Is this where you first heard about the (FRAUD TYPE)?" Add emphasis to the word "first" to communicate the first contact. Add 'video call' to the response category for phone. Conduct further research to investigate how to collect data on a series of communications, if they occur (e.g., use 'select all that apply').
2. For relationship or trust fraud, ask a question on how the respondent was first contacted.	Adopt the question with relevant responses reflecting response options in fraud change 1.
3. Add a question on cryptocurrency.	Adopt the question.
Bias-Motivated Crime	
1. Add a bias-motivated crime question from the core NCVS to the three supplements.	Add the question to the SVS. Do not add it to the ITS or SFS because respondents did not have as much knowledge of who may have committed the crime.

Appendices

Appendix A

Web Screener – Stalking

Appendix A
Web Screener – Stalking

Thank you for participating in this survey for the Bureau of Justice Statistics. Before we can start, there are a few things we need to make you aware of.

What is the research about:
The Bureau of Justice Statistics (BJS), located within the U.S. Department of Justice, is conducting this study. BJS has asked Westat to conduct this survey for them. Westat is a company that provides research services to the government. We are looking for persons who can help evaluate survey questions about cybercrime. Your participation is voluntary; you can stop at any point and you can skip any question.

The survey includes questions about yourself and whether you have experienced certain cybercrimes. The information will be used to evaluate the questions. If you are eligible, we will ask if you would like to participate in a follow-up interview (which will involve more in-depth questions about your experiences), for which you will be compensated. This web survey should take about 8 minutes to complete.

How will my information be protected:
BJS is authorized to conduct this work under Title 34 U.S.C. § 10132. By law, BJS and Westat will only use the information collected during these interviews for statistical and research purposes pursuant to 34 U.S.C. § 10134. All personally identifiable information collected under BJS's authority is protected under the confidentiality provisions of 34 U.S.C. § 10231. The law protects your answers from outside requests by any government agency, private organization or individual.

Your name will not be linked to any of your responses, though we may include quotes you provide in our reports. Your responses will be combined with the responses we get from other participants. You will not be identified by name in any published or presented materials.

What are the possible benefits and risks:
There are no known benefits to you for participating in this study. However, your participation is vital to making this study successful and will be helping BJS improve the quality of the data collected.

Some of the questions might make you feel upset or uncomfortable. On every screen below and at the end of the survey, you will receive telephone numbers for organizations that you can contact to get help.

This survey includes some open-ended questions which allow you to write a unique response. Please be aware these response boxes are not a place to report an incident or request direct assistance. We will not immediately review responses to open-ended questions and therefore cannot take action on anything disclosed in an open-ended question. If you need assistance

please contact one of the organizations listed when clicking on the help button or at the end of the survey.

Questions*:* If you have questions about the study, contact David Cantor at 301-294-2080 or davidcantor@westat.com. If you have questions about your rights and welfare as a research participant, please call the Westat Human Subjects Protections office at 1-888-920-7631. Please leave a message with your first name, the name of the research study that you are calling about (the National Crime Victimization Survey), and a phone number beginning with the area code. Someone will return your call as soon as possible.

If you have technical questions about this web survey you can contact the survey Help Desk at 1-855-389- 0286 or WestatSurvey@westat.com. Leave a message with your question along with your telephone number and email address and someone will respond as soon as possible.

Continuing to the survey means that you have read the information above. It also means you voluntarily agree to participate on this survey.

Consent

- ○ Yes. I agree to participate in this survey → GO TO NEXT PAGE
- ○ No. I do not agree to participate in this survey → Thank-you for your interest. END

Random numbers

For randomizing SQ_WEBSITES_1 and SQ_WEBSITES.
Create random number with 50% of sample R1=0 and 50% R1=1

For randomizing SQ_SOCIALMEDIA_1 AND SQ_SOCIALMEDIA_2
Create random number with 50% of sample R2=0 and 50% R2=1

For randomizing SQ_POSTS AND SQ_POSTS_3
Create random number with 50% of sample R3=0 and 50% R3=1

For randomizing which debriefing questions the respondent gets
Create random number with 25% of sample R4=1, 25% of sample R4=2, 25% of sample R4=3 25% of sample R4=4

For randomizing the race/ethnicity question
Create random number with 50% of sample R5=1, 50% of sample R5=0

Demographics

These first questions ask about you.

A1. What is your date of birth?

___/___/____ (MM/DD/YYYY) A1_MM, A1_DD, A1_YYYY

PROGRAMMER NOTE: IF AGE<18 THEN DISPLAY THE MESSAGE BELOW AND TERMINATE THE SURVEY.
"You need to be at least 18 years old to take the survey"

A1A. Are you male or female?

Female
Male

Note: A2_1 to A2_7 used for both sets – if R5=0 it was set 1 (A2a), else set 2 (A2b)

A2a. If R5=0: What is your race and/or ethnicity? Select all that apply.

01 White

For example, English, German, Irish, Italian, Polish, Scottish, etc.

02 Hispanic or Latino

For example, Mexican, Puerto Rican, Salvadoran, Cuban, Dominican, Guatemalan, etc.

03 Black or African American

For example, African American, Jamaican, Haitian, Nigerian, Ethiopian, Somali, etc.

04 Asian

For example, Chinese, Asian Indian, Filipino, Vietnamese, Korean, Japanese, etc.

05 American Indian or Alaska Native

For example, Navajo Nation, Blackfeet Tribe of the Blackfeet Indian Reservation of Montana, Native Village of Barrow Inupiat Traditional Government, Nome Eskimo Community, Aztec, Maya, etc.

06 Middle Eastern or North African

For example, Lebanese, Iranian, Egyptian, Syrian, Iraqi, Israeli, etc.

07 Native Hawaiian or Pacific Islander

For example, Native Hawaiian, Samoan, Chamorro, Tongan, Fijian, Marshallese, etc.

A2b. If R5=1: What is your race and/or ethnicity? Select all that apply.

01 White
02 Hispanic or Latino
03 Black or African American
04 Asian
05 American Indian or Alaska Native
06 Middle Eastern or North African
07 Native Hawaiian or Pacific Islander

The next questions are about unwanted contacts or behaviors using various technologies, such as your phone, the Internet, or social media apps. Please DO NOT include bill collectors, solicitors, or other sales people.

SQ_TELEPHONE

In the past 12 months has anyone made unwanted phone calls or left voice messages excessively to contact you?

Yes 01

No 02

SQ_TEXTMESSAGES

In the past 12 months has anyone sent excessive unwanted text messages to contact you?

Yes 01

No 02

IF R1 = 1 THEN GO TO SQ_WEBSITES_1, ELSE GO TO SQ_WEBSITES.

SQ_WEBSITES_1

In the past 12 months has anyone sent you unwanted messages using email,-social media apps, dating apps or other internet platforms and applications?

Yes 01

No 02

GO TO SP_TECHNOLOGY_DIRECT

From here on out I will only add var names if different than what is here (or was missing)….

SQ_WEBSITES

In the past 12 months has anyone sent you unwanted messages using email, social media apps, or other internet applications like WhatsApp, Snapchat, Instagram, Twitter (X), YouTube, Facebook or TikTok?

Yes 01

No 02

SQ_TECHNOLOGY_DIRECT

In the past 12 months has anyone spied on you using technologies such as a listening device, camera, or video recorder?

Yes 01

No 02

SQ_TECHNOLOGY_INDIRECT

In the past 12 months has anyone spied on you using computer or cell phone monitoring software?

Yes 01

No 02

SQ_APPLICATION

In the past 12 months has anyone tracked your whereabouts with an electronic tracking device or application, such as GPS, an e-tracker, or, an application on your cell phone?

Yes 01

No 02

IF R2 1 THEN GO TO SQ_SOCIALMEDIA_1. ELSE GO TO SQ_SOCIALMEDIA_2

SQ_SOCIALMEDIA_1

In the past 12 months has anyone monitored or observed your activities on social media apps like Facebook, TikTok, YouTube, Instagram, Twitter (X), or LinkedIn?

Yes 01

No 02

GO TO SQ_IMAGE_BASED_SEXUAL_ABUSE

SQ_SOCIALMEDIA_2

In the past 12 months has anyone monitored or observed your activities on social media apps, discussion forums, or other social networking platforms or apps?

Yes 01

No 02

SQ_IMAGE_BASED_SEXUAL_ABUSE

In the past 12 months has anyone posted nude, intimate or sexually explicit images or videos of you on the internet without your consent or threatened to post this content on the internet?

Yes 01

No 02

If R3 EQ 1 THEN GO TO SQ_POSTS ELSE GO TO SQ_POSTS_3

SQ_POSTS

In the past 12 months has anyone posted or threatened to post inappropriate, unwanted, indecent or personal information about you on the Internet including your name, address, email spreading rumors or other information about you?

Yes 01

No 02

GO TO INTRODUCTION BEFORE CHECK 1

SQ_POSTS_3

In the past 12 months has anyone posted or threatened to post inappropriate, unwanted, indecent, or untrue information about you on the Internet?

Yes 01

No 02

SQ_IMAGES_4

In the past 12 months has anyone posted or threatened to post your personal information, including name, address, email or other details about you on the Internet?

Yes 01

No 02

CHECK ITEM 1:

If R answered "Yes" to one or more of SQ_TELEPHONE-SQ_IMAGES_4, then go to introduction before SQ_REPETITION

If R did not answer "Yes" to any of the above items, then skip to Debriefing.

Still thinking about unwanted contacts and behaviors, please answer the following questions.

SQ_REPETITION

Has anyone done (this/any of these things) to you more than once in the past 12 months?

Yes 01

No 02

CHECK ITEM 2:

If R answered "Yes" to more than one of SQ_TELEPHONE - SQ_IMAGES_4, then go to SQ_FEAR.

If R answered "Yes" to only one of SQ_TELEPHONE - SQ_IMAGES_4 and SQ_REPETITION is 'YES' then go to SQ_FEAR

If R answered "Yes" to only one of SQ_TELEPHONE - SQ_IMAGES_4 and SQ_REPETITION is 'NO' then go to Debriefing.

SQ_FEAR

Did any of these unwanted contacts or behaviors make you fear for your safety or the safety of someone close to you?

Yes 01

No 02

SQ_DISTRESS

Did any of these unwanted contacts or behaviors cause you substantial emotional distress?

Yes 01

No 02

Thinking about the person or persons who committed these unwanted behaviors,

SQ_PROPERTY

In the past 12 months did this person or these people damage or attempt to damage or destroy property belonging to you or someone else in your household?

Yes 01

No 02

SQ_ATTACK_SELF

In the past 12 months did this person or these people physically attack you?

Yes 01

No 02

SQ_ATTEMPT_SELF

In the past 12 months did this person or these people attempt to physically attack you?

Yes 01

No 02

SQ_THREAT_SELF

In the past 12 months did this person or these people threaten to physically attack you?

Yes 01

No 02

SQ_ATTACK_OTH

In the past 12 months did this person or these people physically attack someone close to you or a pet?

Yes 01

No 02

SQ_ATTEMPT_OTH

In the past 12 months did this person or these people attempt to physically attack someone close to you or a pet?

Yes 01

No 02

SQ_THREAT_OTH

In the past 12 months did this person or these people threaten to physically attack someone close to you or a pet?

Yes 01

No 02

SQ_ATTACK

This next question is about any physical attacks against you. In the past 5 years, has anyone attacked you with a weapon or by physical force?

Yes 01

No 02

CHECK ITEM 3

COMMENT: IF ONE BEHAVIOR IS SELECTED AND IT OCCURS MULTIPLE TIMES IN LAST 12 MONTHS AND MET STALKING CONSEQUENCES SET SQ_STALK=1.

If ("Yes" to only one of SQ_TELEPHONE to SQ_IMAGES_4) and (SQ_REPETITION eq YES) and [SQ_FEAR eq YES or SQ_DISTRESS eq YES or SQ_PROPERTY eq YES or SQ_ATTACK_SELF eq YES or SQ_ATTEMPT_SELF eq YES or SQ_THREAT_SELF eq YES or SQ_ATTACK_OTH eq YES or SQ_ATTEMPT_OTH eq YES or SQ_THREAT_OTH eq YES] THEN SQ_STALK eq 1.

COMMENT: IF 2 OR MORE BEHAVIORS ARE SELECTED AND MET STALKING CONSEQUENCES SET SQ_STALK=2.

Else (If "Yes" to 2 or more of SQ_TELEPHONE to SQ_IMAGES_4) and [(SQ_FEAR eq YES or SQ_DISTRESS eq YES or SQ_PROPERTY eq YES or SQ_ATTACK_SELF eq YES or SQ_ATTEMPT_SELF eq YES or SQ_THREAT_SELF eq YES or SQ_ATTACK_OTH eq YES or SQ_ATTEMPT_OTH eq YES or SQ_THREAT_OTH eq YES] THEN SQ_STALK eq 2.

If 1<=SQ_STALK<=2 GO TO CONTACT INFORMATION

COMMENT: IF EXPERIENCED STALKING BEHAVIORS AND IT OCCURRED MORE THAN ONCE BUT DID NOT MEET STALKING CONSEQUENCES set SQ_STALK=3

ELSE [(IF "Yes" to only one of SQ_TELEPHONE to SQ_IMAGES_4) and (SQ_REPETITION eq YES)] OR (If "Yes" to 2 or more of SQ_TELEPHONE to SQ_IMAGES_4)} AND SQ_STALK NE 1,2 then SQ_STALK eq 3.

If SQ_STALK eq 3 then go to SQ_OTHERREACTIONS.

COMMENT: DID NOT EXPERIENCE STALKING BEHAVIORS

ELSE GO TO DEBRIEFING

SQ_OTHERREACTIONS

How did you feel when any of these unwanted contacts or behaviors occurred?

Seriously annoyed	Yes	No
Alarmed	Yes	No
Harassed	Yes	No
Intimidated	Yes	No
None of the above	Yes	No

ERROR MESSAGE: If 'none of the above' is selected and at least one of the other responses is selected, display this message:

INCONSISTENT RESPONSE

You selected 'none of the above' and another feeling. Please correct your answer by changing the 'none of the above' to 'no' or change Alarmed, Intimidated, Harassed and Seriously annoyed to 'no'

If SQ_OTHERREACTIONS is equal to any of (Alarmed, Intimidated, Harassed, Seriously Annoyed) Go to Contact Information

Else go to debriefing

Debriefing

Check Item 4:

If R4 eq 1 then go to DB1
If R4 eq 2 then go to Check Item 5
If R4 eq 3 then go to DB9
If R4 eq 4 then go to Check Item 7

DB1. Earlier you were asked:

"In the past 12 months, has anyone made unwanted phone calls or left voice mail messages excessively to contact you"

DB1_1People can do a lot of things with their phones, such as receive calls, go on the internet and other things. What kind of activities is this question asking about?

DB1_2. Could you describe in your own words what "left voice mail messages excessively to contact you" means to you?

If 'yes' to SQ_TELEPHONE ask DB2, else go to DB3

DB2. You said yes that you had received unwanted phone calls or voice messages. Could you briefly tell us about your unwanted calls or voice messages?

DB3. Earlier you were asked

"In the past 12 months, has anyone sent excessive unwanted text messages to contact you?"

What does 'excessive' mean to you in this question?

GO TO CONTACT INFORMATION

CHECK ITEM 5: If R1 eq 1 then go to DB4. ELSE GO TO DB5

DB4. Earlier you were asked:

"In the past 12 months, has anyone sent you unwanted messages using email, social media apps, dating apps, or other internet platforms and applications?"

This question asks about "email or social media apps." --- When you hear "social media apps" what do you think of?

GO TO DB8

DB5. Earlier you were asked:

In the past 12 months, has anyone sent you unwanted messages using email, social media apps, or other internet applications like WhatsApp, Snapchat, Instagram, Twitter (X), YouTube, Facebook or TikTok?

Do you use any of these internet applications?

Yes
No

DB6. Do you use any other internet applications?

Yes
No

DB7. What are those applications?

DB8. Earlier you were asked:

In the past 12 months, has anyone spied on you using technologies such as a listening device, camera, or video recorder?

In your own words, what does 'spied on' mean to you? Can you give some examples?

GO TO CONTACT INFORMATION

DB9. Earlier you were asked:

In the past 12 months, has anyone tracked your whereabouts with an electronic tracking device or application, such as GPS, an e-tracker, or, an application on your cell phone?

What does 'track your whereabouts' mean to you?

DB10. In addition to what is mentioned in this question, are there other ways that someone can be tracked?

Check Item 6: If R2 eq 1 then go to DB11. Else go to DB13

DB11. Earlier you were asked:

In the past 12 months, has anyone monitored or observed your activities on social media apps like Facebook, TikTok, YouTube, Instagram, Twitter (X), or LinkedIn?

What does 'monitor or observed' mean to you?

DB12. Do you use other social media apps that are not listed in this question? If so, what are they?

GO TO CONTACT INFORMATION

DB13. Earlier you were asked:

"In the past 12 months, has anyone monitored or observed your activities on social media apps, discussion forums, or other social networking platforms or apps?"

What does 'monitor or observed' mean to you?

DB14. What specific social media, discussion forums or social network platforms do you think this question is referring to?

GO TO CONTACT INFORMATION

Check Item 7: If R3 eq 1 then go to DB15. Else go to DB16.

DB15: Earlier you were asked:

In the past 12 months, has anyone posted or threatened to post inappropriate, unwanted, indecent or personal information about you on the Internet including your name, address, email spreading rumors or other information about you?

Could you give a few examples of the type of information that is being asked about??

Check Item 8: Go to Check Item 9

DB16.

Earlier you were asked:

In the past 12 months, has anyone posted or threatened to post inappropriate, unwanted, indecent, or untrue information about you on the Internet?

Can you give a few examples of the type of information that is being asked about?

Check Item 9: If SQ_STALK eq 3 then go to DB17. Else go to contact information

DB17. Earlier you were asked:

How did you feel when any of these unwanted contacts or behaviors occurred?

Seriously annoyed
Alarmed
Harassed
Intimidated
None of the above

Describe in your own words how you felt because of the unwanted behaviors and contacts?

Contact Information

As we mentioned at the beginning, if you are eligible, you will be asked to participate in a one hour Zoom interview. In that interview we will evaluate survey questions on certain crimes you may have experienced. The feedback from you and others will help us improve the survey. You will be compensated $60 for your time. If you would like to be considered for this follow-up study please provide your contact information below. If you are eligible, a Westat scheduler will contact you:

First and last name: FirstName, LastName

Email: Email

Phone Number: (___) ___ - ____ PhoneNumber

Appendix B

Web Screener – Identity Theft

Appendix B
Web Screener – Identity Theft

Thank you for participating in this survey for the Bureau of Justice Statistics. Before we can start, there are a few things we need to make you aware of.

What is the research about:

The Bureau of Justice Statistics (BJS), located within the U.S. Department of Justice, is conducting this study. BJS has asked Westat to conduct this survey for them. Westat is a company that provides research services to the government. We are looking for persons who can help evaluate survey questions about cybercrime. Your participation is voluntary; you can stop at any point and you can skip any question.

The survey includes questions about yourself and whether you have experienced certain cybercrimes. The information will be used to evaluate the questions. If you are eligible, we will ask if you would like to participate in a follow-up interview (which will involve more in-depth questions about your experiences), for which you will be compensated. This web survey should take about 8 minutes to complete.

How will my information be protected:

BJS is authorized to conduct this work under Title 34 U.S.C. § 10132. By law, BJS and Westat will only use the information collected during these interviews for statistical and research purposes pursuant to 34 U.S.C. § 10134. All personally identifiable information collected under BJS's authority is protected under the confidentiality provisions of 34 U.S.C. § 10231. The law protects your answers from outside requests by any government agency, private organization or individual.

Your name will not be linked to any of your responses, though we may include quotes you provide in our reports. Your responses will be combined with the responses we get from other participants. You will not be identified by name in any published or presented materials.

What are the possible benefits and risks:

There are no known benefits to you for participating in this study. However, your participation is vital to making this study successful and will be helping BJS improve the quality of the data collected.

Some of the questions might make you feel upset or uncomfortable. On every screen below and at the end of the survey, you will receive telephone numbers for organizations that you can contact to get help.

This survey includes some open-ended questions which allow you to write a unique response. Please be aware these response boxes are not a place to report an incident or request direct

assistance. We will not immediately review responses to open-ended questions and therefore cannot take action on anything disclosed in an open-ended question. If you need assistance please contact one of the organizations listed when clicking on the help button or at the end of the survey.

Questions*:* If you have questions about the study, contact David Cantor at 301-294-2080 or davidcantor@westat.com. If you have questions about your rights and welfare as a research participant, please call the Westat Human Subjects Protections office at 1-888-920-7631. Please leave a message with your first name, the name of the research study that you are calling about (the National Crime Victimization Survey), and a phone number beginning with the area code. Someone will return your call as soon as possible.

If you have technical questions about this web survey you can contact the survey Help Desk at 1-855-389- 0286 or WestatSurvey@westat.com. Leave a message with your question along with your telephone number and email address and someone will respond as soon as possible.

Continuing to the survey means that you have read the information above. It also means you voluntarily agree to participate on this survey.

- ○ Yes. I agree to participate in this survey → GO TO NEXT PAGE
- ○ No. I do not agree to participate in this survey → Thank-you for your interest. END

Random numbers

Create Random number R1 where
R1=1 for 33.3% of sample,
R1=2 for 33.3% of sample
R1=3 for 33.3% of sample

Create Random number R2 where
R2=0 for 50% of the sample
R2=1 for 50% of the sample

Create Random number R5 where:
R5=1, 50% of sample
R5=2, 50% of sample

Demographics

These first questions ask about you.

1. What is your date of birth?

___/___/____ (MM/DD/YYYY) Q1

PROGRAMMER NOTE: IF AGE<18 THEN DISPLAY THE MESSAGE BELOW AND TERMINATE THE SURVEY.
"You need to be at least 18 years old to take the survey"

1A. Are you male or female? Q1A

Female
Male

2a. If R5=1: What is your race and/or ethnicity? *Select all that apply. Q2A_1 to Q2A_7*

01 White
For example, English, German, Irish, Italian, Polish, Scottish, etc.

02 Hispanic or Latino
For example, Mexican, Puerto Rican, Salvadoran, Cuban, Dominican, Guatemalan, etc.

03 Black or African American
For example, African American, Jamaican, Haitian, Nigerian, Ethiopian, Somali, etc.

04 Asian
For example, Chinese, Asian Indian, Filipino, Vietnamese, Korean, Japanese, etc.

05 American Indian or Alaska Native
For example, Navajo Nation, Blackfeet Tribe of the Blackfeet Indian Reservation of Montana, Native Village of Barrow Inupiat Traditional Government, Nome Eskimo Community, Aztec, Maya, etc.

06 Middle Eastern or North African
For example, Lebanese, Iranian, Egyptian, Syrian, Iraqi, Israeli, etc.

07 Native Hawaiian or Pacific Islander
For example, Native Hawaiian, Samoan, Chamorro, Tongan, Fijian, Marshallese, etc.

2b. If R5=2: What is your race and/or ethnicity? *Select all that apply. Q2B_1 to Q2B_7*

01 White
02 Hispanic or Latino
03 Black or African American
04 Asian
05 American Indian or Alaska Native
06 Middle Eastern or North African
07 Native Hawaiian or Pacific Islander

The next questions are about identity theft. Identity theft means someone else using your personal information without your permission to buy something, get cash or services, pay bills, or avoid the law. We will not ask you for any specific account information.

3. In the past 12 months, has anyone used your checking or savings account to make a purchase or withdraw money without your permission? Q3
   - Include times when someone used your debit or ATM cards to make a purchase or withdraw money without your permission.
   - ONLY include times when money was actually deducted from your checking or savings account, regardless of whether you were reimbursed later or not.
   - DO NOT include times when someone used your credit card or online pay accounts.

YES.....01
NO.....02 (Skip to Q6)

4. How did someone use your checking or savings account? Q4

It was done online 01
It was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02
Both.....03
(If R2=1) Don't Know 04

5. How do you think your personal information was obtained to access your checking or savings account? (Mark all that apply) Q5_1 TO Q5_14

I lost an item that included my personal information ..01
My wallet, checkbook, or purse was stolen 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader.....06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)__ Q5_other_____ 13
(If R2=1) Don't know how it was accessed.....14

6. In the past 12 months has anyone used one or more of your credit card accounts without your permission? ONLY include times when charges actually posted to your account, regardless of whether you were reimbursed later. Q6

YES 01
NO.....02 (Skip to Q9)

7. For any of the incidents occurring in the last 12 months, how did someone use your credit card account? Q7

It was done online 01
It was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02
Both.....03
(If R2=1) Don't Know 04

8. How do you think your personal information was obtained to access your credit card account?

(Mark all that apply) Q8_1 TO Q8_14

I lost an item that included my personal information .. 01
My wallet, checkbook, or purse was stolen..... 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction..... 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call..... 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify Q8_other) 13
(If R2=1) Don't know how it was accessed.....14

9. In the last 12 months, has anyone used your email or social media account without your permission to pretend to be you? Q9

YES 01

NO 02

10. In the last 12 months, has anyone created an email or social media account for you without your permission to pretend to be you? Q10

YES 01
NO 02

IF Q9 OR Q10 = YES, ASK Q10A, ELSE SKIP TO Q11

10a. For the incidents that happened in the last 12 months, how do you think your personal information was obtained to use or create your accounts? Q10a_1 TO Q10a_13 (MARK ALL THAT APPLY)

I lost an item that included my personal information .. 01
My wallet, checkbook, or purse was stolen..... 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction..... 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call..... 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify Q10a_other)_____..... 13

11. In the past 12 months, has anyone used any of your other existing accounts, without your permission, such as…

- telephone account such as for cell phone or landline telephone
- internet account such as for internet or wireless Wi-Fi.
- utilities accounts, such as cable, gas, or electric;
- medical insurance accounts, such as Medicare or a health spending account;
- entertainment accounts, such as for music, movies, or games;
- online payment accounts, such as PayPal or Venmo; or

- some other type of accounts?

Only include times when someone successfully posted charges to, took money from, or otherwise misused your account. Q11

YES 01
NO ..... 02 (Skip to Intro to Q15)

12. For any of the incidents occurring in the last 12 months, how did someone use your account? Q12

It was done online 01
It was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02
Both.....03
(If R2=1) Don't Know 04

13. How do you think your personal information was obtained to access your (Telephone/Utilities/Medical Insurance) account? Q13_1 TO Q13_14 (Mark all that apply)

I lost an item that included my personal information .. 01
My wallet, checkbook, or purse was stolen..... 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction..... 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call..... 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)____
Q13_other_____ 13
(If R2=1) Don't know how it was accessed.....14

The next questions are about any NEW ACCOUNTS someone might have opened using your personal information.

14. In the past 12 months, has anyone, without your permission, used your personal information to successfully open any NEW accounts, such as…

- checking or savings accounts;
- credit card accounts;
- email accounts, such as Gmail or Outlook;
- social media accounts, such as Facebook, Instagram, YouTube, Reddit or Pinterest;
- telephone or internet accounts;
- utilities accounts, such as cable, gas, or electric;
- entertainment accounts, such as for music, movies, or games;
- loans or mortgages;
- insurance policies;
- online payment accounts, such as PayPal or Venmo; or
- some other type of new account?

Please include times when someone successfully opened a new account, even if you did not lose any money or were reimbursed later.

YES 01
NO ..... 02 (Skip to Intro to Q17)

15. How did someone open a new account with your personal information? Q15

It was accessed using a computer 01
withdrawal or purchase was done in-person by the individual taking the money.....02
Both.....03
(If R2=1) Don't Know 04

16. How do you think your personal information was obtained to open a new (checking/credit card/ telephone, utility/entertainment/loan or mortgage/insurance policy)? Q16_1 TO Q16_14
(MARK ALL THAT APPLY)

I lost an item that included my personal information .. 01
My wallet, checkbook, or purse was stolen..... 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction..... 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call..... 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)__
Q16_other_____ 13
(If R2=1) Don't know how it was accessed.....14

The next set of questions are about any other misuses of your personal information.

17. In the past 12 months, has anyone used your personal information for some other fraudulent purpose such as…
- filing a fraudulent tax return;
- getting medical treatment;
- applying for a job;
- providing your information to the police to conceal their identity;
- providing your information to some other government authority such as the Department of Motor Vehicles;
- applying for government benefits; or
- something else?

Q17 Please consider only times when your information was actually used, even if the situation was later resolved.

YES 01
NO ..... 02 (Skip to Check Item 1A)

Q18 18. How did someone use your personal information to do (this/these things)?

It was done online 01
It was done in-some other way (e.g., in-person, over the telephone, by mail, something else).....02
Both.....03
(If R2=1) Don't Know 04

19. How do you think your personal information was obtained? (Mark all that apply) Q19_1 TO Q19_14

I lost an item that included my personal information .. 01
My wallet, checkbook, or purse was stolen..... 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction..... 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call..... 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)_____
Q19_other_____ 13
(If R2=1) Don't know how it was accessed.....14

Check Item 1A

If respondent has not reported any identity theft from prior questions, go to Q20. Else go to Q20A

IDTHEFT=0;
If Q3 = yes or Q6 = yes or Q9 = yes or Q10=yes or Q11 = yes or Q14 = yes or Q17=yes IDTHEFT = 1.

If IDTHEFT ne 1 then go to Q20. Else go Q20a.

20. You have been asked about different ways someone may have used your personal information. This next question concerns whether someone ever obtained your personal information using any of the following methods.
(Mark all that apply) Q20_1 TO Q20_11

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 01
It was stolen during an online purchase/transaction 02
Someone stole it during an in-person purchase/transaction, including using a skimmer card.....03
I responded to a scam email or clicked on a link in the email.....04
I responded to a scam phone call 05
I responded to a scam text message or clicked on a link in the message.....06
I responded to a social media post 07
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....08
My electronic records containing personal information were stolen from a company or other organization.....09
None of the above 10
(If R2=1) Don't Know 11

20a. This next question is about any physical attacks against you. <u>In the past 5 years</u>, has anyone attacked you with a weapon or by physical force? Q20A

YES 01
NO 02

CHECK ITEM 1

CYBERTHEFT=0;
IF Q4 IN(1,3) OR Q5 IN(4 – 12) OR Q7 IN(1,3) OR Q8 IN(4-12) or Q9 eq 1 or Q10 eq 1 or Q12 eq in(1,3) or Q13 in(4-12) or Q15 in(1,3) or Q16 in(4-12) or Q18 in(1,3) or Q19 in(4-12) or Q20 in(4-12) then
CYBERTHEFT=1;
IF CYBERTHEFT EQ 1 THEN GO TO CONTACT SECTION
ELSE GO TO CHECK ITEM 2

Debriefing

Check Item 2:
If Q3 eq 1 (yes) or Q6 eq 1 (yes) or Q9 eq 1 or Q10 eq 1 then go to DB1 Else if Q11 eq 1 (yes) or Q14 eq 1 (yes) then go to DB15 Else if Q17 eq 1 or V20 in(1-9) then go to DB25 Else if R1 eq 1 then go to DB1 Else if R1 eq 2 then go to DB15 Else if R1 eq 3 then go to DB25

DB1. Earlier you were asked:

"In the past 12 months, has anyone used your checking or savings account to make a purchase or withdraw money without your permission?

- Include times when someone used your debit or ATM cards to make a purchase or withdraw money without your permission.
- ONLY include times when money was actually deducted from your checking or savings account, regardless of whether you were reimbursed later or not.
- DO NOT include times when someone used your credit card or online pay accounts."

DB1 – only one variable (the display varied by the value of Q3)

(If Q3=2 (no) or skipped : "Could you describe in your own words what type of incident this question is asking about?")

(If Q3 = 1 (yes): You said that someone had used your checking or savings account to make a purchase or withdraw money without your permission. Could you briefly tell us about what happened? ")

If Q3 = 1 (yes) then go to (DB2)

Else go to (DB6)

DB2. Earlier you were asked

"How did someone use your checking or savings account?

It was done online 01
It was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02
Both.....03
(If R2=1) Don't Know 04

DB2 Please describe more specifically how someone used your checking or savings account.

DB3. What does "It was done online" in this question mean to you? Can you give a few examples?

Earlier you were asked:

How do you think your personal information was obtained to access your checking or savings account?

(Mark all that apply)

I lost an item that included my personal information ..01
My wallet, checkbook, or purse was stolen 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader.....06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)_____.....13
(If R2=1) Don't know how it was accessed.....14

If V5 in(1-13) go to DB4, else go to DB5

DB4. (If only one answer to V5: “Your answer was” (Fill in answer from V5)/If V5 has more than one answer: “Your first answer was”) (fill in first answer from V5). How did you find out this was how it was accessed?

Go to DB6

DB5. You did not say how it was accessed. Do you have any ideas or guesses?

DB6. “In the past 12 months has anyone used one or more of your credit card accounts without your permission? ONLY include times when charges actually posted to your account, regardless of whether you were reimbursed later.?

DB6 – only one variable (the display varied by the value of Q6)

(If Q6=2 (no) or skipped : Could you describe in your own words what type of incident this question is asking about?)

(If Q6 = 1 (yes): You said yes to this question. Could you briefly tell us about the incident?

If Q6 = 1 (yes) then go to into to DB7

Else go to DB11

DB7. Earlier you were asked

"How did someone use your credit card account?

It was done online 01
It was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02
Both.....03
Don't Know 04

DB7 Please describe more specifically how someone used your checking or savings account.

DB8. What does "It was done some other way" in this question mean to you? Can you give a few examples?

Earlier you were asked:

How do you think your personal information was obtained to access your credit card account?

(MARK ALL THAT APPLY)

I lost an item that included my personal information ..01
My wallet, checkbook, or purse was stolen 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader.....06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11

My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)_____.....13
Don't know how it was accessed.....14

If V8 in(1-13) go to DB9, else go to DB10

DB9. (If only one answer to V8: "Your answer was"(Fill in answer from V8)/If V8 has more than one answer: "Your first answer was") (fill in first answer from V8). How did you find out this was how it was accessed?

GO TO DB11

DB10. You did not say how it was accessed. Do you have any ideas or guesses?

DB11. Earlier you were asked:

In the past 12 months, has anyone used your email or social media account without your permission to pretend to be you?

DB11 – only one variable (the display varied by the value of Q9)

(If Q9=2 (no) or skipped : "Could you describe in your own words what type of incident this question is asking about?")

(If Q9 = 1 (yes): "You said yes that you had received unwanted phone calls or voice messages. Could you briefly tell us about your unwanted calls or voice messages")

DB12. Earlier you were also asked:

In the past 12 months, has anyone created an email or social media account for you without your permission to pretend to be you?

DB12 – only one variable (the display varied by the value of Q10)

(If Q10=2 (no) or skipped : "Could you describe in your own words what type of incident this question is asking about?")

(If Q10 = 1 (yes): "You said yes that you had received unwanted phone calls or voice messages. Could you briefly tell us about your unwanted calls or voice messages")

If Q9 eq 1 or Q10 eq 1 then go to introduction before DB13

Else go to Contact information

Earlier you were asked:

For the incidents that happened in the last 12 months, how do you think your personal information was obtained to use or create your accounts?

(Mark all that apply)

I lost an item that included my personal information .. 01
My wallet, checkbook, or purse was stolen..... 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction..... 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call..... 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11

My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)_____ . 13

If V10a in(1-13) go to DB14, else go to DB14

DB13. (If only one answer to V10a: "Your answer was" (Fill with answer to V10a)/If V10a has more than one answer: "Your first answer as") (fill in first answer from V10a). How did you find out this was how it was accessed?

Go to Contact information

DB14. You did not say how it was accessed. Do you have any ideas or guesses?

Go to Contact information

DB15. Earlier you were asked

"In the past 12 months, has anyone used any of your other existing accounts, without your permission, such as…

- telephone account such as for cell phone or landline telephone
- internet account such as for internet or wireless Wi-fi.
- utilities accounts, such as cable, gas, or electric;
- medical insurance accounts, such as Medicare or a health spending account;
- entertainment accounts, such as for music, movies, or games;
- online payment accounts, such as PayPal or Venmo; or
- some other type of accounts?

Only include times when someone successfully posted charges to, took money from, or otherwise misused your account.

DB15 – only one variable (the display varied by the value of Q11)

(If Q11=2 (no) or skipped : “Could you describe in your own words what type of incident this question is asking about?”)

(If Q11 = 1 (yes): “You said yes that someone used your existing accounts. Could you briefly tell us more about what happened?

If Q12 = 1 (yes) then go to (DB16)

Else go to (DB20)

DB16. Earlier you were asked

“How did someone use your account?

It was done online 01
Withdrawal or purchase was done in-person by
the individual taking the money.....02
Both.....03
Don’t Know 04

DB16 Please describe more specifically how someone used your account.

DB17. What does “It was done online” in this question mean to you? Can you give a few examples?

Earlier you were asked:

How do you think your personal information was obtained to access your account?

(Mark all that apply)

I lost an item that included my personal information ..01
My wallet, checkbook, or purse was stolen 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader.....06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)_____.....13
Don't know how it was accessed.....14

If V13 in(1-13) go to DB18, else go to DB19

DB18. (If only one answer to V13: "Your answer was" (Fill with answer to V13)/If V13 has more than one answer: "Your first answer was") (fill in first answer from V13). How did you find out how your personal information was obtained?

Go to DB20

DB19. You did not say how it was obtained. Do you have any ideas or guesses?

DB20. Earlier you were asked:

"In the past 12 months, has anyone, without your permission, used your personal information to successfully open any NEW accounts, such as…

- checking or savings accounts;
- credit card accounts;
- email accounts, such as Gmail or Outlook;
- social media accounts, such as Facebook, Instagram, YouTube, Reddit or Pinterest;
- telephone or internet accounts;
- utilities accounts, such as cable, gas, or electric;
- entertainment accounts, such as for music, movies, or games;
- loans or mortgages;
- insurance policies;
- online payment accounts, such as PayPal or Venmo; or
- some other type of new account?

Please include times when someone successfully opened a new account, even if you did not lose any money or were reimbursed later.

DB20 – only one variable (the display varied by the value of Q14)

(If Q14=2 (no) or skipped : "Could you describe in your own words what type of incident this question is asking about?")

(If Q14 = 1 (yes): "You said yes that you had received unwanted phone calls or voice messages. Could you briefly tell us about your unwanted calls or voice messages")

If Q15 = 1 (yes) then go to (DB21)

Else go to Contact information

DB21. Earlier you were asked

"How did someone open a new account with your personal information?

It was done online 01
Withdrawal or purchase was done in-person by the individual taking the money.....02
Both.....03
Don't Know 04

DB21 Please describe more specifically how someone opened a new account using your personal information.

DB22. What does "It was accessed using a computer" in this question mean to you? Can you give a few examples?

Earlier you were asked:

How do you think your personal information was obtained to open a new account?

(MARK ALL THAT APPLY)

I lost an item that included my personal information ..01
My wallet, checkbook, or purse was stolen 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader.....06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)_____.....13
Don't know how it was accessed.....14

If V16 in(1-13) go to DB23, else go to DB24

DB23. (If only one answer to V16: "Your answer was" (Fill with answer from V16)/If V16 has more than one answer: "Your first answer was") (fill in first answer from V16). How did you find out this was how it was accessed?

Go to Contact Information

DB24. You did not say how it was accessed. Do you have any ideas or guesses?

Go to Contact Information

DB25. Earlier you were asked:

"In the past 12 months has anyone used your personal information for some other fraudulent purpose such as…

- filing a fraudulent tax return;
- getting medical treatment;
- applying for a job;
- providing your information to the police to conceal their identity;
- providing your information to some other government authority such as the Department of Motor Vehicles;
- applying for government benefits; or
- something else?

Please consider only times when your information was actually used, even if the situation was later resolved."

DB25 – only one variable (the display varied by the value of Q17)

(If Q17=2 (no) or skipped : Could you describe in your own words what type of incident this question is asking about?)

(If Q17 = 1 (yes): You said yes to this question. Could you briefly tell us about the incident?

If Q17 = 1 (yes) then go DB26

Else if IDTHEFT eq 0 then go to Intro before DB30

Else go to Contact Information

DB26. Earlier you were asked

"How did someone use your personal information for these fraudulent purposes ?

It was done online 01
It was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02
Both.....03
Don't Know 04

DB26 Please describe more specifically how someone used your personal information for fraudulent purposes.

DB27. What does "It was done some other way" in this question mean to you? Can you give a few examples?

Go to Contact Information

Earlier you were asked:

How do you think your personal information was obtained? (Mark all that apply)

I lost an item that included my personal information ..01
My wallet, checkbook, or purse was stolen 02
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04
It was stolen during an online purchase/transaction 05
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader.....06
I responded to a scam email or clicked on a link in the email.....07
I responded to a scam phone call 08
I responded to a scam text message or clicked on a link in the message.....09
I responded to a social media post 10
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11
My electronic records containing personal information were stolen from a company or other organization.....12
Obtained in another way (specify)_____.....13
Don't know how it was accessed.....14

If V19 in(1-13) go to DB28, else go to DB29

DB28. (If only one answer to V19: "Your answer was" (Fill using answer from V19)/If V19 has more than one answer: "Your first answer was") (fill in answer from V19). How did you find out this was how it was accessed?

Go to Contact Information

DB29. You did not say how it was accessed. Do you have any ideas or guesses?

Go to Contact Information

Earlier you were asked:

You have been asked about different ways someone may have used your personal information. This next question concerns whether someone ever obtained your personal information using any of the following methods. (Mark all that apply)

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 01
It was stolen during an online purchase/transaction 02
Someone stole it during an in-person purchase/transaction, including using a skimmer card.....03
I responded to a scam email or clicked on a link in the email.....04
I responded to a scam phone call 05
I responded to a scam text message or clicked on a link in the message.....06
I responded to a social media post 07
My personal information was stolen from my personnel or human resources electronic records at my place of employment.....08
My electronic records containing personal information were stolen from a company or other organization.....09
None of the above 10
Don't Know 11

If V20 in(1-9) go to DB30, else go to contact information

DB30. (If only one answer to V20: "Your answer was" (Fill in from V20)/If V20 has more than one answer: "Your first answer was") (fill in answer from V20). How did you find out this was how it was accessed?

Contact Information

As we mentioned at the beginning, if you are eligible, you will be asked to participate in a one hour Zoom interview. In that interview we will evaluate survey questions on certain crimes you may have experienced. The feedback from you and others will help us improve the survey. You will be compensated $60 for your time. If you would like to be considered for this follow-up study please provide your contact information below. If you are eligible, a Westat scheduler will contact you:

First and last name: FirstName, LastName

Email: Email

Phone Number: PhoneNumber

Appendix C

Web Screener – Fraud

Appendix C
Web Screener – Fraud

Thank you for participating in this survey for the Bureau of Justice Statistics. Before we can start, there are a few things we need to make you aware of.

What is the research about:

The Bureau of Justice Statistics (BJS), located within the U.S. Department of Justice, is conducting this study. BJS has asked Westat to conduct this survey for them. Westat is a company that provides research services to the government. We are looking for persons who can help evaluate survey questions about cybercrime. Your participation is voluntary; you can stop at any point and you can skip any question.

The survey includes questions about yourself and whether you have experienced certain cybercrimes. The information will be used to evaluate the questions. If you are eligible, we will ask if you would like to participate in a follow-up interview (which will involve more in-depth questions about your experiences), for which you will be compensated. This web survey should take about 8 minutes to complete.

How will my information be protected:
BJS is authorized to conduct this work under Title 34 U.S.C. § 10132. By law, BJS and Westat will only use the information collected during these interviews for statistical and research purposes pursuant to 34 U.S.C. § 10134. All personally identifiable information collected under BJS's authority is protected under the confidentiality provisions of 34 U.S.C. § 10231. The law protects your answers from outside requests by any government agency, private organization or individual.

Your name will not be linked to any of your responses, though we may include quotes you provide in our reports. Your responses will be combined with the responses we get from other participants. You will not be identified by name in any published or presented materials.

What are the possible benefits and risks:
There are no known benefits to you for participating in this study. However, your participation is vital to making this study successful and will be helping BJS improve the quality of the data collected.

Some of the questions might make you feel upset or uncomfortable. On every screen below and at the end of the survey, you will receive telephone numbers for organizations that you can contact to get help.

This survey includes some open-ended questions which allow you to write a unique response. Please be aware these response boxes are not a place to report an incident or request direct assistance. We will not immediately review responses to open-ended questions and therefore cannot take action on anything disclosed in an open-ended question. If you need assistance

please contact one of the organizations listed when clicking on the help button or at the end of the survey.

Questions*:* If you have questions about the study, contact David Cantor at 301-294-2080 or davidcantor@westat.com. If you have questions about your rights and welfare as a research participant, please call the Westat Human Subjects Protections office at 1-888-920-7631. Please leave a message with your first name, the name of the research study that you are calling about (the National Crime Victimization Survey), and a phone number beginning with the area code. Someone will return your call as soon as possible.

If you have technical questions about this web survey you can contact the survey Help Desk at 1-855-389- 0286 or WestatSurvey@westat.com. Leave a message with your question along with your telephone number and email address and someone will respond as soon as possible.
Continuing to the survey means that you have read the information above. It also means you voluntarily agree to participate on this survey.

- ○ Yes. I agree to participate in this survey → GO TO NEXT PAGE
- ○ No. I do not agree to participate in this survey → Thank-you for your interest. END

Random numbers

For randomizing the debriefing:

Random number R1: R1=1 for 33% of sample
Random number R1: R2=2 for 33% of sample
Random number R1: R3=3 for 34% of sample
For randomizing the race/ethnicity question
Create random number with 50% of sample R5=1, 50% of sample R5=2

Demographics

These first questions ask about you.

A1. What is your date of birth?

___/___/____ (MM/DD/YYYY) Q1

PROGRAMMER NOTE: IF AGE<18 THEN DISPLAY THE MESSAGE BELOW AND TERMINATE THE SURVEY.
"You need to be at least 18 years old to take the survey"

A1A. Are you male or female? Q1A

Female
Male

A2. Q2A_1 thru Q2A_7

If R5=1: What is your race and/or ethnicity? Select all that apply.

01 White

For example, English, German, Irish, Italian, Polish, Scottish, etc.

02 Hispanic or Latino

For example, Mexican, Puerto Rican, Salvadoran, Cuban, Dominican, Guatemalan, etc.

03 Black or African American

For example, African American, Jamaican, Haitian, Nigerian, Ethiopian, Somali, etc.

04 Asian

For example, Chinese, Asian Indian, Filipino, Vietnamese, Korean, Japanese, etc.

05 American Indian or Alaska Native

For example, Navajo Nation, Blackfeet Tribe of the Blackfeet Indian Reservation of Montana, Native Village of Barrow Inupiat Traditional Government, Nome Eskimo Community, Aztec, Maya, etc.

06 Middle Eastern or North African
For example, Lebanese, Iranian, Egyptian, Syrian, Iraqi, Israeli, etc.

07 Native Hawaiian or Pacific Islander
For example, Native Hawaiian, Samoan, Chamorro, Tongan, Fijian, Marshallese, etc.

If R5=2: What is your race and/or ethnicity? *Select all that apply. Q2B_1 to Q2B_7*

01 White
02 Hispanic or Latino
03 Black or African American
04 Asian
05 American Indian or Alaska Native
06 Middle Eastern or North African
07 Native Hawaiian or Pacific Islander

The next questions are about experiences in which someone convinced you to pay, invest, or donate money, by tricking or lying to you, hiding information, or promising you something that you never received. We will not ask you any specific account information.

S1. In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], did you pay money to receive a prize, grant, inheritance, lottery winning, or sum of money that you were told was yours?

This can include:

- Money
- Trips
- Jewelry
- Televisions
- Electronics
- Other prizes

YES .....01 (Ask S1b)
NO.....02 (Skip to S1c)

S1b. Did you get all of the money or prizes you were promised?

YES .....01 (Skip to S2)
NO.....02 (Skip to S2)

S1c. How about in the last 5 years, did you pay money to receive a prize, grant, inheritance, lottery winning, or sum of money that you were told was yours

YES .....01 (Skip to S1d)
NO.....02 (Skip to S2)

S1d. Did you get all of the money or prizes you were promised?

YES .....01 (Skip to S2)
NO.....02 (Skip to S2)

Phantom Debt Collection Fraud – Screener*

S2. [IF S1=1 or S1d=2: Not including the time(s) you already reported] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], did you pay money to settle or pay off taxes or a debt, but you found out you were being tricked or lied to and the debt was not real or not yours?

YES .....01 (Skip to S3)
NO.....02 (Skip to S2a)

S2a. How about in the last 5 years, did you pay money to settle or pay off taxes or a debt, but you found out you were being tricked or lied to and the debt was not real or not yours?

YES 01
NO.....02

Charity Fraud – Screener

S3. [IF S1=1 or S1d=2 or S2=1 or S2a=1: Not including the time(s) you already reported] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake? Do not include money given to panhandlers on the street.

YES .....01 (Ask S4)
NO.....02 (Skip to S3a)

S3a. How about in the last 5 years, have you donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake? Do not include money given to panhandlers on the street?

YES 01
NO 02

Employment Fraud – Screener

S4. [IF S1=1 or S1d=2 or S2=1 or S2a=1 or S3=1 or S3a=1: Not including the time(s) you already reported] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you paid money to get a job or get into a business opportunity but were tricked or lied to about how the money would be used or what you would receive in return?

YES .....01 (Ask S5)
NO .....02 (Skip to S4a)

S4a. How about in the 5 years, have you paid money to get a job or get into a business opportunity but were tricked or lied to about how the money would be used or what you would receive in return?

YES 01
NO 02

Consumer Investment Fraud – Screener

S5. [If S1=1 or S1d=2 or S2=1 or S2a=1 or S3=1 or S3a=1 or S4=1 or S4a=1: Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you invested money with a person or company that tricked you or lied to you about what you would receive, such as promising a guaranteed return on your investment or that you would not lose any money?

YES .....01 (Ask S6)
NO .....02 (Skip to S5a)

S5a. How about in the last 5 years, have you invested money with a person or company that tricked you or lied to you about what you would receive, such as promising a guaranteed return on your investment or that you would not lose any money?

YES 01
NO 02

Consumer Products Or Services Fraud (Excluding Unauthorized Billing) – Screener

S6. [IF S1=1 or S1d=2 or S2=1 or S2a=1 or S3=1 or S3a=1 or S4=1 or S4a=1 or S5=1 or S5a =1: Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you paid for any products or services that you NEVER received or that turned out to be a SCAM?

YES 01 (Skip to S7)
NO 02 (Skip to S6a)

S6a. How about in the last 5 years, have you paid for any products or services that you NEVER received or that turned out to be a SCAM?

YES ..... 01 (Skip to S7)
NO ..... 02 (Skip to S7)

Relationship/Trust Fraud – Screener

S7. [IF S1=1 or S1d=2 or S2=1 or S2a=1 or S3=1 or S3a=1 or S4=1 or S4a=1 or S5=1 or S5a =1 or S6=1 or S6a=1: Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you donated, sent, or otherwise given money to someone who PRETENDED to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be?

YES ..... 01 (Skip to S8)
NO ..... 02 (Skip to S7a)

S7a. How about in the last 5 years, have you donated, sent, or otherwise given money to someone who PRETENDED to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be?

YES 01
NO 02

S8. This next question is about any physical attacks against you. In the past 5 years, has anyone attacked you with a weapon or by physical force?

YES 01
NO 02

Check Box 1

If R1 eq 1 and S1d=2 then go to Prize or Grant Fraud Incident Form
Else If R1 eq 1 and S2a =1 then go to Phantom debt collection fraud Incident Form
Else If R1 eq 2 and S3a=1 then go to Charity fraud Incident Form
Else If R1 eq 2 and S4a eq 1 then go to Employment Fraud Incident Form
Else If R1 eq 3 and S5a eq 1 then go to Consumer Investment Fraud Incident Form

Else If R1 eq 3 and S6a eq 1 then go to Consumer products or services fraud Incident Form
Else If R1 eq 3 and S7a eq 1 then go to Relationship/trust Fraud Incident Form

Else go to Contact Information

Prize or Grant Fraud – Incident Form

S1P1intro. You indicated that in the last 5 years you paid money to receive a prize, grant, inheritance, lottery winning, or sum of money.

S1P1. For the most recent time this happened how did you first find out about the money or prize?

Someone told me on a phone call 01
A text message 02
Chat application, such as WhatsApp, Telegram or Signal.....03
The TV, radio or a newspaper.....04
Social media.....05
Website 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or delivery to my home or business 09
Some other way (Specify: _____).....10

(Overlay on the same page after answering. If necessary, use a separate page for each open ended question, repeating the original question for reference)

S1P1_1. Could you elaborate on your answer? Provide more details on how you first found out.

_____

_____

_____

S1P1_2. When answering this question, what did 'Social Media' mean to you? Give a few examples

S1P1_3. How does "Social Media" differ from "Website"?

S1P2. Did you provide the money using cryptocurrency?

YES 01
NO 02

(Overlay on the same page after answering.)

S1P2_1. Many people are not familiar with cryptocurrency. What does this mean to you?

Go to Contact Information

Phantom Debt Collection Fraud – Incident Form

S2P1intro. You indicated that in the last 5 years you paid money to settle or pay off taxes or a debt, but you found out you were being tricked or lied to and the debt was not real or not yours?.

S2P1. For the most recent incident, how did you first find out about the debt you were told you owed?

Someone told me on a phone call 01
A text message 02
Chat application, such as WhatsApp, Telegram or Signal.....03
The TV, radio or a newspaper.....04
Social media.....05
Website 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or delivery to my home or business 09
Some other way (Specify: __S2P1_other_____).....10

(Overlay on the same page after answering. If necessary, use a separate page for each open ended question, repeating the original question for reference)

S2P1_1. Could you elaborate on your answer? Provide more details on how you first found out.

S2P1_2. When answering this question, what did 'Social Media' mean to you? Give a few examples

S2P1_3. How does "Social Media" differ from "Website"?

S2P2. Did you provide the money using cryptocurrency?

YES 01
NO 02

(Overlay on the same page after answering.)

S2P2_1. Many people are not familiar with cryptocurrency. What does this mean to you?

Go to Contact Information

Charity Fraud – Incident Form

S3P1intro. You indicated that in the last 5 years you donated money to a charity or a charitable cause that later turned out to be fake or you later suspected was fake.

S3P1. For the most recent time, how did you first find out about the request to donate to a charity or charitable cause that later turned out to be fake or you suspected was fake?

Someone told me on a phone call 01
A text message 02
Chat application, such as WhatsApp,
Telegram or Signal.....03
The TV, radio or a newspaper.....04
Social media.....05
Website 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or
delivery to my home or business 09
Some other way (Specify:
___S3P1_other_____).....10

(Overlay on the same page after answering. If necessary, use a separate page for each open ended question, repeating the original question for reference)

S3P1_1. Could you elaborate on your answer? Provide more details on how you first found out.

_____

_____

_____

S3P1_2. When answering this question, what did 'Social Media' mean to you? Give a few examples

_____

_____

_____

S3P1_3. How does "Social Media" differ from "Website"?

_____

_____

_____

S2P2. Did you provide the money using cryptocurrency?

YES 01
NO 02

(Overlay on the same page after answering.)

S3P2_1. Many people are not familiar with cryptocurrency. What does this mean to you?

_____

_____

_____

Go to Contact Information

Employment Fraud – Incident Form

S4P1intro. You indicated that in the last 5 years you paid money to get a job or get into a business opportunity but were tricked or lied to about how the money would be used or what you would receive in return.

S4P1. For the most recent time, how did you first find out about paying the money to get a job or get into a business opportunity?

Someone told me on a phone call 01
A text message 02
Chat application, such as WhatsApp,
Telegram or Signal.....03
The TV, radio or a newspaper.....04
Social media.....05
Website 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or
delivery to my home or business 09
Some other way (Specify:
__S4P1_other_____).....10

(Overlay on the same page after answering. If necessary, use a separate page for each open ended question, repeating the original question for reference)

S4P1_1. Could you elaborate on your answer? Provide more details on how you first found out.

S4P1_2. When answering this question, what did 'Social Media' mean to you? Give a few examples

S4P1_3. How does "Social Media" differ from "Website"?

S4P2. Did you provide the money using cryptocurrency?

YES 01
NO 02

(Overlay on the same page after answering.)

S4P2_1. Many people are not familiar with cryptocurrency. What does this mean to you?

Go to Contact Information

Consumer Investment Fraud – Incident Form

S5P1intro. You indicated that in the last 5 years you invested money with a person or company that tricked you or lied to you, and you believe the investment was made up or your money was never invested at all.

S5P1. For the most recent time, how did you first find out about investing with the person or company?

Someone told me on a phone call 01
A text message 02
Chat application, such as WhatsApp,
Telegram or Signal.....03
The TV, radio or a newspaper.....04
Social media.....05
Website 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or
delivery to my home or business 09
Some other way (Specify:
____S5P1_other_____).....10

(Overlay on the same page after answering. If necessary, use a separate page for each open ended question, repeating the original question for reference)

S5P1_1. Would you elaborate on your answer? Provide more details on how you first found out.

_____

_____

_____

S5P1_2. When answering this question, what did 'Social Media' mean to you? Give a few examples

_____

_____

_____

S5P1_3. How does "Social Media" differ from "Website"?

_____

_____

_____

S5P2. Did you provide the money using cryptocurrency?

YES.....01
NO.....02

(Overlay on the same page after answering.)

S5P2_1. Many people are not familiar with cryptocurrency. What does this mean to you?

Go to Contact Information

Consumer Products or Services Fraud (Excluding Unauthorized Billing) – Incident Form

S6P1intro. You indicated that in the last 5 years you paid for a product or service that you never received or turned out to be a scam.

S6P1. For the most recent time, how did you first find out about purchasing the product or service?

Website 01
Someone told me in-person 02
From an email I received 03
From material I received in the mail or delivery to my home or business 04
Some other way (Specify: ___S6P1_other_____).....05

(Overlay on the same page after answering. If necessary, use a separate page for each open ended question, repeating the original question for reference)

S6P1_1. Could you elaborate on your answer? Provide more details on how you first found out.

S6P1_2. When answering this question, what did ‘Social Media’ mean to you? Give a few examples

S6P1_3. How does “Social Media” differ from “Website”?

S6P2. Did you provide the money using cryptocurrency?

YES 01
NO 02

(Overlay on the same page after answering.)

S6P2_1. Many people are not familiar with cryptocurrency. What does this mean to you?

Go to Contact Information

Relationship/Trust Fraud – Incident Form

S7P1intro. You indicated that in the last five years you donated, sent, or otherwise gave money to someone who pretended to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be.

S7P1. For the most recent time, which ONE of the following BEST DESCRIBES how you were first contacted by this person?

Through a chat application such as WhatsApp, Telegram, or Signal.....01
Through a dating app 02
Through social media such as Facebook, TikTok, Instagram, or LinkedIn.....03
Through a website.....04
In an email 05
By a text message.....06
By a phone call, or 07
Some other way?.....08

(Overlay on the same page after answering. If necessary, use a separate page for each open ended question, repeating the original question for reference)

S7P1_1. Could you elaborate on your answer? Provide more details on how you were first contacted.

_____

_____

_____

S7P1_2. In this question, how does “Social Media” differ from “Website”? Give examples of a possible website.

_____

_____

_____

S7B4. How much money, altogether, did you give to this person or company?

Please provide your best estimate.

$_____

S7B41. Did you provide the money using cryptocurrency?

YES 01
NO 02

(Overlay on the same page after answering.)

S7B41_1. Many people are not familiar with cryptocurrency. What does this mean to you?

_____

_____

_____

Go to Contact Information

Contact Information

As we mentioned at the beginning, if you are eligible, you will be asked to participate in a one hour Zoom interview. In that interview we will evaluate survey questions on certain crimes you may have experienced. The feedback from you and others will help us improve the survey. You will be compensated $60 for your time. If you would like to be considered for this follow-up study please provide your contact information below. If you are eligible, a Westat scheduler will contact you:

First and last name: FirstName, LastName

Email: Email

Phone Number: (___) ___ - ____PhoneNumber

Appendix D

Cognitive Interview Protocol – Stalking

Appendix D
Cognitive Interview Protocol – Stalking

Hello, thank you for taking the time to talk with me today. My name is _____. I work for Westat, a research company in Rockville, Maryland. For this project, Westat is under contract with the Bureau of Justice Statistics (or BJS), to evaluate survey questions that collects data about certain crimes you may have experienced. The feedback from you and others will help us improve the survey.

We have previously sent you information about this interview and the conditions related to participating. I'll go over the main points related to participating.

What is involved: We will be asking you about your experience of certain crimes. The session will take about 60 minutes. When the interview has concluded, we will email you the digital gift card with $60 loaded on it. Your participation is voluntary; you can stop at any point and you can skip any question.

Confidentiality: BJS will protect and maintain the confidentiality of your personal information to the fullest extent under federal law. BJS, its employees, and its contractors (Westat staff) will only use the information provided for statistical or research purposes pursuant to 34 U.S.C. § 10134. All personally identifiable information collected under BJS's authority is protected under the confidentiality provisions of 34 U.S.C. § 10231. The law protects your answers from outside requests by any government agency, private organization or individual.

You will never be identified by name. The things you tell us may be put in a report, but there will be no way to identify who said what, and your name will not be used anywhere.

Risks: One possible risk is that some questions may upset you if you experienced an unwanted contact. At the end of the interview, you will receive telephone numbers for organizations that you can contact to get help.

Benefits: There are no direct benefits to you for participating in this study. However, you will be helping BJS improve the quality of the data collected.

Questions: If you have questions about the study, contact David Cantor at 301-294-2080 or davidcantor@westat.com. If you have questions about your rights and welfare as a research participant, please call the Westat Human Subjects Protections office at 1-888-920-7631. Please leave a message with your first name, the name of the research study that you are calling about (the National Crime Victimization Survey), and a phone number beginning with the area code. Someone will return your call as soon as possible.

Today, we will be asking you survey questions and asking for your answers. We will then ask you what the question means to you and what your answer means. We will also ask you questions about specific parts of the question. There are no right or wrong answers. We are

interested in everything you have to say. The information that you give us will help us improve the survey. So that you can speak freely about your experiences, I would recommend that you find a private area to participate in our interview today. At the end of the interview, we will email you a list of national organizations that you can call if you want to talk about any feelings or emotions you experience during the interview.

Request

Do you have any questions about anything I just went over?

Finally, because I want to pay close attention to what you say, I would like to record our interview so that we can have an accurate record of what you say while writing our report. Is that okay?

- [UPDATE RESPONDENT ZOOM NAME TO THEIR PARTICIPANT ID]
- [IF REFUSES RECORDING, END INTERVIEW]

Okay great, I'll start recording [START ZOOM RECORDING – TO CLOUD], and I need to ask your permission one more time so that it is recorded. Today is [mo/day/year] at [time]. Do you agree to participate in this interview and to have it recorded?

Interview Protocol

Now, I would like to ask you some questions about times when you may have experienced unwanted contacts or behaviors. I want to remind you that the information you provide is confidential. When answering, please think about anyone who may have done these things, including current or former spouses or partners, other people you may know, or strangers. However, please DO NOT include bill collectors, solicitors, or other salespeople. We ask that you not share specific names of people so that we can reduce the amount of personally identifiable information we receive.

SQ1. In the past 12 months, have you experienced any unwanted contacts or behaviors? By that I mean…

SQ_FOLLOWED
SQ1a. Has anyone followed you around and watched you?

Yes 01
No.....02

SQ_SNEAKED

SQ1b. Has anyone snuck into your home, car, or any place else and done unwanted things to let you know they had been there?

Yes 01
No.....02

SQ_WAITED

SQ1c. Has anyone waited for you at your home, work, school, or any place else when you didn't want them to?

Yes 01
No.....02

The following questions refer to unwanted contacts, in the past 12 months…

SQ_SHOWEDUP

SQ1d. Has anyone shown up, ridden or driven by places where you were when they had no business being there?

Yes 01
No.....02

SQ_ITEMS

SQ1e. Has anyone left or sent unwanted items, such as cards, letters, presents, flowers, or any other unwanted items?

Yes 01
No.....02

SQ_HARASSED

SQ1f. Has anyone harassed or repeatedly asked your friends or family for information about you or your whereabouts?

Yes 01
No.....02

Now I want to ask about unwanted contacts or behaviors using various technologies, such as your phone, the Internet, or social media apps. Again, please DO NOT include bill collectors, solicitors, or other sales people. In the past 12 months…

SQ_TELEPHONE

SQ1g. Has anyone made unwanted phone calls or left voice messages excessively to contact you?

Yes 01
No.....02

If 'no' - Tell me more about how you arrived at your answer.

If 'yes' – Please tell me more about your answer. Probe for how often it occurred.

(If needed for 'yes' responses. Ask all 'No' responses) What does 'left voice mail messages excessively to contact you' mean to you? What does 'excessive' mean to you?

SQ_TEXTMESSAGES

SQ_1g1. Has anyone sent excessive unwanted text messages to contact you?

Yes 01
No.....02

If 'no' - Tell me more about how you arrived at your answer.

If 'yes' – Please tell me more about your answer. (If needed) Probe for how often it occurred.

(If needed for 'yes' responses. Ask all 'No' responses) What does 'left voice mail messages excessively to contact you' mean to you? What does 'excessive' mean to you?

Ask for half of sample Version 1

SQ_WEBSITES

SQ1h. Has anyone sent you unwanted messages using email, social media apps, dating apps or other internet platforms and applications?

Yes..... 01 (Go to SQ1i)
No..... 02 (Go to SQ1i)

Could you tell me more about your answer? (if yes) Please describe what happened.

What does 'unwanted messages' mean to you? (if no) Can you give an example?

What does 'dating apps' mean to you?

What does 'or other internet platforms and applications' mean to you? Can you give a few examples of what these are?

Ask for half the sample Version 2

SQ_WEBSITES_1

SQ1h1. Has anyone sent you unwanted messages using email, social media apps, or other internet applications like WhatsApp, SnapChat, Instagram, Twitter (X), YouTube, Facebook or TikTok?

Yes..... 01
No..... 02

If 'yes' - Could you tell me more about your answer? Please describe what happened.

If 'no' - How did you come up with your answer?

What does 'or other internet platforms and applications' mean to you? (if no) Can you give a few examples of what these are?

SQ_TECHNOLOGY_DIRECT

SQ1i. Has anyone spied on you using technologies such as a listening device, camera, or video recorder?

Yes 01
No.....02

If 'yes' - Could you tell me more about your answer? Please tell me what happened.

If 'no' - How did you come up with your answer?

If 'no' - Can you give a few examples of what type of spying this is referring to?

SQ_TECHNOLOGY_INDIRECT

SQ1i1. Has anyone spied on you using computer or cell phone monitoring software?

Yes 01
No.....02

If 'yes' - Could you tell me more about your answer? Tell me what happened.

If 'no' - How did you come up with your answer?

If 'no' - Can you give a few examples of what type of spying this is referring to?

(everyone) What does 'computer or cell phone monitoring software' mean to you?

(everyone) The last question was REPEAT SQ1i. This question was REPEAT SQ1i1.

How do these two questions differ?

Still thinking about unwanted contacts and behaviors, in the past 12 months…

SQ_APPLICATION

SQ1j. Has anyone tracked your whereabouts with an electronic tracking device or application, such as GPS, an e-tracker, or an application on your cell phone?

Yes 01
No.....02

If 'yes' - Could you tell me more about your answer? Please describe the incident.

If 'no' - How did you come up with your answer?

What does 'tracked your whereabouts' mean to you?

What does 'an e-tracker' mean to you?

Ask for half of sample Version 1

SQ_SOCIALMEDIA

SQ1k. Has anyone monitored or observed your activities on social media apps like Facebook, TikTok, YouTube, Instagram, Twitter (X), or LinkedIn?

Yes.....01 (SQ1X)
No 02 (SQ1X)

If 'yes' - Could you tell me more about your answer? Please describe the incident.

If 'no' - How did you come up with your answer?

What does 'monitored or observed' mean to you? (if not already given) Can you give an example?

What does 'social media apps' mean to you? Can you give a few examples?

Ask for half the sample Version 2

SQ_SOCIALMEDIA_1

SQ1k1. Has anyone monitored or observed your activities on social media apps, discussion forums, or other social networking platforms or apps?

Yes..... 01
No..... 02

If 'yes'- Could you tell me more about your answer?

If 'no' - How did you come up with your answer?

What does 'monitored or observed' mean to you? (if not already given) Can you give an example?

What does 'discussion forums or other social networking platforms or apps' mean to you?

Can you give a few examples of what these are?

SQ_IMAGE_BASED_SEXUAL_ABUSE

SQ1X. Has anyone posted nude, intimate, or sexually explicit images or videos of you on the internet without your consent or threatened to post this content on the internet?

Yes 01
No.....02

If 'yes' - Could you tell me more about your answer? Please describe the incident.

If 'no' - How did you come up with your answer?

Ask for half of sample Version 1

SQ_POSTS

SQ1l. Has anyone posted or threatened to post inappropriate, unwanted, indecent, or personal information about you on the Internet including your name, address, email, spreading rumors or other information about you?

Yes..... 01 (Go to Check Item1)
No ..... 02(Go to Check Item1)

If 'yes' - Could you tell me more about your answer? Please describe the incident.

If 'no' - How did you come up with your answer?

What does 'inappropriate, unwanted, indecent or personal information' mean to you? (if not already given) Can you give an example?

Ask for half the sample Version 2

SQ_POSTS_1

SQ1l1. Has anyone posted or threatened to post inappropriate, unwanted, indecent, or untrue information about you on the Internet?

Yes..... 01
No 02

If 'yes' - Could you tell me more about your answer? Please describe the incident.

If 'no' - Tell me more about how you arrived at your answer.

What does inappropriate, unwanted, indecent or untrue information' mean to you?

SQ_POSTS_2

SQ1l2. Has anyone posted or threatened to post your personal information, including name, address, email, or other details about you on the Internet?

Yes..... 01
No 02

If 'yes' – Can you tell me more about your answer? Please describe the incident.

If no - Tell me more about how you arrived at your answer.

The last question was (REPEAT SQ1l1). This question asked (REPEAT SQ1l2). Can you tell me the difference between the two?

CHECK ITEM 1:
If R answered "Yes" to one or more of SQa to SQ1l2 (SQ_FOLLOWED-SQ_POSTS_2), then skip to SQ2 (SQ_REPETITION).

If R did not answer "Yes" to any of the above items, then skip to END.

SQ_REPETITION

SQ2. Has anyone done (this/any of these things) to you more than once in the past 12 months?

Yes 01
No.....02

CHECK ITEM 2:
If R answered "Yes" to more than one of SQ1a to SQ1l2 (SQ_FOLLOWED-SQ_POSTS_2), then skip to SQ_FEAR.

If R answered "Yes" to only one of SQ1a to SQ1l2 (SQ_FOLLOWED-SQ_POSTS_2) and SQ_REPETITION is "Yes" then skip to SQ_FEAR.

If R answered "Yes" to only one of SQ1a to SQ1l2 (SQ_FOLLOWED-SQ_POSTS_2) and SQ_REPETITION is "No" then skip to. SQ_OTHERREACTIONS

SQ_FEAR

SQ3a. Did any of these unwanted contacts or behaviors make you fear for your safety or the safety of someone close to you?

Yes 01
No.....02

SQ_DISTRESS

SQ3b. Did any of these unwanted contacts or behaviors cause you substantial emotional distress?

Yes 01
No.....02

Now I have some additional questions about the time someone (autofill 'yes' responses from SQ1a through SQ1l2. Thinking about the person or persons who committed these unwanted contacts or behaviors in the **past 12 months**, did any of the following occur –

SQ_PROPERTY

SQ4. Did this person or these people damage or attempt to damage or destroy property belonging to you or someone else in your household?

Yes 01
No.....02

SQ5. (Thinking about the person or persons who committed these unwanted contacts or behaviors in the **past 12 months**…)

Did this person or these people…

SQ_ATTACK_SELF

Physically attack you?

Yes 01
No.....02

SQ_ATTEMPT_SELF

Attempt to physically attack you?

Yes 01
No.....02

SQ_THREAT_SELF

Threaten to physical attack you?

Yes 01
No.....02

SQ6. (Thinking about the person or persons who committed these unwanted contacts or behaviors in the **past 12 months**…)

Did this person or these people…

SQ_ATTACK_OTH

Physically attack someone close to you or a pet?

Yes 01
No.....02

SQ_ATTEMPT_OTH

Attempt to physically attack someone close to you or a pet?

Yes 01
No.....02

SQ_THREAT_OTH

Threaten to physically attack someone close to you or a pet?

Yes 01
No.....02

SQ_OTHERREACTIONS

Did you feel any of the following feelings when any of these unwanted contacts or behaviors occurred?

(MARK ALL THAT APPLY)
Alarmed.....01
Intimidated 02
Harassed 03
Seriously annoyed.....04
None of the above 05

If 'yes' to any of the emotions: Could you tell me more about your answer? How long did this feeling last?

If 'yes' Were there other emotions that you felt?

If 'none of the above' – Were there any emotions you felt that are not listed?

Closing and Incentive

Those are all the questions I have for you. Is there anything we haven't discussed that you would like to mention?

DISCUSS ANY RESPONDENT COMMENTS. STOP RECORDER.

Before we finish, I just want to make sure you're doing ok. (REFER TO DISTRESS PROTOCOL IF NEEDED).

Here is some contact information for local and national organizations that you can call if you want to talk about any feelings or emotions you experience. (GIVE RESOURCE LIST TO R)

Your gift card will be sent to you using the same email that the scheduler used. Thank you for your time.

Appendix E

Cognitive Interview Protocol – Identity Theft

Appendix E
Cognitive Interview Protocol – Identity Theft

Hello, thank you for taking the time to talk with me today. My name is _____. I work for Westat, a research company in Rockville, Maryland. For this project, Westat is under contract with the Bureau of Justice Statistics (or BJS), to evaluate survey questions that collects data about race-ethnicity and certain crimes you may have experienced. The feedback from you and others will help us improve the survey.

We have previously sent you information about this interview and the conditions related to participating. I'll go over the main points related to participating.

What is involved: We will be asking you about your experience of certain crimes. The session will take about 60 minutes. When the interview has concluded, we will email you the digital gift card with $60 loaded on it. Your participation is voluntary; you can stop at any point and you can skip any question.

Confidentiality: BJS will protect and maintain the confidentiality of your personal information to the fullest extent under federal law. BJS, its employees, and its contractors (Westat staff) will only use the information provided for statistical or research purposes. All personally identifiable information collected under BJS's authority. Since the survey is protected under 34 U.S.C. § 10134 and 10231. The law protects your answers from outside requests by any government agency, private organization or individual.

You will never be identified by name. The things you tell us may be put in a report, but there will be no way to identify who said what, and your name will not be used anywhere.

Risks: One possible risk is that some questions may upset you if you experienced an unwanted contact. At the end of the interview, you will receive telephone numbers for organizations that you can contact to get help.

Benefits: There are no direct benefits to you for participating in this study. However, you will be helping BJS improve the quality of the data collected.

Questions: If you have questions about the study, contact David Cantor at 301-294-2080 or davidcantor@westat.com. If you have questions about your rights and welfare as a research participant, please call the Westat Human Subjects Protections office at 1-888-920-7631. Please leave a message with your first name, the name of the research study that you are calling about (the National Crime Victimization Survey), and a phone number beginning with the area code. Someone will return your call as soon as possible.

Today, we will be asking you survey questions and asking for your answers. We will then ask you what the question means to you and what your answer means. We will also ask you questions about specific parts of the question. There are no right or wrong answers. We are

interested in everything you have to say. The information that you give us will help us improve the survey. So that you can speak freely about your experiences, I would recommend that you find a private area to participate in our interview today. At the end of the interview we will email you a list of national organizations that you can call if you want to talk about any feelings or emotions you experience during the interview.

Request

Do you have any questions about anything I just went over?

Finally, because I want to pay close attention to what you say, I would like to record our interview so that we can have an accurate record of what you say while writing our report. Is that okay?

- [UPDATE RESPONDENT ZOOM NAME TO THEIR PARTICIPANT ID]
- [IF REFUSES RECORDING, END INTERVIEW]

Okay great, I'll start recording [START ZOOM RECORDING – TO CLOUD], and I need to ask your permission one more time so that it is recorded. Today is [mo/day/year] at [time]. Do you agree to participate in this interview and to have it recorded?

Interview Protocol

First, I'd like to ask you some questions about the possible misuse of EXISTING ACCOUNTS, which includes existing checking, savings, credit card, social media, and other types of accounts. We ask that you not share specific names of people so that we can reduce the amount of personally identifiable information we receive.

BANK_ACCT_EVER

Q1. Have you ever had a checking or savings account in your name through a bank or financial institution?

Yes 01

No ..... 02 (Skip to Q5)

BANK_ACCT_EVER_USED

Q2. Has anyone EVER used your checking or savings account to make a purchase or withdraw money without your permission?

- Include times when someone used your debit or ATM cards to make a purchase or withdraw money without your permission.
- ONLY include times when money was actually deducted from your checking or savings account, regardless of whether you were reimbursed later or not.
- DO NOT include times when someone used your credit card or online pay accounts.

Yes 01

No.....02 (Skip to Q5)

BANK_ACCT_USED_PASTYR

Q3. Has this happened during the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

Yes 01

No ..... 02 (Skip to Q5)

P1. For the incidents occurring in the last 12 months, how did someone use your checking or savings account?

It was done online 01

It was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02

Both.....03

You answered "SAY THEIR ANSWER". Can you say more about your answer?

Can you tell us how you know it was done that way?

What does 'online' mean to you?

One of the response options says that it "was done in some other way (for example, in-person, over the telephone, by mail, something else)". Can you say in your own words what this means?

P2. How do you think your personal information was obtained to access your checking or savings account?
(MARK ALL THAT APPLY)

I lost an item that included my personal information ..01

My wallet, checkbook, or purse was stolen 02

My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04

It was stolen during an online purchase/transaction 05

Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader.....06

I responded to a scam email or clicked on a link in the email.....07

I responded to a scam phone call 08

I responded to a scam text message or clicked on a link in the message.....09

I responded to a social media post 10

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11

My electronic records containing personal information were stolen from a company or other organization.....12

Obtained in another way (specify)_____.....13

Can you say in your own words what the question is asking?

How did you find out how your personal information was obtained?

(If needed) When you hear "to access your checking or savings account" what does that make you think of?

One answer is "I responded to a scam email or clicked on a link in the email" in your own words, what is this describing?

"I responded to a scam text message or clicked on a link in the message" in your own words, what is this describing?

"I responded to a social media post" in your own words, what is this describing?

"My personal information was stolen from my personnel or human resources electronic records at my place of employment" in your own words, what is this describing?

"My electronic records containing personal information were stolen from a company or other organization" in your own words, what is this describing?

BANK_ACCT_YEAR

Q4a. Did this most recently happen in 2025 or 2024?

2025.....01

2024.....02

BANK_ACCT_MONTH

Q4b. And in what month?

_____ Month (01-12)

If you don't know, please provide your best estimate.

Next, I have some questions about the possible misuse of EXISTING CREDIT CARD ACCOUNTS.

CREDIT_CARD_EVER

Q5. Have you ever had a credit card account in your name? Include major credit cards such as a MasterCard or Visa, and credit cards through retailers, such as Kohl's, Walmart, or Amazon. Please do not include debit cards or gift cards.

Yes 01

No.....02 (Skip to Q9)

CREDIT_CARD_EVER_USED

Q6. Has anyone EVER used one or more of your credit card accounts without your permission? ONLY include times when charges actually posted to your account, regardless of whether you were reimbursed later.

Yes 01

No.....02 (Skip to Q9)

CREDIT_CARD_USED_PASTYR

Q7. Has this happened during the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

Yes 01

No.....02 (Skip to Q9)

P3. For any of the incidents occurring in the last 12 months, how did someone use your credit card account?

It was done online 01

It was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02

Both.....03

You answered "SAY THEIR ANSWER". Can you say more about your answer?

Can you tell us how you know it was done that way?

How sure are you that it was done "THEIR ANSWER"?

What does 'online' mean to you?

One of the response options says that it "was done in some other way (for example, in-person, over the telephone, by mail, something else)". Can you say in your own words what this means?

P4. How do you think your personal information was obtained to access your credit card account?

(MARK ALL THAT APPLY)

I lost an item that included my personal information .. 01

My wallet, checkbook, or purse was stolen..... 02

My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04

It was stolen during an online purchase/transaction..... 05

Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06

I responded to a scam email or clicked on a link in the email.....07

I responded to a scam phone call..... 08

I responded to a scam text message or clicked on a link in the message.....09

I responded to a social media post 10

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11

My electronic records containing personal information were stolen from a company or other organization.....12

Obtained in another way (specify)..... 13

Can you say in your own words what the question is asking?
How did you find out how your personal information was obtained?
One answer is "I responded to a scam email or clicked on a link in the email" in your own words, what is this describing?
"I responded to a scam text message or clicked on a link in the message" in your own words, what is this describing?
"I responded to a social media post" in your own words, what is this describing?
"My personal information was stolen from my personnel or human resources electronic records at my place of employment" in your own words, what is this describing?
"My electronic records containing personal information were stolen from a company or other organization" in your own words, what is this describing?

CREDIT_CARD_YEAR

Q8a. Did this most recently happen in 2025 or 2024

2025.....01

2024.....02

CREDIT_CARD_MONTH
Q8b. And in what month?

_____ Month (01-12)

If you don't know, please provide your best estimate.

These next questions focus on the possible misuse of your existing EMAIL OR SOCIAL MEDIA ACCOUNTS.

EMAIL_SOCIAL_EVER
Q9a. Have you ever had at least one email account, such as Gmail or Outlook, or social media account such as Facebook, Instagram, YouTube, Reddit or Pinterest?

Yes 01

No ..... 02 (Skip to Intro to Q11)

Can you say in your own words what this question is asking?

What do you consider a "social media" account to be?

Do you consider "YouTube, Reddit, and Pinterest" social media accounts?

Can you say more about that?

EMAIL_SOCIAL_EVER_USED
Q9b. Has anyone EVER used your email or social media account without your permission to pretend to be you?

Yes 01

No 02

Q9bb. Has anyone EVER created an email or social media account for you without your permission to pretend to be you?

Yes 01

No 02

You said 'yes', could you say more about your answer? Can you describe what happened?

You said 'no' -- how do you know that for sure?

If 9b or 9bb is Yes, go to 10a. Else skip to Q11.

EMAIL_SOCIAL_USED_PASTYR

Q10a. Has this happened during the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

Yes 01

No ..... 02 (Skip to Intro to Q11)

Which account was used without your permission...

EMAIL_USED

Q10b. Email account, such as Gmail or Outlook?

Yes 01

No 02

SOCIALMEDIA_USED

Q10c. Social media account, such as Facebook or Instagram, YouTube, Reddit or Pinterest?

Yes 01

No 02

P5. For the incidents that happened in the last 12 months, how do you think your personal information was obtained to (use your email or social media account/created an email or social media account for you)?
(MARK ALL THAT APPLY)

I lost an item that included my personal information .. 01

My wallet, checkbook, or purse was stolen..... 02

My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04

It was stolen during an online purchase/transaction..... 05

Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06

I responded to a scam email or clicked on a link in the email.....07

I responded to a scam phone call..... 08

I responded to a scam text message or clicked on a link in the message.....09

I responded to a social media post 10

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11

My electronic records containing personal information were stolen from a company or other organization.....12

Obtained in another way (specify)_____ . 13

You answered, "THEIR ANSWER". Can you tell us what happened?

Do you know or have an idea how that happened?

Can you say more about that?

EMAIL_SOCIAL_YEAR

Q10d. Please think about the most recent time someone misused [this/one of these] account(s). Did this most recently happen in 2025 or 2024?

2025.....01

2024.....02

EMAIL_SOCIAL_MONTH
Q10e. And in what month?

_____ Month (01-12)

If you don't know, please provide your best estimate.
These next questions ask about the possible misuse of any of your other EXISTING ACCOUNTS aside from your bank, credit card, email or social media accounts.

EXISTING_ACCTS_USED_PASTYR
Q11. Has anyone EVER used any of your other existing accounts, without your permission, such as…

- Telephone account such as for cell phone or landline telephone
- Internet account such as for internet or wireless Wi-Fi.
- Utilities accounts, such as cable, gas, or electric;
- Medical insurance accounts, such as Medicare or a health spending account;
- Entertainment accounts, such as for music, movies, or games;
- Online payment accounts, such as PayPal or Venmo; or
- Some other type of accounts?

Only include times when someone successfully posted charges to, took money from, or otherwise misused your account.

Yes 01

No ..... 02 (Skip to Intro to Q15)

(if 'yes') Can you describe what happened?

EXISTING_ACCTS_USED_PASTYR
Q12. Has this happened during the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

Yes 01

No ..... 02 (Skip to Intro to Q15)

Q13. Which of the following types of your EXISTING accounts, other than credit card, bank, email, or social media accounts, did someone post charges to, take money from, or otherwise misuse? Did they misuse one or more of your…

EX_PHONE

Q13a. Telephone accounts such as cell phones or landline?

Yes 01

No 02

Q13aa. Internet accounts such as wireless or Wi-Fi?

Yes 01

No.....02

You said 'yes' to "THEIR ANSWER", could you tell me more about your answer?

Can you describe what happened?

EX_UTILITY

Q13b. Utilities accounts, such as cable, gas, or electric?

Yes 01

No.....02

EX_MEDICAL

Q13c. Medical insurance accounts, such as Medicare or a health spending account?

Yes 01

No.....02

EX_ENTERTAINMENT

Q13d. Entertainment accounts, such as for music, movies, or games?

Yes 01

No.....02

EX_PAYPAL

Q13e. Online payment accounts, such as PayPal or Venmo?

Yes 01

No.....02

OTHER_EX

Q13f. Some other type of account?

Yes 01

No.....02

OTHER_ACCOUNT_SP

[IF YES] What other types of accounts were misused?

_____

If telephone (Q13a), utilities (Q13b) or medical insurance (Q13c) accounts is 'yes' go to P6, else skip to P7.

P6. Thinking about the last 12 months, how did someone use your (Telephone/Utility/Medical Insurance) account?

It was online.....01

The was done in some other way (e.g., in-person, over the telephone, by mail, something else).....02

Both.....03

You answered "ONLINE/SOME OTHER WAY". Can you tell us what happened?

How did you figure out how it happened?

Can you say more about that?

P7. How do you think your personal information was obtained to access your account? (MARK ALL THAT APPLY)

I lost an item that included my personal information .. 01

My wallet, checkbook, or purse was stolen..... 02

My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04

It was stolen during an online purchase/transaction..... 05

Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06

I responded to a scam email or clicked on a link in the email.....07

I responded to a scam phone call..... 08

I responded to a scam text message or clicked on a link in the message.....09

I responded to a social media post 10

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11

My electronic records containing personal information were stolen from a company or other organization.....12

Obtained in another way (specify)_____ 13

In your own words, can you tell us what the question is asking?
You answered [THEIR ANSWER IF 04-13] – how did you figure out that it was [THEIR ANSWER 04-13] that caused access to your account?
Can you say more about that?

EXISTING_ACCTS_YEAR

Q14a. Please think about the most recent time someone misused [this/one of these] existing account(s).

Did this most recently happen in 2025 or 2024?

2025.....01

2024.....02

EXISTING_ACCTS_MONTH

Q14b. And in what month?

_____ Month (01-12)

If you don't know, please provide your best estimate.

Next, I have some questions about any NEW ACCOUNTS someone might have opened using your personal information.

OPEN_NEWACCT_EVER

Q15. Has anyone EVER, without your permission, used your personal information to successfully open any NEW accounts, such as…

- Checking or savings accounts;
- Credit card accounts;
- Email accounts, such as Gmail or Outlook;
- Social media accounts, such as Facebook, Instagram, YouTube, Reddit or Pinterest;
- Telephone or
- Internet accounts;
- Utilities accounts, such as cable, gas, or electric;
- Entertainment accounts, such as for music, movies, or games;
- Loans or mortgages;
- Insurance policies;
- Online payment accounts, such as PayPal or Venmo; or
- Some other type of new account?

Please include times when someone successfully opened a new account, even if you did not lose any money or were reimbursed later.

Yes 01

No ..... 02 (Skip to Intro to Q19)

(If 'yes') – Could you describe what happened?

(If 'no') – Could you describe what this question is asking in your own words?

What types of incidents do you think this question is asking about?

OPEN_NEWACCT_PASTYR

Q16. Has this happened during the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

Yes 01

No ..... 02 (Skip to Intro to Q19)

Q17. With this next question, I'm going to read a list of 12 NEW accounts someone may have successfully opened using your personal information without your permission during the past 12 months. You can say yes to more than one account.

Did someone open…

NEW_BANK

Q17a. New checking or savings accounts?

Yes 01

No.....02

NEW_CREDIT_CARD

Q17b. New credit card accounts?

Yes 01

No.....02

NEW_EMAIL

Q17c. New email accounts, such as Gmail or Outlook?

Yes 01

No.....02

NEW_SOCIALMEDIA

Q17d. New social media accounts, such as Facebook, Instagram, YouTube, Reddit or Pinterest?

Yes 01

No.....02

(if 'yes') – You said 'yes' to "YouTube, Reddit or Pinterest; Telephone or Internet accounts" could you tell me more about your answer?

How did you find out what happened?

(if 'no') – You said 'no' to "YouTube, Reddit or Pinterest; Telephone or Internet accounts". Would you please describe what this question is asking?

NEW_PHONE

Q17e. New telephone accounts?

Yes 01

No.....02

Q17ee. New internet accounts?

Yes 01

No.....02

NEW_UTILITIES

Q17f. New utilities accounts, such as cable, gas, or electric?

Yes 01

No.....02

Did someone open...

NEW_ENTERTAINMENT

Q17g. New entertainment accounts, such as for music, movies, or games?

Yes 01

No.....02

NEW_LOAN

Q17h. New loans or mortgages?

Yes 01

No.....02

NEW_MEDICAL

Q17i. New insurance policies?

Yes 01

No.....02

NEW_PAYPAL

Q17j. New online payment accounts, such as PayPal or Venmo?

Yes 01

No.....02

NEW_OTHER

Q17k. Some other type of new account?

Yes 01

No.....02

NEW_OTHER_SP

[IF YES] What other type of new account was opened?

_____

If new checking (Q17a), credit card (Q17b), telephone (Q17e), utilities (Q17f), entertainment (Q17f), loans (Q17g) or mortgage (Q17h), insurance policy (Q17i) or online payment acct (Q17j) is "yes" go to P8. Else skip to P9.

P8. For any of the incidents occurring in the last 12 months, how did someone open a new (checking/ credit card/telephone, utility/entertainment/loan or mortgage/insurance policy) account with your personal information?
(MARK ALL THAT APPLY)

It was accessed using a computer 01

Withdrawal or purchase was done in-person by the individual taking the money.....02

Both.....03

Can you say in your own words what this question is asking?
You answered "USING A COMPUTER/IN-PERSON/BOTH".
Can you tell us what happened?

How did you figure out that it happened "THEIR ANSWER"?

Can you say more about that?

P9. How do you think your personal information was obtained to open a new (checking/credit card/ telephone/internet, utility/entertainment/loan or mortgage/insurance policy)?
(MARK ALL THAT APPLY)

I lost an item that included my personal information .. 01

My wallet, checkbook, or purse was stolen..... 02

My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04

It was stolen during an online purchase/transaction..... 05

Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06

I responded to a scam email or clicked on a link in the email.....07

I responded to a scam phone call..... 08

I responded to a scam text message or clicked on a link in the message.....09

I responded to a social media post 10

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11

My electronic records containing personal information were stolen from a company or other organization.....12

Obtained in another way (specify)_____..... 13

Can you say in your own words what this question is asking?

You answered "THEIR ANSWER 04-13". Can you tell us what happened?

How did you figure out that it happened "[THEIR ANSWER 04-13]"?

Can you say more about that?

OPEN_NEWACCT_YEAR

Q18a. Please think about the most recent time someone successfully opened [this/one of these] new account(s).

Did this most recently happen in 2025 or 2024?

2025.....01

2024.....02

OPEN_NEWACCT_MONTH

Q18b. And in what month?

_____ Month (01-12)

If you don't know, please provide your best estimate.

The next set of questions are about any other misuses of your personal information.

SOME_OTHER_FRAUD_EVER

Q19. Has anyone EVER used your personal information for some other fraudulent purpose such as…

- Filing a fraudulent tax return;
- Getting medical treatment;
- Applying for a job;
- Providing your information to the police to conceal their identity;
- Providing your information to some other government authority such as the Department of Motor Vehicles;
- Applying for government benefits; or
- Something else?

Please consider only times when your information was actually used, even if the situation was later resolved.

Yes 01

No..... 02 (Skip to Check Item A)

SOME_OTHER_FRAUD_PASTYR

Q20. Has this happened during the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

Yes 01

No..... 02 (Skip to Check Item A)

Q21. In which of the following ways has someone used your personal information during the past 12 months? Was your personal information used…

TAX_RETURN_FRAUD

Q21a. To file a fraudulent tax return?

Yes 01

No.....02

OBTAIN_MEDICAL

Q21b. To get medical treatment?

Yes 01

No.....02

APPLY_FOR_JOB

Q21c. To apply for a job?

Yes 01

No.....02

FALSE_INFO_TO_LAW

Q21d. To provide false information to the police to conceal their identity?

Yes 01

No.....02

FALSE_INFO_TO_GOVT

Q21e. To provide false information to some other government authority such as the Department of Motor Vehicles?

Yes 01

No.....02

GOVT_BENEFITS

Q21f. To apply for government benefits?

Yes 01

No.....02

MISUSED_OTHER_WAY

Q21g. In some other way not already mentioned?

Yes 01

No.....02

MISUSED_OTH_WAY_SP

[IF YES] How else was your personal information misused?

_____

P10. For any of the incidents occurring in the last 12 months, how did someone use your personal information to do (this/these things)?

It was done online 01

It was done in-some other way (e.g., in-person, over the telephone, by mail, something else).....02

Both.....03

Can you say in your own words what this question is asking?

You answered "ONLINE/IN-PERSON/BOTH". Can you tell us what happened?

How did you figure out that it happened "ONLINE/IN-PERSON/BOTH"?

Can you say more about that?

P11. How do you think your personal information was obtained to (file a fraudulent tax return/get medical treatment/apply for a job/to provide false information to the police to conceal their identity/provide false information to a government agency/apply for government benefits/misuse your personal information)?
(MARK ALL THAT APPLY)

I lost an item that included my personal information .. 01

My wallet, checkbook, or purse was stolen..... 02

My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.....03

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 04

It was stolen during an online purchase/transaction..... 05

Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader..... 06

I responded to a scam email or clicked on a link in the email.....07

I responded to a scam phone call..... 08

I responded to a scam text message or clicked on a link in the message.....09

I responded to a social media post 10

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....11

My electronic records containing personal information were stolen from a company or other organization.....12

Obtained in another way (specify)_____..... 13

Can you say in your own words what this question is asking?
You answered "THEIR ANSWER 04-13". Can you tell us what happened?

How did you figure out that it happened "[THEIR ANSWER 04-13]"?

Can you say more about that?

SOME_OTHER_FRAUD_YEAR

Q22a. Please think about the most recent time your personal information was misused in [this way/one of these ways].
Did this most recently happen in 2025 or 2024?

2025.....01

2024.....02

SOME_OTHER_FRAUD_MONTH

Q22b. And in what month?

_____ Month (01-12)

If you don't know, please provide your best estimate.

CHECK ITEM A - If respondent has not reported any of the methods below from prior questions (P2, P4, P5, P7, P9, or P11), go to P12. Else Go To Race/Ethnicity section.

P12. I've asked you about different ways someone may have used your personal information. This next question concerns whether someone ever obtained your personal information using any of the following methods.
(MARK ALL THAT APPLY)

It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 01

It was stolen during an online purchase/transaction 02

Someone stole it during an in-person purchase/transaction, including using a skimmer card.....03

I responded to a scam email or clicked on a link in the email.....04

I responded to a scam phone call 05

I responded to a scam text message or clicked on a link in the message.....06

I responded to a social media post 07

My personal information was stolen from my personnel or human resources electronic records at my place of employment.....08

My electronic records containing personal information were stolen from a company or other organization.....09

None of the above 10

You answered that your personal information was accessed electronically from [THEIR ANSWER]. How did you know that it was accessed because [THEIR ANSWER]?
Can you say more about that?

P13. Has this happened during the past 12 months, that is from [AUOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

YES 01

NO.....02

You said "Yes/No" to its happening in the past 12 months. How do you know it was [in the past 12 months/not in the past 12 months]?

Can you say more about that [HOW THEY CALCULATED / ANCHORED TO KNOW PAST 12 MONTHS].

Race and Ethnicity Questions

THREE ALTERNATIVES: ONE ALTERNATIVE WILL BE TESTED IN EACH COGNITIVE INTERVIEW. RESPONDENTS WILL BE RANDOMLY ASSIGNED TO ONE OF THE THREE ALTERNATIVES.

Option 1
Next I am going to ask you questions about the race and ethnicity of each person who lives in your household. I will ask about each person, starting with you. You do not have to use the names of the person, you can use nicknames, initials or just refer to each individual as 'person 1', 'person 2', etc…

First, how many people live in your household, including any babies or small children?

Number _____

Before we start, can you tell us what you think of when you hear "race and ethnicity"?

Just tell us whatever jumps into your head.

ASK FOR THE FIRST THREE PERSONS

R1. What is (your/Person #) race and/or ethnicity? Select all that apply.

Is it…

American Indian or Alaska Native	01	01	01
Asian	02	01	01
Black or African American	03	01	01
Hispanic or Latino	04	01	01
Middle Eastern or North African	05	01	01
Native Hawaiian or Pacific Islander	06	01	01
White	07	01	01

If American Indian or Alaska Native ask:

R1aa. You said you were American Indian or Alaska Native. Which of the following are you? Select all that apply.

Navajo Nation	01	01	01
Blackfeet Tribe of the Blackfeet Indian Reservation of Montana	02	01	01
Native Village of Barrow Inupiat Traditional Government	03	01	01
Nome Eskimo Community	04	01	01
Aztec	05	01	01
Maya	06	01	01
Other	07	01	01

Specify

_____

If Asian ask:

R1ba. You said (you are/Person # is) Asian. Which of the following are you? Select all that apply.

Chinese	01	01	01
Asian Indian	02	01	01
Filipino	03	01	01
Vietnamese	04	01	01
Korean	05	01	01
Japanese	06	01	01
Other	07	01	01

Specify

_____

If Black or African American ask:

R1ca.You said (you are/Person # is) Black or African American. Which of the following are you? Select all that apply.

African American	01	01	01
Jamaican	02	01	01
Haitian	03	01	01
Nigerian	04	01	01
Ethiopian	05	01	01
Somali	06	01	01
Other	07	01	01

Specify

_____

If Hispanic or Latino ask:

R1da. You said (you are/Person # is) Hispanic or Latino. Which of the following are you? Select all that apply.

Mexican	01	01	01
Puerto Rican	02	01	01
Salvadoran	03	01	01
Cuban	04	01	01
Dominican	05	01	01
Guatemalan	06	01	01
Other	07	01	01

Specify _____

If Middle Eastern ask:

R1ea. You said (you are/Person # is) Middle Eastern or North African. Which of the following are you? Select all that apply.

Lebanese	01	01	01
Iranian	02	01	01
Egyptian	03	01	01
Syrian	04	01	01
Iraqi	05	01	01
Israeli	06	01	01
Other	07	01	01

Specify _____

If Native Hawaiian or Pacific Islander ask:

R1fa. You said (you are/Person # is) Native Hawaiian or Pacific Islander. Which of the following (are you/is Person #)? Select all that apply.

Native Hawaiian	01	01	01
Samoan	02	01	01
Chamorro	03	01	01
Tongan	04	01	01
Fijian	05	01	01
Marshallese	06	01	01
Other	07	01	01

Specify _____

If White ask:

R1ga. You said (you are/Person # is) White. Which of the following are you? Select all that apply.

English	01	01	01
German	02	01	01
Irish	03	01	01
Italian	04	01	01
Polish	05	01	01
Scottish	06	01	01
Other	07	01	01

Specify

_____

DEBRIEF FOR RACE/ETHNICITY OF RESPONDENT

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that you are "<Major Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What about reading all of the categories to you. What did you think about that?

Why do you think we read all the categories?

DEBRIEF ABOUT THE DETAILED RACE CATEGORIES - SCROLL BACK OVER THE CATEGORIES FOR THE RESPONDENT AND READ A FEW ALOUD. GET THE RESPONDENT TO ATTEND TO THEM.

You said you are "<Detailed Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What do you think of the race descriptions relating to the country of origin? How did you use them when answering the question?

(IF DID NOT USE EXAMPLES) Do the categories relating to the country of origin represent who you feel you are? Why or why not?
What makes you say that? Can you say more about that?
ADMINISTER R1 TO R1GA FOR UP TO TWO OTHER HOUSEHOLD MEMBERS.

OK, now let's' turn to [PERSON #] in your household.

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that Person # is "<Major Race>" How did you arrive at your answer?

What is the relationship of Person # to you (spouse, child, cousin, unrelated)

What about reading all of the categories to you? What did you think about that? Why do you think we read all the categories?

How do you know their background?

Option 2
Next I am going to ask you questions about the race and ethnicity of each person who lives in your household. I will ask about each person, starting with you. You do not have to use the names of the person, you can use nicknames, initials or just refer to each individual as 'person 1', 'person 2', etc…

First, how many people live in your household, including any babies or small children?

Number _____

Before we start, can you tell us what you think of when you hear "race and ethnicity"?

Just tell us whatever jumps into your head.

ASK FOR THE FIRST THREE PERSONS

R2. What is (your/Person #) race and/or ethnicity?

R2a. Is it American Indian or Alaska Native?

For example Navajo Nation, Blackfeet Tribe of the Blackfeet Indian Reservation of Montana, Native Village of Barrow lnupiat Traditional Government, Nome Eskimo Community, Aztec, Maya, etc.

YES	01	01	01
NO	02	01	01

R2b. Is it Asian?

For example, Chinese, Asian Indian, Filipino, Vietnamese, Korean, Japanese, etc.

YES	01	01	01
NO	02	01	01

R2c. Is it Black or African American?

For example, African American, Jamaican, Haitian, Nigerian, Ethiopian, Somali, etc.

YES	01	01	01
NO	02	01	01

R2d. Is it Hispanic or Latino?

For example, Mexican, Puerto Rican, Salvadoran, Cuban, Dominican, Guatemalan, etc., etc.

YES	01	01	01
NO	02	01	01

R2e. Is it Middle Eastern or North African?

For example, Lebanese, Iranian, Egyptian, Syrian, Iraqi, Israeli, etc.

YES	01	01	01
NO	02	01	01

R2f. Is it Native Hawaiian or Pacific Islander?

For example, Native Hawaiian, Samoan, Chamorro, Tongan, Fijian, Marsha/Iese, etc

YES	01	01	01
NO	02	01	01

R2g. Is it White?

For example, English, German, Irish, Italian, Polish, Scottish, etc.

YES	01	01	01
NO	02	01	01

If American Indian or Alaska Native ask:

R2aa. You said (you are/Person # is) American Indian or Alaska Native. Which of the following (are you/is Person #)? Select all that apply.

Navajo Nation	01	01	01
Blackfeet Tribe of the Blackfeet Indian Reservation of Montana	01	01	01
Native Village of Barrow Inupiat Traditional Government	03	01	01
Nome Eskimo Community	04	01	01
Aztec	05	01	01
Maya	06	01	01
Other	07	01	01

Specify

_____

If Asian ask:

R2ba. You said (you are/Person # is) Asian. Which of the following (are you/is Person #)? Select all that apply.

Chinese	01	01	01
Asian Indian	02	01	01
Filipino	03	01	01
Vietnamese	04	01	01
Korean	05	01	01
Japanese	06	01	01
Other	07	01	01

Specify

_____

If Black or African American ask:

R2ca. You said (you are/Person # is) Black or African American. Which of the following (are you/is Person #)? Select all that apply.

African American	01	01	01
Jamaican	02	01	01
Haitian	03	01	01
Nigerian	04	01	01
Ethiopian	05	01	01
Somali	06	01	01
Other	07	01	01

Specify

_____

If Hispanic or Latino ask:

R2da. You said (you are /Person # is) Hispanic or Latino. Which of the following (are you/is Person #)? Select all that apply.

Mexican	01	01	01
Puerto Rican	02	01	01
Salvadoran	03	01	01
Cuban	04	01	01
Dominican	05	01	01
Guatemalan	06	01	01
Other	07	01	01

Specify

_____

If Middle Eastern ask:

R2ea. You said (you are/Person # is) Middle Eastern or North African. Which of the following (are you/is Person #)? Select all that apply.

Lebanese	01	01	01
Iranian	02	01	01
Egyptian	03	01	01
Syrian	04	01	01
Iraqi	05	01	01
Israeli	06	01	01
Other	07	01	01

Specify

_____

If Native Hawaiian or Pacific Islander ask:

R2fa. You said (you are/Person # is) Native Hawaiian or Pacific Islander. Which of the following (are you/is Person #)? Select all that apply.

Native Hawaiian	01	01	01
Samoan	02	01	01
Chamorro	03	01	01
Tongan	04	01	01
Fijian	05	01	01
Marshallese	06	01	01
Other	07	01	01

Specify _____

If White ask:

R2ga. You said (you are/Person # is) White. Which of the following (are you/is Person #)? Select all that apply.

English	01	01	01
German	02	01	01
Irish	03	01	01
Italian	04	01	01
Polish	05	01	01
Scottish	06	01	01
Other	07	01	01

Specify

_____

DEBRIEF FOR RACE/ETHNICITY OF RESPONDENT

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that you are "<Major Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What about reading all of the categories to you. What did you think about that?

Why do you think we read all the categories?

DEBRIEF ABOUT THE DETAILED RACE CATEGORIES - SCROLL BACK OVER THE CATEGORIES FOR THE RESPONDENT AND READ A FEW ALOUD. GET THE RESPONDENT TO ATTEND TO THEM.

You said you are "<Detailed Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What do you think of the race descriptions relating to the country of origin? How did you use them when answering the question?

(IF DID NOT USE EXAMPLES) **Do the categories relating to the country of origin represent who you feel you are? Why or why not?**

What makes you say that? Can you say more about that?

ADMINISTER R2 TO R2GA FOR UP TO TWO OTHER HOUSEHOLD MEMBERS.

OK, now let's' turn to [PERSON #] in your household.

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that Person # is "<Major Race>" How did you arrive at your answer?

What is the relationship of Person # to you (spouse, child, cousin, unrelated)

What about reading all of the categories to you? What did you think about that? Why do you think we read all the categories?

How do you know their background?

Option 3

R3.Next I am going to ask you questions about the race and ethnicity of each person who lives in your household. I will ask about each person, starting with you. You do not have to use the names of the person, you can use nicknames, initials or just refer to each individual as 'person 1', 'person 2', etc…

First, how many people live in your household, including any babies or small children?

Number _____

Before we start, can you tell us what you think of when you hear "race and ethnicity"?

Just tell us whatever jumps into your head.

ASK FOR THE FIRST THREE PERSONS

What is (your/person #) race and/or ethnicity? You can select more than one category.

R3a. Is it American Indian? For example, Navajo Nation, Blackfeet Tribe of the Blackfeet Indian Reservation of Montana, Native Village of Barrow Inupiat Traditional Government, Nome Eskimo Community, Aztec, Maya, etc…

YES	01	Go to R3aa	01 01
NO	02	Go to R3b	01 01

R3aa. Which of the following (are you/is person #)? Select all that apply

Navajo Nation	01	01	01
Blackfeet Tribe of the Blackfeet Indian Reservation of Montana	02	01	01
Native Village of Barrow Inupiat Traditional Government	03	01	01
Nome Eskimo Community	04	01	01
Aztec	05	01	01
Maya	06	01	01
Other	07	01	01

Specify

_____

R3b. Is it Asian?

YES .....01 Go to R3ba 01 01
NO .....02 Go to R3c 01 01

R3ba. Which of the following (are you/is person #)? Select all that apply

Chinese	01	01	01
Asian Indian	02	01	01
Filipino	03	01	01
Vietnamese	04	01	01
Korean	05	01	01
Japanese	06	01	01
Other	07	01	01

Specify

_____

R3c. Is it Black or African American?

YES .....01 Go to R3ca 01 01
NO .....02 Go to R3d 01 01

R3ca. Which of the following (are you/is person #)? Select all that apply

African American	01	01	01
Jamaican	02	01	01
Haitian	03	01	01
Nigerian	04	01	01
Ethiopian	05	01	01
Somali	06	01	01
Other	07	01	01

Specify

_____

R3d. Is it Hispanic or Latino?

YES .....01 Go to R3da 01 01
NO .....02 Go to R3e 01 01

R3da. Which of the following (are you/is person #)? Select all that apply

Mexican	01	01	01
Puerto Rican	02	01	01
Salvadoran	03	01	01
Cuban	04	01	01
Dominican	05	01	01
Guatemalan	06	01	01
Other	07	01	01

Specify

_____

R3e. Is it Middle Eastern or North African?

YES	01	Go to R3ea	01 01
NO	02	Go to R3f	01 01

R3ea. Which of the following (are you/is person #)? Select all that apply

Lebanese	01	01	01
Iranian	02	01	01
Egyptian	03	01	01
Syrian	04	01	01
Iraqi	05	01	01
Israeli	06	01	01
Other	07	01	01

Specify

_____

R3f. Is it Native Hawaiian or Pacific Islander?

YES	01	Go to R3fa	01 01
NO	02	Go to R3g	01 01

R3fa. Which of the following (are you/is person #)? Select all that apply

Native Hawaiian	01	01	01
Samoan	02	01	01
Chamorro	03	01	01
Tongan	04	01	01
Fijian	05	01	01
Marshallese	06	01	01
Other	07	01	01

Specify

_____

R3g. Is it White?

YES .....01 Go to R3fa 01 01
NO.....02 Go to debrief 01 01

R3ga. Which of the following (are you/is person #)?

English	01	01	01
German	02	01	01
Irish	03	01	01
Italian	04	01	01
Polish	05	01	01
Scottish	06	01	01
Other	07	01	01

Specify

_____

DEBRIEF FOR RACE/ETHNICITY OF RESPONDENT

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that you are "<Major Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What about reading all of the categories to you. What did you think about that?

Why do you think we read all the categories?

DEBRIEF ABOUT THE DETAILED RACE CATEGORIES - SCROLL BACK OVER THE CATEGORIES FOR THE RESPONDENT AND READ A FEW ALOUD. GET THE RESPONDENT TO ATTEND TO THEM.

You said you are "<Detailed Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What do you think of the race descriptions relating to the country of origin? How did you use them when answering the question?

(IF DID NOT USE EXAMPLES) Do the categories relating to the country of origin represent who you feel you are? Why or why not?

What makes you say that? Can you say more about that?

ADMINISTER R3 TO R3GA FOR UP TO TWO OTHER HOUSEHOLD MEMBERS.

OK, now let's' turn to [PERSON #] in your household.

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that Person # is "<Major Race>" How did you arrive at your answer?

What is the relationship of Person # to you (spouse, child, cousin, unrelated)

What about reading all of the categories to you? What did you think about that? Why do you think we read all the categories?

How do you know their background?

Closing and Incentive

Those are all the questions I have for you. Is there anything we haven't discussed that you would like to mention?

DISCUSS ANY RESPONDENT COMMENTS.

STOP RECORDER.

Before we finish, I just want to make sure you're doing ok. (REFER TO DISTRESS PROTOCOL IF NEEDED).

Here is some contact information for local and national organizations that you can call if you want to talk about any feelings or emotions you experience. (GIVE RESOURCE LIST TO R)

Your gift card will be sent to you using the same email that the scheduler used. Thank you for your time.

Appendix F

Cognitive Interview Protocol – Fraud

Appendix F
Cognitive Interview Protocol – Fraud

Hello, thank you for taking the time to talk with me today. My name is _____. I work for Westat, a research company in Rockville, Maryland. For this project, Westat is under contract with the Bureau of Justice Statistics (or BJS), to evaluate survey questions that collects data about race-ethnicity and certain crimes you may have experienced. The feedback from you and others will help us improve the survey.

We have previously sent you information about this interview and the conditions related to participating. I'll go over the main points related to participating.

What is involved: We will be asking you about your experience of certain crimes. The session will take about 60 minutes. When the interview has concluded, we will email you the digital gift card with $60 loaded on it. Your participation is voluntary; you can stop at any point and you can skip any question.

Confidentiality: BJS will protect and maintain the confidentiality of your personal information to the fullest extent under federal law. BJS, its employees, and its contractors (Westat staff) will only use the information provided for statistical or research purposes pursuant to 34 U.S.C. § 10134. All personally identifiable information collected under BJS's authority is protected under the confidentiality provisions of 34 U.S.C. § 10231. The law protects your answers from outside requests by any government agency, private organization or individual.

You will never be identified by name. The things you tell us may be put in a report, but there will be no way to identify who said what, and your name will not be used anywhere.

Risks: One possible risk is that some questions may upset you if you experienced an unwanted contact. At the end of the interview, you will receive telephone numbers for organizations that you can contact to get help.

Benefits: There are no direct benefits to you for participating in this study. However, you will be helping BJS improve the quality of the data collected.

Questions: If you have questions about the study, contact David Cantor at 301-294-2080 or davidcantor@westat.com. If you have questions about your rights and welfare as a research participant, please call the Westat Human Subjects Protections office at 1-888-920-7631. Please leave a message with your first name, the name of the research study that you are calling about (the National Crime Victimization Survey), and a phone number beginning with the area code. Someone will return your call as soon as possible.

Today, we will be asking you survey questions and asking for your answers. We will then ask you what the question means to you and what your answer means. We will also ask you questions about specific parts of the question. There are no right or wrong answers. We are

interested in everything you have to say. The information that you give us will help us improve the survey. So that you can speak freely about your experiences, I would recommend that you find a private area to participate in our interview today. At the end of the interview we will email you a list of national organizations that you can call if you want to talk about any feelings or emotions you experience during the interview.

Request

Do you have any questions about anything I just went over?

Finally, because I want to pay close attention to what you say, I would like to record our interview so that we can have an accurate record of what you say while writing our report. Is that okay?

- [UPDATE RESPONDENT ZOOM NAME TO THEIR PARTICIPANT ID]
- [IF REFUSES RECORDING, END INTERVIEW]

Okay great, I'll start recording [START ZOOM RECORDING – TO CLOUD], and I need to ask your permission one more time so that it is recorded. Today is [mo/day/year] at [time]. Do you agree to participate in this interview and to have it recorded?

Interview Protocol

The next questions are about experiences in which someone convinced you to pay, invest, or donate money, by tricking or lying to you, hiding information, or promising you something that you never received. We will not ask you any specific account information. And we ask that you not share specific names of people so that we can reduce the amount of personally identifiable information we receive.

S1. **In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], did you pay money to receive a prize, grant, inheritance, lottery winning, or sum of money that you were told was yours?**
This can include:

- *Money*
- *Trips*
- *Jewelry*
- *Televisions*
- *Electronics*
- *Other prizes*

YES 01
NO .....02 (Skip to S2)

S1a. Did you get all of the money or prizes you were promised?

YES 01
NO 02

S1b. For the most recent time this happened how did you first find out about the money or prize?

Someone told me on a phone call 01
A text message 02
The TV, radio or a newspaper.....03
Social media.....04
Website 05
Chat application, such as WhatsApp, Telegram or Signal 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or delivery to my home or business.....09
Some other way (Specify: _____).....10

Could you elaborate on your answer? Provide more details on how you first found out.

Here are the categories I just read to you (Share your screen and display showcard #1 to R). How did these categories fit when you were selecting an answer?

Is there anything that we are missing?

What does 'Social Media' mean to you? Could you give some examples?

What does 'Chat application' mean to you?

When answering this question, what did 'Social Media' mean to you? Can you give a few examples?

How does 'Social Media' differ from "Website or other internet applications"

S1d. **Did you provide the money using cryptocurrency?**

YES 01
NO 02

Many people are not familiar with cryptocurrency. What does this mean to you?

S2. **[Not including the time(s) you already reported] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], did you pay money to settle or pay off taxes or a debt, but you found out you were being tricked or lied to and the debt was not real or not yours?**

YES 01
NO .....02 Go to S3

S2a. **For the most recent incident, how did you first find out about the debt you were told you owed?**

Someone told me on a phone call 01
A text message 02
The TV, radio or a newspaper.....03
Social media.....04
Website 05
Chat application, such as WhatsApp, Telegram or Signal 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or delivery to my home or business.....09
Some other way (Specify: _____).....10

Could you elaborate on your answer? Provide more details on how you first found out.

Here are the categories I just read to you (Share your screen and display showcard #1 to R).

How did these categories fit when you were selecting an answer?

Is there anything that we are missing?

ASK IF NOT ALREADY ASKED
What does 'Social Media' mean to you? Could you give some examples?

What does 'Chat application' mean to you?

ASK IF NOT ALREADY ASKED
When answering this question, what did 'Social Media' mean to you? Give a few examples?

ASK IF NOT ALREADY ASKED

How does 'Social Media' differ from "Website or other internet applications"?

S2c. Did you provide the money using cryptocurrency?

YES 01
NO 02

ASK IF NOT ALREADY ASKED

Many people are not familiar with cryptocurrency. What does this mean to you?

S3. [Not including the time(s) you already reported] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake? Do not include money given to panhandlers on the street.

YES 01
NO .....02 (Go to S4)

S3a. For the most recent time, how did you first find out about the request to donate to a charity or charitable cause that later turned out to be fake or you suspected was fake?

Someone told me on a phone call 01
A text message 02
The TV, radio or a newspaper.....03
Social media.....04
Website 05
Chat application, such as WhatsApp, Telegram or Signal 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or delivery to my home or business.....09
Some other way (Specify: _____).....10

Could you elaborate on your answer?
Provide more details on how you first found out.

Here are the categories I just read to you (Share your screen and display showcard #1 to R). How did these categories fit when you were selecting an answer? Is there anything that we are missing?

ASK IF NOT ALREADY ASKED
What does 'Social Media' mean to you?
Could you give some examples?
What does 'Chat application' mean to you?

ASK IF NOT ALREADY ASKED
When answering this question, what did 'Social Media' mean to you? Give a few examples

ASK IF NOT ALREADY ASKED
How does 'Social Media' differ from "Website or other internet applications"

S3b. Did you provide the money using cryptocurrency?

YES 01
NO 02

ASK IF NOT ALREADY ASKED
Many people are not familiar with cryptocurrency.
What does this mean to you?

S4. [Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you paid money to get a job or get into a business opportunity but were tricked or lied to about how the money would be used or what you would receive in return?

Yes 01
No .....02 (Skip to S5)

S4a. How did you first find out about paying the money to get a job or get into a business opportunity?

Someone told me on a phone call 01
A text message 02
The TV, radio or a newspaper.....03
Social media.....04
Website 05
Chat application, such as WhatsApp, Telegram or Signal 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or delivery to my home or business.....09
Some other way (Specify: _____).....10

Could you elaborate on your answer?
Provide more details on how you first found out.

Here are the categories I just read to you (Share your screen and display showcard #1 to R). How did these categories fit when you were selecting an answer?
Is there anything that we are missing?

ASK IF NOT ALREADY ASKED
What does 'Social Media' mean to you? Could you give some examples?
What does 'Chat application' mean to you?

ASK IF NOT ALREADY ASKED
When answering this question, what did 'Social Media' mean to you? Give a few examples

ASK IF NOT ALREADY ASKED
How does 'Social Media' differ from "Website or other internet applications"

S4b. Did you provide the money using cryptocurrency?

YES 01
NO.....02

ASK IF NOT ALREADY ASKED
Many people are not familiar with cryptocurrency.
What does this mean to you?

S5. **[Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you invested money with a person or company that tricked you or lied to you about what you would receive, such as promising a guaranteed return on your investment or that you would not lose any money?**

Yes 01
No.....02 (Skip to S6)

S5b. **How did you first find out about investing with the person or company?**

Someone told me on a phone call 01
A text message 02
The TV, radio or a newspaper.....03
Social media.....04
Website 05
Chat application, such as WhatsApp, Telegram or Signal 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or delivery to my home or business.....09
Some other way (Specify: _____).....10

Could you elaborate on your answer? Provide more details on how you first found out.

Here are the categories I just read to you (Share your screen and display showcard #1 to R). How did these categories fit when you were selecting an answer? Is there anything that we are missing?

ASK IF NOT ALREADY ASKED
What does 'Social Media' mean to you? Could you give some examples?
What does 'Chat application' mean to you?

ASK IF NOT ALREADY ASKED
When answering this question, what did 'Social Media' mean to you? Give a few examples

ASK IF NOT ALREADY ASKED
How does 'Social Media' differ from "Website or other internet applications"

S5b. **Did you provide the money using cryptocurrency?**

YES 01
NO.....02

ASK IF NOT ALREADY ASKED
Many people are not familiar with cryptocurrency.
What does this mean to you?

S6. **[Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you paid for any products or services that you NEVER received or that turned out to be a SCAM?**

Yes 01
No.....02 (Skip to S7)

6a. **How did you first find out about purchasing the product or service?**

Someone told me on a phone call 01
A text message 02
The TV, radio or a newspaper.....03
Social media.....04
Website 05
Chat application, such as WhatsApp, Telegram or Signal 06
Someone told me in-person 07
From an email I received 08
From material I received in the mail or delivery to my home or business.....09
Some other way (Specify: _____).....10

Could you elaborate on your answer?
Provide more details on how you first found out.

Here are the categories I just read to you (Share your screen and display showcard #1 to R). How did these categories fit when you were selecting an answer?
Is there anything that we are missing?

ASK IF NOT ALREADY ASKED
What does 'Social Media' mean to you?
Could you give some examples?
What does 'Chat application' mean to you?

ASK IF NOT ALREADY ASKED
When answering this question, what did 'Social Media' mean to you?
Give a few examples

ASK IF NOT ALREADY ASKED
How does 'Social Media' differ from "Website or other internet applications"

S6b. **Did you provide the money using cryptocurrency?**

YES 01
NO.....02

ASK IF NOT ALREADY ASKED

Many people are not familiar with cryptocurrency.
What does this mean to you?

S7. **[Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you donated, sent, or otherwise given money to someone who PRETENDED to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be?**

Yes 01
No.....02 (Go to Race/ethnicity)

S7a. Which ONE of the following BEST DESCRIBES how you were first contacted by this person?

Through a chat application such as WhatsApp, Telegram, or Signal.....01
Through a dating app 02
Through social media such as Facebook, TikTok, Instagram, or LinkedIn.....03
Through a website 04
In an email 05
By a text message.....06
By a phone call.....07
Some other way (Specify: _____).....08

Could you elaborate on your answer?
Provide more details on how you first found out.

Here are the categories I just read to you (Share your screen and display showcard #2 to R). **How did these categories fit when you were selecting an answer?**
Is there anything that we are missing?

ASK IF NOT ALREADY ASKED

What does 'Social Media' mean to you?

Could you give some examples?

What does 'Chat application' mean to you?

ASK IF NOT ALREADY ASKED
When answering this question, what did 'Social Media' mean to you? Give a few examples

ASK IF NOT ALREADY ASKED
How does 'Social Media' differ from "Website or other internet applications"

S5b. Did you provide the money using cryptocurrency?

YES 01
NO 02

ASK IF NOT ALREADY ASKED
Many people are not familiar with cryptocurrency.
What does this mean to you?

Race and Ethnicity Questions

THREE ALTERNATIVES: ONE ALTERNATIVE WILL BE TESTED IN EACH COGNITIVE INTERVIEW. RESPONDENTS WILL BE RANDOMLY ASSIGNED TO ONE OF THE THREE ALTERNATIVES.

Option 1
Next I am going to ask you questions about the race and ethnicity of each person who lives in your household. I will ask about each person, starting with you. You do not have to use the names of the person, you can use nicknames, initials or just refer to each individual as 'person 1', 'person 2', etc…

First, how many people live in your household, including any babies or small children?

Number _____

Before we start, can you tell us what you think of when you hear "race and ethnicity"?

Just tell us whatever jumps into your head.

ASK FOR THE FIRST THREE PERSONS

R1. What is (your/Person #) race and/or ethnicity? Select all that apply.

Is it…

American Indian or Alaska Native	01	01	01
Asian	02	01	01
Black or African American	03	01	01
Hispanic or Latino	04	01	01
Middle Eastern or North African	05	01	01
Native Hawaiian or Pacific Islander	06	01	01
White	07	01	01

If American Indian or Alaska Native ask:

R1aa. You said you were American Indian or Alaska Native. Which of the following are you? Select all that apply.

Navajo Nation	01	01	01
Blackfeet Tribe of the Blackfeet Indian Reservation of Montana	02	01	01
Native Village of Barrow Inupiat Traditional Government	03	01	01
Nome Eskimo Community	04	01	01
Aztec	05	01	01
Maya	06	01	01
Other	07	01	01

Specify

_____

If Asian ask:

R1ba. You said (you are/Person # is) Asian. Which of the following are you? Select all that apply.

Chinese	01	01	01
Asian Indian	02	01	01
Filipino	03	01	01
Vietnamese	04	01	01
Korean	05	01	01
Japanese	06	01	01
Other	07	01	01

Specify

_____

If Black or African American ask:

R1ca.You said (you are/Person # is) Black or African American. Which of the following are you? Select all that apply.

African American	01	01	01
Jamaican	02	01	01
Haitian	03	01	01
Nigerian	04	01	01
Ethiopian	05	01	01
Somali	06	01	01
Other	07	01	01

Specify

_____

If Hispanic or Latino ask:

R1da. You said (you are/Person # is) Hispanic or Latino. Which of the following are you? Select all that apply.

Mexican	01	01	01
Puerto Rican	02	01	01
Salvadoran	03	01	01
Cuban	04	01	01
Dominican	05	01	01
Guatemalan	06	01	01
Other	07	01	01

Specify _____

If Middle Eastern ask:

R1ea. You said (you are/Person # is) Middle Eastern or North African. Which of the following are you? Select all that apply.

Lebanese	01	01	01
Iranian	02	01	01
Egyptian	03	01	01
Syrian	04	01	01
Iraqi	05	01	01
Israeli	06	01	01
Other	07	01	01

Specify _____

If Native Hawaiian or Pacific Islander ask:

R1fa. You said (you are/Person # is) Native Hawaiian or Pacific Islander. Which of the following (are you/is Person #)? Select all that apply.

Native Hawaiian	01	01	01
Samoan	02	01	01
Chamorro	03	01	01
Tongan	04	01	01
Fijian	05	01	01
Marshallese	06	01	01
Other	07	01	01

Specify _____

If White ask:

R1ga. You said (you are/Person # is) White. Which of the following are you? Select all that apply.

English	01	01	01
German	02	01	01
Irish	03	01	01
Italian	04	01	01
Polish	05	01	01
Scottish	06	01	01
Other	07	01	01

Specify

_____

DEBRIEF FOR RACE/ETHNICITY OF RESPONDENT

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that you are "<Major Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What about reading all of the categories to you. What did you think about that?

Why do you think we read all the categories?

DEBRIEF ABOUT THE DETAILED RACE CATEGORIES - SCROLL BACK OVER THE CATEGORIES FOR THE RESPONDENT AND READ A FEW ALOUD. GET THE RESPONDENT TO ATTEND TO THEM.

You said you are "<Detailed Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What do you think of the race descriptions relating to the country of origin? How did you use them when answering the question?

(IF DID NOT USE EXAMPLES) Do the categories relating to the country of origin represent who you feel you are? Why or why not?

What makes you say that? Can you say more about that?
ADMINISTER R1 TO R1GA FOR UP TO TWO OTHER HOUSEHOLD MEMBERS.

OK, now let's' turn to [PERSON #] in your household.

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that Person # is "<Major Race>" How did you arrive at your answer?

What is the relationship of Person # to you (spouse, child, cousin, unrelated)

What about reading all of the categories to you? What did you think about that? Why do you think we read all the categories?

How do you know their background?

Option 2
Next I am going to ask you questions about the race and ethnicity of each person who lives in your household. I will ask about each person, starting with you. You do not have to use the names of the person, you can use nicknames, initials or just refer to each individual as 'person 1', 'person 2', etc…

First, how many people live in your household, including any babies or small children?

Number _____

Before we start, can you tell us what you think of when you hear "race and ethnicity"?

Just tell us whatever jumps into your head.

ASK FOR THE FIRST THREE PERSONS

R2. What is (your/Person #) race and/or ethnicity?

R2a. Is it American Indian or Alaska Native?

For example Navajo Nation, Blackfeet Tribe of the Blackfeet Indian Reservation of Montana, Native Village of Barrow lnupiat Traditional Government, Nome Eskimo Community, Aztec, Maya, etc.

YES	01	01	01
NO	02	01	01

R2b. Is it Asian?

For example, Chinese, Asian Indian, Filipino, Vietnamese, Korean, Japanese, etc.

YES	01	01	01
NO	02	01	01

R2c. Is it Black or African American?

For example, African American, Jamaican, Haitian, Nigerian, Ethiopian, Somali, etc.

YES	01	01	01
NO	02	01	01

R2d. Is it Hispanic or Latino?

For example, Mexican, Puerto Rican, Salvadoran, Cuban, Dominican, Guatemalan, etc., etc.

YES	01	01	01
NO	02	01	01

R2e. Is it Middle Eastern or North African?

For example, Lebanese, Iranian, Egyptian, Syrian, Iraqi, Israeli, etc.

YES	01	01	01
NO	02	01	01

R2f. Is it Native Hawaiian or Pacific Islander?

For example, Native Hawaiian, Samoan, Chamorro, Tongan, Fijian, Marsha/Iese, etc

YES	01	01	01
NO	02	01	01

R2g. Is it White?

For example, English, German, Irish, Italian, Polish, Scottish, etc.

YES	01	01	01
NO	02	01	01

If American Indian or Alaska Native ask:

R2aa. You said (you are/Person # is) American Indian or Alaska Native. Which of the following (are you/is Person #)? Select all that apply.

Navajo Nation	01	01	01
Blackfeet Tribe of the Blackfeet Indian Reservation of Montana	01	01	01
Native Village of Barrow Inupiat Traditional Government	03	01	01
Nome Eskimo Community	04	01	01
Aztec	05	01	01
Maya	06	01	01
Other	07	01	01

Specify

_____

If Asian ask:

R2ba. You said (you are/Person # is) Asian. Which of the following (are you/is Person #)? Select all that apply.

Chinese	01	01	01
Asian Indian	02	01	01
Filipino	03	01	01
Vietnamese	04	01	01
Korean	05	01	01
Japanese	06	01	01
Other	07	01	01

Specify

_____

If Black or African American ask:

R2ca. You said (you are/Person # is) Black or African American. Which of the following (are you/is Person #)? Select all that apply.

African American	01	01	01
Jamaican	02	01	01
Haitian	03	01	01
Nigerian	04	01	01
Ethiopian	05	01	01
Somali	06	01	01
Other	07	01	01

Specify

_____

If Hispanic or Latino ask:

R2da. You said (you are /Person # is) Hispanic or Latino. Which of the following (are you/is Person #)? Select all that apply.

Mexican	01	01	01
Puerto Rican	02	01	01
Salvadoran	03	01	01
Cuban	04	01	01
Dominican	05	01	01
Guatemalan	06	01	01
Other	07	01	01

Specify

_____

If Middle Eastern ask:

R2ea. You said (you are/Person # is) Middle Eastern or North African. Which of the following (are you/is Person #)? Select all that apply.

Lebanese	01	01	01
Iranian	02	01	01
Egyptian	03	01	01
Syrian	04	01	01
Iraqi	05	01	01
Israeli	06	01	01
Other	07	01	01

Specify

_____

If Native Hawaiian or Pacific Islander ask:

R2fa. You said (you are/Person # is) Native Hawaiian or Pacific Islander. Which of the following (are you/is Person #)? Select all that apply.

Native Hawaiian	01	01	01
Samoan	02	01	01
Chamorro	03	01	01
Tongan	04	01	01
Fijian	05	01	01
Marshallese	06	01	01
Other	07	01	01

Specify _____

If White ask:

R2ga. You said (you are/Person # is) White. Which of the following (are you/is Person #)? Select all that apply.

English	01	01	01
German	02	01	01
Irish	03	01	01
Italian	04	01	01
Polish	05	01	01
Scottish	06	01	01
Other	07	01	01

Specify

_____

DEBRIEF FOR RACE/ETHNICITY OF RESPONDENT

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that you are "<Major Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What about reading all of the categories to you. What did you think about that?

Why do you think we read all the categories?

DEBRIEF ABOUT THE DETAILED RACE CATEGORIES - SCROLL BACK OVER THE CATEGORIES FOR THE RESPONDENT AND READ A FEW ALOUD. GET THE RESPONDENT TO ATTEND TO THEM.

You said you are "<Detailed Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What do you think of the race descriptions relating to the country of origin? How did you use them when answering the question?

(IF DID NOT USE EXAMPLES) **Do the categories relating to the country of origin represent who you feel you are? Why or why not?**

What makes you say that? Can you say more about that?

ADMINISTER R2 TO R2GA FOR UP TO TWO OTHER HOUSEHOLD MEMBERS.

OK, now let's' turn to [PERSON #] in your household.

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that Person # is "<Major Race>" How did you arrive at your answer?

What is the relationship of Person # to you (spouse, child, cousin, unrelated)

What about reading all of the categories to you? What did you think about that? Why do you think we read all the categories?

How do you know their background?

Option 3

R3.Next I am going to ask you questions about the race and ethnicity of each person who lives in your household. I will ask about each person, starting with you. You do not have to use the names of the person, you can use nicknames, initials or just refer to each individual as 'person 1', 'person 2', etc…

First, how many people live in your household, including any babies or small children?

Number _____

Before we start, can you tell us what you think of when you hear "race and ethnicity"?

Just tell us whatever jumps into your head.

ASK FOR THE FIRST THREE PERSONS

What is (your/person #) race and/or ethnicity? You can select more than one category.

R3a. Is it American Indian? For example, Navajo Nation, Blackfeet Tribe of the Blackfeet Indian Reservation of Montana, Native Village of Barrow Inupiat Traditional Government, Nome Eskimo Community, Aztec, Maya, etc…

YES	01	Go to R3aa	01 01
NO	02	Go to R3b	01 01

R3aa. Which of the following (are you/is person #)? Select all that apply

Navajo Nation	01	01	01
Blackfeet Tribe of the Blackfeet Indian Reservation of Montana	02	01	01
Native Village of Barrow Inupiat Traditional Government	03	01	01
Nome Eskimo Community	04	01	01
Aztec	05	01	01
Maya	06	01	01
Other	07	01	01

Specify

_____

R3b. Is it Asian?

YES .....01 Go to R3ba 01 01
NO .....02 Go to R3c 01 01

R3ba. Which of the following (are you/is person #)? Select all that apply

Chinese	01	01	01
Asian Indian	02	01	01
Filipino	03	01	01
Vietnamese	04	01	01
Korean	05	01	01
Japanese	06	01	01
Other	07	01	01

Specify

_____

R3c. Is it Black or African American?

YES .....01 Go to R3ca 01 01
NO .....02 Go to R3d 01 01

R3ca. Which of the following (are you/is person #)? Select all that apply

African American	01	01	01
Jamaican	02	01	01
Haitian	03	01	01
Nigerian	04	01	01
Ethiopian	05	01	01
Somali	06	01	01
Other	07	01	01

Specify

_____

R3d. Is it Hispanic or Latino?

YES .....01 Go to R3da 01 01
NO .....02 Go to R3e 01 01

R3da. Which of the following (are you/is person #)? Select all that apply

Mexican	01	01	01
Puerto Rican	02	01	01
Salvadoran	03	01	01
Cuban	04	01	01
Dominican	05	01	01
Guatemalan	06	01	01
Other	07	01	01

Specify

_____

R3e. Is it Middle Eastern or North African?

YES	01	Go to R3ea	01 01
NO	02	Go to R3f	01 01

R3ea. Which of the following (are you/is person #)? Select all that apply

Lebanese	01	01	01
Iranian	02	01	01
Egyptian	03	01	01
Syrian	04	01	01
Iraqi	05	01	01
Israeli	06	01	01
Other	07	01	01

Specify

_____

R3f. Is it Native Hawaiian or Pacific Islander?

YES	01	Go to R3fa	01 01
NO	02	Go to R3g	01 01

R3fa. Which of the following (are you/is person #)? Select all that apply

Native Hawaiian	01	01	01
Samoan	02	01	01
Chamorro	03	01	01
Tongan	04	01	01
Fijian	05	01	01
Marshallese	06	01	01
Other	07	01	01

Specify

_____

R3g. Is it White?

YES .....01 Go to R3fa 01 01
NO.....02 Go to debrief 01 01

R3ga. Which of the following (are you/is person #)?

English	01	01	01
German	02	01	01
Irish	03	01	01
Italian	04	01	01
Polish	05	01	01
Scottish	06	01	01
Other	07	01	01

Specify

_____

DEBRIEF FOR RACE/ETHNICITY OF RESPONDENT

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that you are "<Major Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What about reading all of the categories to you. What did you think about that?

Why do you think we read all the categories?

DEBRIEF ABOUT THE DETAILED RACE CATEGORIES - SCROLL BACK OVER THE CATEGORIES FOR THE RESPONDENT AND READ A FEW ALOUD. GET THE RESPONDENT TO ATTEND TO THEM.

You said you are "<Detailed Race>" How did you arrive at your answer? Is this information the respondent knows or were they guessing?

What do you think of the race descriptions relating to the country of origin? How did you use them when answering the question?

(IF DID NOT USE EXAMPLES) Do the categories relating to the country of origin represent who you feel you are? Why or why not?

What makes you say that? Can you say more about that?

ADMINISTER R3 TO R3GA FOR UP TO TWO OTHER HOUSEHOLD MEMBERS.

OK, now let's' turn to [PERSON #] in your household.

OBSERVE:

DID THEY INTERRUPT WHEN READING MAJOR CATEGORIES OR PARTS OF THE DETAILED RACE LISTS?

DID RESPONDENT HAVE THE KNOWLEDGE TO ANSWER THE QUESTIONS? IS THIS INFORMATION THE RESPONDENT KNOWS OR WERE THEY GUESSING? OBSERVE FOR BOTH MAJOR AND DETAILED RACE QUESTIONS

WHAT WAS THE OVERALL REACTION WHEN READING THE MAJOR CATEGORIES?

DID THEY OBJECT TO READING THEM ALL?

SHOW SIGNS OF ANNOYANCE?

You said that Person # is "<Major Race>" How did you arrive at your answer?

What is the relationship of Person # to you (spouse, child, cousin, unrelated)

What about reading all of the categories to you? What did you think about that? Why do you think we read all the categories?

How do you know their background?

Closing and Incentive

Those are all the questions I have for you. Is there anything we haven't discussed that you would like to mention?

DISCUSS ANY RESPONDENT COMMENTS. STOP RECORDER.

Before we finish, I just want to make sure you're doing ok. (REFER TO DISTRESS PROTOCOL IF NEEDED).

Here is some contact information for local and national organizations that you can call if you want to talk about any feelings or emotions you experience. (GIVE RESOURCE LIST TO R)

Your gift card will be sent to you using the same email that the scheduler used. Thank you for your time.

Appendix G

Cognitive Interview Protocol – Bias Motivated Crime

Appendix G
Cognitive Interview Protocol – Bias Motivated Crime

Hello, thank you for taking the time to talk with me today. My name is _____. I work for Westat, a research company in Rockville, Maryland. For this project, Westat is under contract with the Bureau of Justice Statistics (or BJS), to evaluate survey questions that collects data about certain crimes you may have experienced. The feedback from you and others will help us improve the survey.

Today we are going to follow-up with some of the information that you gave when we interviewed you the last time. We have sent you information about this interview and the conditions related to participating. I'll go over the main points related to participating.

What is involved: We will be asking you about your experience of certain crimes. The session will take about 10 minutes. When the interview has concluded, we will email you the digital gift card with $10 loaded on it. Your participation is voluntary; you can stop at any point and you can skip any question.

Confidentiality: BJS will protect and maintain the confidentiality of your personal information to the fullest extent under federal law. BJS, its employees, and its contractors (Westat staff) will only use the information provided for statistical or research purposes pursuant to 34 U.S.C. § 10134. All personally identifiable information collected under BJS's authority is protected under the confidentiality provisions of 34 U.S.C. § 10231. The law protects your answers from outside requests by any government agency, private organization or individual.

You will never be identified by name. The things you tell us may be put in a report, but there will be no way to identify who said what, and your name will not be used anywhere.

Risks: One possible risk is that some questions may upset you if you experienced an unwanted contact. At the end of the interview, you will receive telephone numbers for organizations that you can contact to get help.

Benefits: There are no direct benefits to you for participating in this study. However, you will be helping BJS improve the quality of the data collected.

Questions: If you have questions about the study, contact David Cantor at 301-294-2080 or davidcantor@westat.com. If you have questions about your rights and welfare as a research participant, please call the Westat Human Subjects Protections office at 1-888-920-7631. Please leave a message with your first name, the name of the research study that you are calling about (the National Crime Victimization Survey), and a phone number beginning with the area code. Someone will return your call as soon as possible.

Today, we will be asking you about one survey question and asking for your answers. We will then ask you what the question means to you and what your answer means. We will also ask you

questions about specific parts of the question. There are no right or wrong answers. We are interested in everything you have to say. The information that you give us will help us improve the survey. So that you can speak freely about your experiences, I would recommend that you find a private area to participate in our interview today. At the end of the interview, we will email you a list of national organizations that you can call if you want to talk about any feelings or emotions you experience during the interview.

Request

Do you have any questions about anything I just went over?

Finally, because I want to pay close attention to what you say, I would like to record our interview so that we can have an accurate record of what you say while writing our report. Is that okay?

- [UPDATE RESPONDENT ZOOM NAME TO THEIR PARTICIPANT ID]
- [IF REFUSES RECORDING, END INTERVIEW]

Okay great, I'll start recording [START ZOOM RECORDING – TO CLOUD], and I need to ask your permission one more time so that it is recorded. Today is [mo/day/year] at [time]. Do you agree to participate in this interview and to have it recorded?

Interview Protocol

We want to ask you one question about the incident that you reported at our last interview. After I ask the question, I'll follow-up with a few questions about your answer.

You may find the question a little repetitive based on what you already told me at our last interview. But we still want to get your reactions to the question. It will help us design the question for other people who are in your situation.

Last time you told me that: "Fill in situation from last time"

The next question is about why the offender may have targeted you.
The reason may have been prejudice or bigotry toward those with your characteristics or religious beliefs, even if the offender mistakenly thought you had those characteristics or beliefs. This kind of reason is different from just being angry or wanting to get something from you.

Do you think the offender was targeting you because of prejudice or bigotry toward your race/ethnic background, your religion, your disability, your sexual orientation, your sex or any other of your personal characteristic?

Yes..... 01
No..... 02

Probes:
Opening probe: Could you tell me more about your answer?
<u>If no and not already answered</u>
What type of incident do you think this question is asking about? Can you give me a few examples?
What does 'targeting you because of prejudice or bigotry" mean to you?
How would you know if you were targeted in this way?
[*interviewer instruction: if you think this could have been a hate crime ask*] Do you think this was a hate crime? Can you tell me more about your answer?
<u>If yes and not already answered</u>
Could you tell me what type of prejudice or bigotry the offender had toward you?
What leads you to believe you were targeted in this way?
Do you think this was a hate crime? Can you tell me more about your answer? What do you think of when you hear 'hate crime'?
<u>Ask everyone</u>
The question asks about "targeting you because of prejudice or bigotry toward your race/ethnic background, your religion, your disability, your sexual orientation, your sex or any other of your personal characteristic?"

In your mind, what does targeting someone because of their sex mean to you?
What do you think 'other personal characteristic' refers to? Can you give a few examples?

Closing and Incentive

Those are all the questions I have for you. Is there anything we haven't discussed that you would like to mention?

DISCUSS ANY RESPONDENT COMMENTS. STOP RECORDER.

Before we finish, I just want to make sure you're doing ok. (REFER TO DISTRESS PROTOCOL IF NEEDED).

Here is some contact information for local and national organizations that you can call if you want to talk about any feelings or emotions you experience. (GIVE RESOURCE LIST TO R)

Your gift card will be sent to you using the same email that the scheduler used. Thank you for your time.

Appendix H

Notes from the Cognitive Interviews

Appendix H
Notes from the Cognitive Interviews

Detailed Notes for Stalking Cognitive Interviews

Sq1g (Phone).

Now I want to ask about unwanted contacts or behaviors using various technologies, such as your phone, the Internet, or social media apps. Again, please DO NOT include bill collectors, solicitors, or other sales people. In the past 12 months… Has anyone made unwanted phone calls or left voice messages excessively to contact you?

Responses: **No (11) Yes (14)**

- Out of the 14 "yes" responses:
  - Six described spam, phishing and fraudulent activity
    - "*People keep calling a lot, excessively - different numbers… spam*."
    - After a probe from the I: "*Well, if you said exclude solicitors, because again, I don't know, I would say yes. I have received them because I think they're scams*." << this R excluded sales but included phishing
  - Four individuals described calls from ex partners
  - Three described contacts from those who had unrequited interest in the respondent, and
  - One described an assault and subsequent stalking (including cyber) by a stranger
- Out of the 11 "no" responses
  - Examples of answers to the probe include:
    - *"It just means that you're constantly trying to call me, and I'm not interested."*
    - *"Because I don't think anybody has."*
    - *"Excessively. That's the operative word. You have to listen very carefully to that question on. Well, well, 1st of all, it, those sorts of things did not happen at all, let alone excessively."*
- Most seemed to have a definition for "excessive" – some gave large amounts, some gave small amounts, some said it would depend.
  - *"For me once, I tell you now, once you understand, once we have an agreement, when our understanding, where we are in our relationship. One time past is too many."*
  - *"In this context, I think even one is excessive, because I don't believe it should be happening."*
  - *"4 or 5 voicemails."*

- *"Excessive is like, I don't know, somewhat unnatural like for somebody to call you 50 times in 1 minute"*
- *"I don't know that I could put a number on it. Maybe, if a call happens from the same number more than once a day. Possibly I don't know."*

SQ1g1 (Text).

Has anyone sent excessive unwanted text messages to contact you?

Responses: No (12) Yes (13)

- Out of the 13 "yes" responses:
  - Five described spam, phishing and fraudulent activity
    - "*Again it comes down to to spam. I've had several local political text messages. mostly from outfits that I agree with, but I still don't want to see them as text messages.*"
    - *"I could get a text message, and I'll unsubscribe for it, and then I'll turn around and I'll get another text message from a whole another company. But it's the same company."*
  - Three individuals described texts from ex partners
  - Three described contacts from those they had unrequited interest in – but unclear whether BJS wants only SMS messaging at this question or whether other messaging counts (e.g., Facebook messenger)…
    - "*It's on Facebook and Instagram, you know. Those are the 2 places that I get a lot of excessive, you know, messages where I don't want to talk to them, and they just keep trying to talk to me, and then pretty soon I have to block them and restrict them..* "
  - One mentioned a single text threat
    - *"I had a couple. One was a threat and the other one was just different stuff. And that's it."*
  - One described harassment from a former friend
- Out of the 12 "no" responses
  - Respondents seemed to have an accurate interpretation of the question

o Most seemed to have a definition for "excessive" – some gave large amounts, some gave small amounts, some said it would depend.

- One respondent said after the person is "*told no more*" any additional texts would be excessive
- *"Too many.. I'll say 10."* Another suggested 20, another said 25. Others suggested 3-4, or 6-7.
- *"Someone who texts me every 3 mins, even if even at nighttime, when I am in bed. Constantly at inappropriate times. That's excessive."*

SQ1h and SQ1h1 (Email).

Version 1:

SQ1h. Has anyone sent you unwanted messages using email, social media apps, dating apps or other internet platforms and applications?

Version 2:

SQ1h1. Has anyone sent you unwanted messages using email, social media apps, or other internet applications like WhatsApp, SnapChat, Instagram, Twitter (X), YouTube, Facebook or TikTok?

Responses:

SQ1h: No (4) Yes (8)
SQ1h1: No (5) Yes (7) Missing (1)

- Out of the 15 "yes" responses:
  - Five described phishing and potential fraudulent activity
    - *"I mean, there's a spam folder is full every day with a couple of dozen lots of nonsense."*
    - *"A recent one is the scam where they are.. sending you an email to tell you they've hacked your system, and they've gained compromising information or photographs about you. And if you don't send the most recent one said $2,000 worth of Bitcoin, they're going to expose it to everyone in your contacts."*
    - *[Scam where emailer claims] "a package [has] been left at the post Office"*
  - Some did not provide sufficient information to determine whether it could be a false positive or not
    - *"Yes, through Facebook messenger and also through Snapchat."*
    - *"Yes, on WhatsApp, yeah, but not on email..Instagram, definitely..on Instagram and Facebook."*
  - Some "yes" responses did go beyond just phishing scams:
    - A few reported exes and people who were interested in them romantically
    - Two reported being the victim of bullying/harassment behavior (one from a stranger, the other from a known offender)

- Examples of "no" responses:
    - "I probably do a good job of limiting that because I keep my circle of friends in the social media world small."
    - "Unwanted that that not really. I had a I had a an online argument, but that doesn't count. That was with my brother-in-law's brother. But yeah, that's not. I just unfriended him, that was all, but nothing else. No."
    - "That's kind of a weird one. I mean I don't know how to answer that. No is no."
    - "I can't think of anything right now. No, nothing"
- Version 1: Examples of what 'unwanted messages' mean:
    - Generally respondents had an idea of what "unwanted" meant to them – examples:
        - *"I told you stop messaging me, and I meant that, and you keep doing it."*
        - *"If you ask them to stop and not do it, and they continuously to do it. Then that's unwanted."*
        - *"It means I didn't want to. I never written them."*
        - *"if you ask them to stop and not do it, and they continuously to do it. Then that's unwanted"*
- Examples of what 'dating apps' means:
    - *"A dating app means a site where you go to meet potential … companions."*
    - *"Tinder, Hinge those kinds of things."*
    - *"I'm not on any at the moment, but I met my present wife through a dating app. So yeah, dating apps are very familiar, and I suppose they can become threatening or unwanted."*
    - *"Dating apps are very dangerous. I wouldn't go on them."*
- Examples of 'other internet platforms and applications' included**:**
    - Version 1 Question (SQ1h)
        - Most respondents who heard version 1 of the question were able to list examples:
            - "Facebook, Instagram. TikTok. There's a new one called Thread."
            - "Instagram, Snapchat, and X"
        - Out of the 12 version 1 respondents, three could not come up with any examples.

- Version 2 Question (SQ1h1)
  - This probe proved trickier for the version 2 respondents because they couldn't think of anything beyond the examples already provided:
    - *"I have no idea. I don't know what they mean by other."*
  - Some just reiterated the examples already provided in the question. Two respondents were able to come up with examples not included in the question (Reddit and Google Chat and Google Meet were provided as additional examples).

SQ1i (Spy Tech).

Has anyone spied on you using technologies such as a listening device, camera, or video recorder?

Responses: No (17) Don't know (2) Yes (6)

- Out of the 6 "yes" responses:
  - One respondent who answered "no" reported that their neighbor has a camera pointed at his home. They know the neighbor watches the recordings because they have mocked some things that the R's family has done (within view of the camera). The R answered "no" here because he did not count this as "spying" since the camera is out in the open.
  - A respondent who answered "yes" seemed to be talking about Facebook (the company) recording conversations.
  - We spoke with a respondent who believed his phone is being tapped (*we suspect this particular respondent may not be reliable – he had quite a few unlikely claims*).
  - Two respondents reported being recorded without their awareness by a current or former partner.
  - Another described a landlord putting cameras in her home without her permission. (She was aware the cameras were there – they were not hidden.)
  - A final respondent has very minimal evidence: R explained her phone did some weird things a few times. In the middle of a call it sounds like they had someone on hold -- there was a beep.
- Many of the respondents who answered this as "no" responded said they couldn't be certain – when asked "How they arrived at their answer" respondents said:
  - *"Not that I know of. I've never had that before."*
  - *"Not that I know of"*

- *"I read about people who've been spied on people who've been arrested for those things. So technically, yes, I could have gone into a dressing room. I could have gone into the airport bathroom. and if it didn't make video or I didn't see the little hole in the wall. I have no clue"*
- *"No, not that I know of. "*
- *"at least to the best of my knowledge, I'm you know, this. This is when this sort of thing happens to you. There, there are a lot of things that you don't know. I'm I'm willing to bet, and I I would I would, you know, not not concede that that perhaps someone has been watching me in some way, but but maybe not with an actual device. You just don't know"*
- *"Just gonna say, not that I'm aware of. "*
- *"I suppose you can't be 100% certain that somebody has got a long way to spin photo lens, or, you know, crowding around the house. You don't see them"*

- Examples given of spying that aligned with the question:
  - A few mentioned a Nanny Cam.
  - *"Cameras audio, like recording machines. Cause I know where I live. I rent a room from someone. and she has the whole camera thing set up in her house and cameras around her whole house. So I know she can see who comes in and out"*
  - One respondent celebrities and paparazzi as an example.
  - *"I think that some people have cameras on people to see if they're you know, to stalk them..if someone's spying on you and they're stalking you."*
  - *"As in like hidden cameras, or like hidden listening devices… my phone being tapped"*
- Examples that did NOT align with the question:
  - *"I mean, they could spy on you on Facebook. They could spy on you. you know, looking in your windows, or, you know, going around your neighborhood that type of thing if you I don't work. But, you know, showing up at your workplace now, there's many ways they can spy on you without you, potentially knowing."*
  - *"I would imagine that someone in a bad relationship going through a a possessive partner and then putting air pods in their property or on their vehicle, or a GPS device on their vehicle, something like that."*
  - *"Spying would be watching the house when I'm coming and going"*
  - *"Like hacking into your accounts and following you"*
  - *"I think spying has to do a lot with the government, or you have to have that type of job or that type of licenses. Because my thing is, why would you spy on somebody if you're not getting paid for it? If you're not legally have a contract to do so, it's an invasion of people's privacy."*

SQ1i1 (PC Monitored).

Has anyone spied on you using computer or cell phone monitoring software?

Responses: No (20) Don't know (2) Yes (3)

- There were two don't know responses. One respondent said they were unaware of this happening but it was possible. The second respondent said she didn't know but it was possible because her ex boyfriend (who had lived there) was very tech savvy: "*They're the one who installed everything because we used to live together … then, when we separated, I never like checked… But it would be weird, because he would sometimes know things that he wouldn't know unless he was able to look through my technology, because I would look stuff up online. And then he would say, 'Oh, you went here today. And I would be like. that's kind of weird, because I only looked that up, you know, so.'* "
- The three 'yes' responses included:
  - One sited the "beep" she heard on her telephone. In the middle of a call, it sounded like they had someone on hold -- there was a beep.
  - One was the respondent who we think is unreliable (and provided no details beyond a "yes" response).
  - The third described an incident from 3 years ago (and so was out of scope). In this case the spying was a way to take her PII and hack into her bank accounts (fraud).
- After this probe was asked, most respondents who had initially answered "no" decided they wouldn't know if they were being monitored on in this way:
  - *A majority simply answered this probe as: "Not that I'm aware of."*
  - *"If they're spying on you, how would you even know? Once again. you know, I don't know. That's kind of vague. Again."*
  - *"Again. I'd have to say if it happens, it's unbeknownst to me. I don't believe it's happened. But again, you know, I've watched the 2020 reports where they say your television can they have can monitor you just like you yourself, you know. And when I click on this. Are you still able to monitor me after you know the Zoom Meeting is over, so I have no idea."*
  - *"Nowadays you can never really be too sure."*
- One seemed confident they were not being monitored:
  - *"No, I scan my device on a regular basis for our recently installed apps"*
- One respondent described fraud (unrelated to the question):
  - *"I'm pretty good at spotting phishing emails as well like we've had to do a couple of seminars at work about them. I know the spelling errors to look for in the language and the little things at the bottom of the page, and stuff like that."*

- Respondents seemed to understand what 'computer or cell phone monitoring software
    - One R defined this as "*a program designed to either infiltrate or run behind the scenes*"
    - Another R described an incident that happened to his roommate: *"Under the guise of being technical support. [My roommate] responded to a spam email and they phoned the number listed in email. And they talked him into downloading a remote access program. And they had access to his device. ...He noticed this because there were changes made to his email account that he had not made, and I became aware of it. and I helped him get backed out of it before any more harm had been done"*
    - One R said perhaps a webcam installed on a phone, and then the victim could be watched every second – perhaps they could also look at her texts and bank account.
    - One respondent mentioned a "listening bug"
    - One response did not align with the question: this respondent mentioned

SQ1j (Tracking).

Has anyone tracked your whereabouts with an electronic tracking device or application, such as GPS, an e-tracker, or an application on your cell phone?

Responses: No (20) Yes (5)

- Two were "willingly" or at least knowingly tracked (e.g., Life 360 App, "Find" apps) – one younger respondent answered "no" but mentioned that his family members are able to track him. And another respondent answered "yes" with the caveat that it is with her "consent."
- Three who answered "yes" do not align with the question content:
    - One reported a qualifying incident but it was probably not within the past 12 months: *"I think they have in the past, but not recently..I think that it was probably somebody that was..had got maybe my information or something, and they were, it might have been an old boyfriend that did that."* << note: it is very likely that respondents were forgetting that we were asking about "the past 12 months."
    - One respondent described something that does not fit the question: *"I have had that happen I've had like in the midst of me, taking like a survey I've had. It came up that my stuff was being tracked, and it was sent to other companies."*
    - And the third respondent is the one who we think is unreliable.
- One "yes" response fits the question intent because permission was not given:
    - One respondent described being tracked (presumably by family members) but she did not give her permission to be tracked.
- Respondents who had answered "no":
    - Similar to the prior question, some admitted they would not actually know:
        - *"Between you, me and hold the wall. Since we're being recorded, everybody else. once a Marine, always Marine, but I'm a former Marine. I love my country. So let's get that right up front. But it doesn't mean, I trust, my government per se. And you know, especially since the whole the bush administration with, you know. Oh, we're not tapping our phones. Oh, we are tapping our phones! There was a matter of, and all of a sudden they have laws on the National security where they're allowed to. So there's the answer. I guess I wouldn't know if they did. Let's hope not."*
        - *You wouldn't know. Unless it became obvious.*

        - *If the if it has happened, I'm not aware of it.*
    - Others were more confident that it had not happened to them:
        - *"I monitor the apps that are installed on my phone, and there would have to be something that would be visible. And there has not been."*
        - *"I never experienced GPS tracking. I mean the person that I was with always wanted to know my whereabouts, but never like asked me for my location or asked me, for I think it's what they call it nowadays air tag, or something like that for iphones, so I never had to go through that experience with her. So you know, it was more like, call me, where are you at? Or text me your location, you know. I have an android phone. So I'm able to ping ping my location to the person. But I never had to like go through any of that with her."*
        - One respondent said he keeps his location off at all times in case someone could be tracking him without his knowledge.
        - *"always have my phone. Nobody uses my phone, has my phone. My phone has a lock on it. So I think they would have to have some kind of if they're gonna put something like that on my phone, they would have to have in possession of my phone."*
        - *"I'm unaware of anything like that occurring. There's no reason for me to suspect that, or be suspicious of that."*
    - One respondent correctly focused on the word "unwanted": "*if you're saying unwanted, I'll say no, or if you're saying that I was aware of then. Yes."*
    - Two respondents may have missed the intention of this question:
        - *"No, I don't have a car."*
        - *"I just don't think anybody would have any reason to. And I'm I'm pretty careful with where I share my data, especially credit card and social security and stuff like that."*

- Respondents generally understood what ‘tracked your whereabouts’ meant:
    - *“It's the same thing as when you access your location on your computer. You know, if someone has to be. You know, I'm in the second floor of my townhouse, you know. Specifically, yeah. You know, I'm in this city. You know, this area code within this proximity of this cell tower, whatever it might be.”*
    - *"Where I am at any particular time, or where my car is, if I'm in my car. Yeah, that's that's straightforward."*
    - *“Like a chip or… a little GPS thing on your car, or something of that nature to track your whereabouts… or getting into your Google, where they can share your location or something like that.”*
- A significant number of respondents were not familiar with ‘e-tracker’
    - Many said they had not heard the term “e-tracker” before. Some respondents posited a guess:
    - *"keeping track of how, where you, how, what distance you run is that? That's what I would consider a e-tracker like a Fitbit or Garmin."*
    - *"I don't really have an answer for that, because I would assume it might be something like a sim that you could use to test another phone service provider. And that would imply. maybe software. But that one's not clear to me at all, I would not know."*
    - *"I assume it means electronic tracker. I would assume again, this is just opinion is that it's the same device as any any tracking device.”*

SQ1k and SQ1k1 (Social Media).

Version 1:

SQ1k. Has anyone monitored or observed your activities on social media apps like Facebook, TikTok, YouTube, Instagram, Twitter (X), or LinkedIn?

Version 2:

SQ1k1. Has anyone monitored or observed your activities on social media apps, discussion forums, or other social networking platforms or apps?

Responses:

SQ1k: No (4) Yes (8)
SQ1k1: No (8) Yes (5)

- Most people had a clear understanding of "social media" apps:
    - *"So to me, when I think of that, I think of Reddit, which is where you have various sub forums based on various topics where people discuss issues related to that topic."*
    - *"Facebook TikTok Instagram, reddit."*
    - *"Facebook, Twitter, Snapchat"*
    - *"They mean to me an environment where I can share my opinions and my input on different topics."*
- Most understood what 'being monitored or observed' meant. They thought of this in terms of how social media might be involved:
    - R thinks it is a continuous thing, like someone is constantly checking in on your social media pages. This is different from just viewing or interacting with something you post on TikTok or Instagram. If they liked what you posted, they could follow you and consistently engage with your content, but that seems less malicious.
    - *" if I were participating in that public forum in some way making comments or or doing something that they would pay attention to that. Know who did it, you know. Well, he said, this then, and that sort of thing. I mean, people are free to do these things. you know, if if they wish, I mean I you know what I can't stop them. "*
    - *" it means like they just if you posted something they're able to see what you posted. if you like certain things like, for example, Instagram. That's where I would say I've that's where I caught him. He could watch my reels like if I interacted with certain reels about the relationship through TikTok he could go through my reposts to see if I was feeling emotional about the situation, or like how my thoughts were being projected."*
    - *"They're monitoring me by what they're saying in their post. They're talking about things that only a person who is closely watching. You would know. Then they use the phrase discussion, forums, or other social networking platforms or apps. "*
- Out of the 13 'yes' responses, there are three that were clearly on target– one from the version 1 screener, two from version 2:
    - *"Yes, that ex-boyfriend that's been kind of stalking me. Yeah. He found me on Facebook, and I blocked him. But yeah." "Well, he just posted this like a picture message to me. Kind of to show that was before. Yeah, before he started coming around kind of like, oh, here I am, you know. Yeah. that was kind of creepy."*
    - *"…there was somebody that just didn't like it, and began basically stalking me on there, creating different names to harass me. And what's scary is in one of their posts on the Forum. They put a partial part of my email address, and I have no idea how they could have gotten that. It was very scary. So I eventually got off of the platform. I'm not on there anymore, because it got really creepy. It was over a year of harassment."*
    - *"[my ex] has multiple different accounts of like it's not even his name. They're just random. he, I don't know follows you, and you think it's somebody else, and then you follow them back, and then he's able to watch."*
- There are 2 'yes' responses that are vague – unclear whether they reach the question intent or not (one from version 1, one from version 2):
    - *"Well, you know, every time you look up when you see the same person on people, you may know that if I'm not mistaken, that means that they've been on your page."* When

probed more on why she answered yes, R said there have been people she doesn't really know from her past who appear under the "*people you may know*."

- *"I don't really know who's watching my page or who's lurking"*

- The remainder seem to be misaligned with the question's intent – six of the version 1 respondents and one of the version 2 respondents answered "yes" but it doesn't seem to match the intent of the question. Examples include:
  - *"yes, my family and friends mainly you know, like I'll go on there, you know, maybe once or twice a day, especially around the holiday time."*
  - R seems to be thinking of security apps that monitor her activities. *"Yes, that's what they do actively. I get reports every day of them going and checking my password reports activity, logs and everything."*
  - *"Again. This is a difficult question to answer. not because I think I'm being tracked by somebody. But yes. Do I think organizations track me absolutely when I go into, even though I don't go into social media accounts."*
- Out of the 12 'no responses, most admit they may not know if this is happening – examples include:
    - *Not knowingly. I think I've got some people out there that. Behind the scenes, and they watch what I do. They don't make up. They don't make me aware of it like I have a hunch. But no. not to my knowledge.*
    - *Another respondent said not to his knowledge, but admitted you never really know who is behind a profile. He also described situations in the past where he thought he was contacting one person but it turned out to be someone completely different.*
    - *"Not that I'm aware of"* was a common response.
  - A few felt more certain that they were not being stalked on social media:
    - A couple said they don't use social media enough for it to be an issue.
    - One mentioned software that tracks (although unclear whether they were thinking of social media or not: *"Because I have like spyware and the different, like the VM stuff on my computer. So I check it periodically just to see if somebody's tracking me, or to see if, like, my information has been sent out to other companies."*

SQ1x (Nude Photos).

Has anyone posted nude, intimate, or sexually explicit images or videos of you on the internet without your consent or threatened to post this content on the internet?

Responses: No (24) Yes (1)

- Everyone seemed to understand the question with the exception of the timeframe – three people asked for clarification of whether we were asking about "ever" or recently.
- How did respondents arrive at their answer?
  - *"Because they haven't. I haven't seen anything. I'm not in the habit of taking nude photos of myself, anyway, so no."*
  - *"because I've never taken nude pictures of myself, or posted any."*
  - *"Well, since I don't provide that material, I'm assuming that people can't. So yeah, let's hope not."*
- One person responded yes and another individual described a less recent incident:
  - *"It was like an escort site, and I wasn't on it. He posted it, I guess, to see who would respond and who would give him money, pretending to be me once again, using my pictures and stuff."*
  - *"I think it was because someone had hacked into my messenger and put those on there..I went on messenger I think, to message somebody, and there was these naked pictures."*
- There was a related incident where photos were posted but they were not of an intimate nature (note that the respondent correctly answered this as 'no'):
  - *" gentleman was posting the pictures of me and my husband online about being meth feelers and things like that. There was no nudity, there was nothing."*

SQ1l, SQ1l1 and SQ1l2 (Threats).

Version 1:

SQ1l. Has anyone posted or threatened to post inappropriate, unwanted, indecent, or personal information about you on the Internet including your name, address, email, spreading rumors or other information about you?

Version 2:

SQ1l1. Has anyone posted or threatened to post inappropriate, unwanted, indecent, or untrue information about you on the Internet?

SQ1l2. Has anyone posted or threatened to post your personal information, including name, address, email, or other details about you on the Internet?

Responses:

SQ1l: No (8) Yes (4)
SQ1l1: No (9) Yes (4)
SQ1l2: No (10) Yes (3)

SQ111 and SQ111 combined:

- 8 respondents answered 'no' to both questions
  - 3 respondents answered 'yes' to one of the questions
  - 2 respondents answered 'yes' to both of the questions

- People generally had reasonable definitions of what "inappropriate, unwanted, indecent or personal information" might include (Version 1 and similar for Version 2):
  - *"Anything that's derogatory or threatening"*
  - *"Telling you lies about yourself, what you what you do, and then maybe showing places your body in areas that you don't approve like you know what I said."*
  - *" Anything that's outside of proper societal standards."*
  - *"Pretty much spreading false information"*
- Version 1 – The Combination Question
  - There were 4 respondents who answered the version 1 question as 'yes.'
    - There was one clear case that seems to meet the intentions of this question:
      - *"I've had my ex-husband post on social media, my name, my date of birth, my social security number, my checking account number, my balance of the account, the withdrawals."*
    - A second case seems more like identity theft:
      - Someone made a fake Instagram account in his name and started following similar people. The interviewer probed on how he would answer this question. He said *"Yes, because I think that qualifies as posting my name."*
    - The final two are somewhat questionable or too vague to assess:
      - In one, the interviewer reports that it was a scam (rather than a threat).
      - A second case is vague, with the respondent reporting that something was posted but they had it removed.

- Of the 'no' responses, some admitted it was possible (although unlikely)
  - *"Well, on one hand, there's always a possibility there's something out there. But as connected as the world is today. you would hear about it, I would assume, if you have any friends, you would hear about it sooner or later, and these days sooner."*
  - *"Because I feel like I would have heard about it from somebody I'm friends with on social media or in real life, because it would obviously be someone I know, like."*
  - *"because I haven't seen anything to indicate that happened, I think I'd be aware of it"*
- Others simply repeated "no, hasn't happened" or similar.

- Version 2 – Slanderous Content
  - There were 4 respondents who answered the version 2 slander question as 'yes.'
    - One was responding for their lifetime experience (rather than past 12 months).
    - The others seem to meet the intentions of the question:
      - One respondent reported an offender posting a digitally changed photo of her and her husband with a meth pipe to the internet and saying they were both meth dealers.
      - A second respondent had slanderous content posted by her husband: *"Yeah. My ex-husband has, he has posted it, stuff that were untrue about me..and my people that I know they tell them to take it down. They said 'you need to take that down. That's not true, and you know it' and so he took it down. But there's been so many that he hasn't taken down."*
      - The third respondent had false accusations posted against him (while his name was never used in the posts, the individuals in the forum was aware who the content was about).
  - Of the 'no' responses, examples include:
    - *"I've never seen any example of it. I've never seen any confirmation of it, and I pay. I'm on my phone all the time, and because it's connected to my hearing aid. So I constantly have my phone with me so I can hear things. So I'm aware of everything that comes through."*
    - *"I've never read anything or seen anything that."*
    - *"Not within the last 12 months, but in the past, when I had Facebook."*
    - *"Because that has not happened in the last 12 months."*

- Version 2 – Personally identifiable information (PII)
    - There were 3 respondents who answered the version 2 PII question as 'yes.'
        - One incident involved a family member
            - A respondent said that her offender (an ex-boyfriend) was posting PII of her relative – presumably this would not be in scope (since the relative is the victim).
        - A second respondent is the one who reported the distorted photos presenting her as a drug dealer (same incident described above).
        - A third respondent said that a fellow forum member (who had been harassing her) posted a partial email address for her in the forum.
    - Of the 'no' responses, examples include:
        - *"If I would have seen it, I could say yes, but I've not seen that anywhere."*
        - *"no one ever posted my name. My 1st name, my last name, anything which I thought was really really interesting. I kept track of this thread for a while to see when the comments would actually end, and I was interested in whether someone would actually personally identify me by name. I was interested in that, and it never happened."*
        - A respondent said not within the last year, but it has happened before. In the past, there was a situation where he called off a relationship with someone and she was threatening to post his social security number on the internet.
        - Other respondents simply reiterated that it has not happened to them.

SQ_OTHERREACTIONS (Emotions).

Did you feel any of the following feelings when any of these unwanted contacts or behaviors occurred: Alarmed? Intimidated? Harassed? Seriously annoyed?

Responses:

Alarmed:	***12 responses***
Intimidated:	***7 responses***
Harassed:	***17 responses***
Seriously annoyed:	***14 responses***
None of the Above:	***1 response***
N/A (question not asked):	***1 not asked (all questions answered 'no')***

Discussion:

- Other emotions included fear, anger and sadness/depression.
- Some sample comments from those with incidents that appear to be "in scope":
    - *"I'm still fighting it to this day, like you might hear me get a little shaky. You might hear me stutter a little bit like. Ptsd is no joke."*
    - *"I'm scared. I mean, I guess you could say annoyed, but that was like low on the list of my feelings."*
- Some sample comments from those who appear to have incidents that are about spam and phishing:
    - *"Disappointed. Kind of, you know, taken back by it all, you know."*
- How long did the emotions last?
    - This varied by the type of incident. Those who had some level of fear had long lasting distress:
        - *"I wonder if they mean. after the actual incident or months? Why, you know, if it's after the actual incident, it usually would take me a couple hours to feel relaxed again. Feel that I could let my guard down and not be. I'd be like looking in the windows. And you know, yeah, being nervous. But if it's how long have I felt that way through the whole thing? It would be like over a year."*
    - Those who described unwanted contacts in the form of spam had short emotional episodes:
        - *"it keeps happening. Why, you know that sort of thing, but it's very minimum. We're talking here seconds, and it's over"*

Detailed Notes for Identity Theft Cognitive Interviews

P1.

For the incidents occurring in the last 12 months, how did someone use your checking or savings account?

Answers: Online (4) Some other way (1) Both (0) Don't know (1)

Discussion:

- 5 out of the 6 respondents interpreted the question as asking how the account was accessed or how the transaction occurred. One person did not select an answer because she did not know how it happened.
- Out of the 4 who responded "online":
    - 1 placed an order through social media but never received the product. The company was no longer there when he called.
    - 1 respondent's nephew used her debit card to make a purchase on Temu.
    - 2 respondents mentioned the word "hacked" – 1 described it as online transaction to someone they did not know. The other suspected someone hacked their account and used the info to make a purchase.
- The person who responded "some other way" said her bank informed her that the unauthorized transaction occurred in person at her local Walmart. She believes an employee copied her debit info and used it to purchase something in the store.
- The person who did not select a response said she was alerted by her bank that her debit card was used out of state. R did not know someone got her information, but thought it was usually done online.
- Interpretation of "online":
    - Out of 4 respondents, 3 defined it as internet/app-based transactions (e.g., Google, Amazon, social media). 1 stated "online means being connected to a form of communication which shares my thoughts and opinions"
- Interpretation of "It was done in some other way (e.g., in-person, over the telephone, by mail, something else):
    - Examples included scam telemarketers, paying a bill online or calling an 800 number, and in-person transactions (e.g., at a restaurant or at a store)

P2.

How do you think your personal information was obtained to access your checking or savings account? (MARK ALL THAT APPLY)
I lost an item that included my personal information
My wallet, checkbook, or purse was stolen
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device
It was stolen during an online purchase/transaction
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader
I responded to a scam email or clicked on a link in the email
I responded to a scam phone call
I responded to a scam text message or clicked on a link in the message
I responded to a social media post
My personal information was stolen from my personnel or human resources electronic records at my place of employment
My electronic records containing personal information were stolen from a company or other organization
Obtained in another way (specify)_____

Discussion:

- All 5 respondents who were asked this question understood it to mean how their debit card/personal information was obtained.
    - *"How do you think they got your personal information?"*
    - *"How I feel my information was put out for someone to get it."*
    - *"What's the best way they could have gotten ahold of my information"*
    - *How the information was obtained from her debit card.*
    - *"How did someone get their hands on my debit card to place the order?"*
- Two respondents were not sure how their debit card information was obtained, so they responded with "maybe" or "possibly" for certain items
    - One additional person selected "My electronic records containing personal information were stolen from a company or other organization," but it was unclear how she arrived at this.

- Interpretation of "I responded to a scam email or clicked on a link in the email":
    - Two respondents referred to social media and/or text messages in their responses:
        - *"Responding to a spam email/not watching what your social media is doing"*
        - *One person described an instance where someone with a fake Facebook profile (not email) messaged her asking for money. She also mentioned scam text messages that she's received.*
    - The other three interpreted it as intended.
        - *"Open an email, there's an offer or virus protection outdated, so you click on a link and put in your information, but it is a scam."*
        - *One person referred to spam emails, then described a prior incident where she clicked on a link in an email that revealed an image of a fishing hook accompanied by a message demanding $200 if she didn't want her PayPal account to be blocked.*
        - *"It was a fake email, a fake person"*
- Interpretation of "I responded to a scam text message or clicked on a link in the message":
    - No obvious issues, but none of the three respondents who were asked this probe referred specifically to text messages in their response.
        - *"Responded to a link, don't know how else to phrase it."*
        - *"Somebody sent me something that I would feel would be one thing, and it ended up being just a way for them to get my information."*
        - One person said it was "*kind of the same thing"* as "I responded to a scam email…"
- Interpretation of "I responded to a social media post":
    - One respondent did not know what this meant because they did not use social media.
    - Another respondent was confused at first by "social media ***post,***" but understood it in the context of Facebook messenger.
        - *"If you post a post on Facebook and I go and comment on it, there's no way that somebody can get my checking account information just by commenting on a social media post… Now, if it had said about clicking on a link in messenger, versus just social media period. That would be something different. Because I do get those spam messages [on FB messenger]."*
    - No issues with the other three respondents who were asked this probe.
- Interpretation of "My personal information was stolen from my personnel or human resources electronic records at my place of employment":
    - No issues. Respondents interpreted this in the context of data breaches as well as individuals who might steal information from HR/payroll.
- Interpretation of "My electronic records containing personal information were stolen from a company or other organization"
    - No obvious issues. Most respondents interpreted this as data breaches.

P3.

For any of the incidents occurring in the last 12 months, how did someone use your credit card account?

Answers:
Online (2) Some other way (0) Both (2)
Discussion:

- Three respondents may not have answered this question as intended; their comments suggest they may have been thinking about a mix of how their information was *obtained*, and how it was *used*.
    - One person initially selected "Both," because he believed his information was taken from him online or through a text scam, but one of the unauthorized purchases occurred in-store based on the transaction history. Later, he seemed to change his answer to "it was done online," referring to the text scam.
    - Another person said someone made unauthorized purchases from her Amazon account using her Amazon credit card. She said she was "80% sure" it was done online, noting that it would be unlikely to have happened by phone because she doesn't speak to telemarketers. Her response implied that she may have been thinking about how her information was obtained rather than how it was used.
    - The notes suggest a third respondent did not answer the question as intended but it's somewhat unclear. This person initially selected "it was done online," but later changed it to "both." She knew that one purchase was made online because she received her statement that included a shipping fee. The interviewer was not able to determine why she also thinks "it was done in some other way."
- All four of these respondents relied on statements or their transaction history to determine how the incident to their credit card was done, including one respondent who initially found out after receiving a notification from a store stating that his merchandise was ready for pickup.
- Interpretation of "online":
    - No issues.
    - Respondents described it as either through the internet; through a computer/device/app; an online retailer (where you can purchase "without going to the store"); and "without actually physically taking the card and using it."
- Interpretation of it "was done in some other way (for example, in-person, over the telephone, by mail, something else)":
    - No issues.

P4.

How do you think your personal information was obtained to access your credit card account? (MARK ALL THAT APPLY)
I lost an item that included my personal information
My wallet, checkbook, or purse was stolen
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device
It was stolen during an online purchase/transaction
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader
I responded to a scam email or clicked on a link in the email
I responded to a scam phone call
I responded to a scam text message or clicked on a link in the message

I responded to a social media post
My personal information was stolen from my personnel or human resources electronic records at my place of employment
My electronic records containing personal information were stolen from a company or other organization
Obtained in another way (specify)_____

Discussion:

- All 4 respondents who were asked this question understood it to mean how their credit card information was accessed, stolen, or compromised. None of them were 100% sure how it was obtained, but 2 of the respondents were more confident their responses than the others.
- Interpretation of "I responded to a scam email or clicked on a link in the email":
    - No issues.
        - *"[…] those are just phishing scams to see if people will respond."*
        - *"Emails that look almost exactly like they are coming from a legitimate company."*
        - *"Getting an email and responding to it or clicking a link in that email."*
- Interpretation of "I responded to a scam text message or clicked on a link in the message":
    - No issues
        - *"I clicked on something from my electric company, and it says, 'Call immediately.' So I called the number that was attached to the text, and they're like, 'your electric is going to be turned off in 1 hour if you don't send us a credit card or your payment of $800.' I've never had an electric bill that [high]. I said, 'What is your name?' And they hung up on me, so I immediately called the electric company."*
        - *"Same as a scam email, but a text message instead"*
- Interpretation of "I responded to a social media post":
    - 1 respondent described it in the context of making a purchase through social media; 1 respondent gave an example of a fake social media profile sending messages asking for money; and 1 respondent had not seen this kind of post on social media.
        - *"When people are on Facebook, TikTok […] they have these different options to buy things, make purchases, and anything that sounds too good to be true it probably is, and a lot of times these people are fishing to get your money, and if it's not a reputable company that you are used to doing business with, don't do it, and they're very, very clever, because they can even have and print up things to make their logo look just like Amazon."*
        - *"A typical one is someone posing as a family member to ask for bond money to get out of jail"*
        - *"Responding to a social media like Instagram, or something that ends up being a scam. But I've never actually seen that."*
- Interpretation of "My personal information was stolen from my personnel or human resources electronic records at my place of employment"
    - No issues.
        - *"When someone in human resources or coworkers have had access to your personal information and files that happens a lot, especially in the workplace."*

- *Someone who "went to my previous employer, perhaps posing as somebody who's looking to hire me"*
- *"If I have my personal information stored with my HR and it's being stolen through them, and it's out of my control."*

- Interpretation of "i"
    - No issues.
        - *"That's when they get that 3rd party where you agree to opt into things. And they all of your personal information is synced, or you got it locked in your phone or your computers. And when that 3rd party get a hold of it, your information is exposed."*
        - *"That's all my information that's out in the ether, and may have been compromised or stolen. Whether it's Google or any of these other companies that have my information."*

Q9a.

Have you ever had at least one email account, such as Gmail or Outlook, or social media account such as Facebook, Instagram, YouTube, Reddit or Pinterest?

Answers: Yes (23) No (2)

Discussion:

- 5 out of 25 respondents did not answer the question as intended, including one who changed their answer when the Q was repeated. All 5 of these Rs thought (or initially thought) it was asking if their email/social media accounts had ever been misused or hacked into.
    - 1 additional respondent may have misinterpreted the Q. Upon probing, they said, *"It's asking, have any of your personal information been compromised via a social media group?"*
- Interpretation of "social media accounts"
    - Most respondents considered social media accounts to be online platforms where you can connect and interact with other people. Some mentioned they were places for sharing content, information, entertainment, or otherwise expressing yourself.
    - Common examples included Facebook, WhatsApp, TikTok, Twitter/X, and Instagram.
- Opinions on YouTube, Pinterest, and Reddit as social media:
    - About half of respondents considered YouTube, Reddit, and Pinterest social media.
    - Another ~6 respondents considered them social media, but noted that they are used differently (less interaction between users, particularly for YouTube and Pinterest)
        - *"Sort of. For Pinterest, you socialize but it's more like recipe sharing, it's different."*
        - *"Technically yes. You're not directly speaking to someone, but you're viewing what they share."*
        - *"Not as directly as Facebook and TikTok, but yes because people can subscribe to YouTube, people are posting things. It's a source of information but there's less interaction."*
    - Four respondents did not consider YouTube social media; three respondents didn't consider Pinterest; and one respondent did not consider Reddit social media.
    - YouTube seemed to be the most widely recognized by participants, followed by Pinterest and Reddit.

Q9bb.

Has anyone EVER created an email or social media account for you without your permission to pretend to be you?

Answers: Yes (8) No (16) Missed (1)
Discussion:

- Several respondents may have been thinking about misuse of their existing email/social media accounts when answering this question—either alone or in combination with someone creating an email/social media account to impersonate them.
    - One person said she had checked for social media accounts that use her existing email address
    - One person said they always check their social media accounts and cited an absence of suspicious activity on their own account.
        - *"I always check my social media accounts. [..] For instance, with Facebook, they had sent me an email and saying that it was suspicious activity on my account, so I changed my password. That's how I know."*
    - One person said she monitors whether anyone is using her email account on the dark web.
        - *"I don't know for sure. I know I have a company that checks my email and lets me know if it's out there. Everyone is on the dark web."*
    - One person said 'yes' to both Q9b and Q9bb. It's not clear whether she misinterpreted Q9bb or if she was just thinking about Q9b when responding to the probe.
- Most of those who responded 'Yes' said they knew because friends and/or family alerted them to the fake account.
    - 1 person who responded 'Yes' described an instance where her account was hacked into and taken over rather than an account that was created.

- Of those who responded 'No,' 8 respondents indicated that they did not know for sure if anyone had ever created an account pretending to be them.
    - Two respondents said they had not received alerts about suspicious activity, suggesting they may have been thinking about someone accessing their existing accounts. Two other respondents said they had checked to see if any accounts existed that use their email addresses.
        - *"I always check my social media accounts. [..] For instance, with Facebook, they had sent me an email and saying that it was suspicious activity on my account, so I changed my password. That's how I know."*
        - *"I don't know for sure. I know I have a company that checks my email and lets me know if it's out there. Everyone is on the dark web."*
        - *1 R said she had her daughter check to see if there were any social media accounts using her email/pretending to be her.*

P5.

For the incidents that happened in the last 12 months, how do you think your personal information was obtained to (use your email or social media account/created an email or social media account for you)? (MARK ALL THAT APPLY)
I lost an item that included my personal information
My wallet, checkbook, or purse was stolen
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device
It was stolen during an online purchase/transaction
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader
I responded to a scam email or clicked on a link in the email
I responded to a scam phone call
I responded to a scam text message or clicked on a link in the message
I responded to a social media post
My personal information was stolen from my personnel or human resources electronic records at my place of employment
My electronic records containing personal information were stolen from a company or other organization
Obtained in another way (specify)_____

Discussion:

- 3 of the 4 respondents who got this question initially said that they did not know how their personal information was obtained.
    - One person ultimately selected "I responded to a scam text message or clicked on a link in the message." She interpreted a Facebook message as a text message.
    - Another ended up selecting three possible options
    - The third person did not select any response options, but instead said, *"I think it was through a 3rd party, or maybe someone, one of my individuals I was conversing with or messaging and things like that maybe perhaps they were compromised, and therefore they were [able to get my information] by being compromised on their end.*
- 1 respondent selected "Obtained in another way." She said she had previously logged into her Facebook account on a friend's phone, forgot to log out, and the friend continued to use the account without permission to post/comment without her consent.
    - This person found out because she noticed the posts/comments that she did not make and checked her settings to see which devices were in use.

Q11.

Has anyone EVER used any of your other existing accounts, without your permission, such as…
· Telephone account such as for cell phone or landline telephone
· Internet account such as for internet or wireless Wi-Fi.
· Utilities accounts, such as cable, gas, or electric;
· Medical insurance accounts, such as Medicare or a health spending account;
· Entertainment accounts, such as for music, movies, or games;
· Online payment accounts, such as PayPal or Venmo; or
· Some other type of accounts?

Answers: Yes (13) No (12)

Discussion:

- Two of the 13 "yes" responses were not consistent with the question, and it was unclear whether another three responses were consistent.
    - Of the two that were not consistent:
        - 1 respondent described an incident with his social media
        - 1 respondent said she received notice from either her insurance company or a hospital informing her that her personal information (including SSN) was part of a data leak, but there was no resulting activity on her accounts.

Of the three that were unclear:

- 1 respondent said someone spoofed her cell phone number to make spam calls, but her cell phone account was not accessed.
- 1 respondent said someone "took money" from his Cash App. It happened when he was reimbursing someone, and the payment went to someone else accidentally, who did not return it.
- 1 respondent said someone used his Gmail account to set up a Google wallet, which resulted in him owing $4000. He did not previously have a Google Wallet set up (unclear if this would count as a new or existing account, but since it was through his Google account he interpreted it as an existing account)

- A couple other respondents described multiple incidents, not all of which were consistent with the question. Incidents that were inconsistent included:
  - An attempt to open a utilities account in Rs name without permission
  - A phishing attempt via email from a fake PayPal email address. She contacted PayPal to confirm that it was not a real email.

Q13a.

Telephone accounts such as cell phones or landline?
Answers: Yes (2) No (3)
Discussion:

- 1 respondent who responded “Yes” said her cell phone number was *"used to make spam calls to other people."* She confirmed that her cell phone account was not accessed, just that her number was being used/spoofed. She became aware of the situation when she received angry calls from people asking her to stop calling them.
- 1 respondent said an ex-partner (who had been on his cell phone plan) "demoted" him so that he was no longer the primary user, then cut off his service. He found out when his service stopped. He also said this happened 12-16 months prior.

Q13aa.

Internet accounts such as wireless or Wi-Fi?
Answers: Yes (0) No (5)
Discussion: No Rs responded “Yes” to this question.

P6.

Thinking about the last 12 months, how did someone use your (Telephone/Utility/Medical Insurance) account?

Answers: Online (1) Some other way (0) Both (1)
Discussion:

- 1 respondent said "It was online" but said she didn't know what happened. She speculated that an employee of her insurance company or the hospital may have stole her information (She was referring to an instance where she received notice either from her insurance company or a hospital stating that her personal info was compromised in a data leak.)
- 1 respondent selected "both" because he suspected that his former partner, who had been on his cell phone plan, misused his account using a combination of methods (in-person at a store, and online/by phone)

P7.

How do you think your personal information was obtained to access your (Telephone/Utilities/Medical Insurance) account? (MARK ALL THAT APPLY)
I lost an item that included my personal information
My wallet, checkbook, or purse was stolen
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device
It was stolen during an online purchase/transaction
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader
I responded to a scam email or clicked on a link in the email
I responded to a scam phone call
I responded to a scam text message or clicked on a link in the message
I responded to a social media post
My personal information was stolen from my personnel or human resources electronic records at my place of employment
My electronic records containing personal information were stolen from a company or other organization
Obtained in another way (specify)_____

Discussion:

- 1 respondent was asked this question. She selected "My electronic records containing personal information were stolen from a company or other organization" because the incident she was referring to was a data breach.

Q15.

Has anyone EVER, without your permission, used your personal information to successfully open any NEW accounts, such as…
· Checking or savings accounts;
· Credit card accounts;
· Email accounts, such as Gmail or Outlook;
· Social media accounts, such as Facebook, Instagram, YouTube, Reddit or Pinterest;
· Telephone or
· Internet accounts;
· Utilities accounts, such as cable, gas, or electric;
· Entertainment accounts, such as for music, movies, or games;
· Loans or mortgages;
· Insurance policies;
· Online payment accounts, such as PayPal or Venmo; or
· Some other type of new account?

Answers: Yes (7) No (18)
Discussion:

- Only 1 person responded "Yes" to both Q9bb and this question (Q9bb is slightly different)
    - I other person responded "No" to this question but reiterated that the only new account someone created for her was the FB account pretending to be her.
- For those who responded "Yes," examples included utilities accounts, telephone accounts or new phone lines added to an existing account, checking accounts, internet accounts, a health insurance policy, and a Facebook profile.
    - 1 person responded "Yes," but the example he gave was inconsistent with the Q. He said someone opened up two additional phone lines on his existing cell phone account.

- Most of those who responded "No" understood the question.
    - 2 respondents thought the question was asking about existing accounts.
        - 1 person interpreted it as "Has anybody tried to scam her by using her credit cards." She was thinking about existing cards as she described going online to your credit card statement and seeing charges you didn't make as an example.
        - *"[It's asking] if I had noticed any unauthorized activity on set accounts." [Interviewer: And is this accounts you already have, or, brand new accounts?] "Probably accounts I've already had currently have."*

Q17d.

New social media accounts, such as Facebook, Instagram, YouTube, Reddit or Pinterest?
Answers: Yes (0) No (1)
Discussion:

- Only 1 respondent was asked this question. When asked what it was asking, they included "Telephone" accounts in their response:
    - *"[it's asking] if anybody has created accounts under my name without my consent, whether telephone or Internet or Reddit, Facebook Gmails."*

P8.

For any of the incidents occurring in the last 12 months, how did someone open a new (checking/ credit card/telephone, utility/entertainment/loan or mortgage/insurance policy) account with your personal information? (MARK ALL THAT APPLY)

Answers:
Using a computer (1) Withdrawal/purchase in-person (0) Both (0)

Discussion:

- Only 1 R was asked this question.
    - *"Well, the marketplace and the government. They usually get all of our personal information through computer systems through the welfare system. And so that's how I'm assuming that that's how they retained obtained my information." When probed on the computer aspect: "Because that's how they, I guess the welfare system, communicates with them. They don't actually sit down and make phone calls and communicate with marketplace to be like, Hey, she should change to a billed insurance policy to get her off of Medicaid. So it's all processed to go computer system.. welfare flags it through the system through marketplace and says, Ok, she's flagged, she needs to switch over. You guys need to reach out to her to see if she's interested in the marketplace insurance."*

P9.

How do you think your personal information was obtained to open a new (checking/credit card/ telephone/internet, utility/entertainment/loan or mortgage/insurance policy)? (MARK ALL THAT APPLY)
I lost an item that included my personal information
My wallet, checkbook, or purse was stolen
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device
It was stolen during an online purchase/transaction
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader
I responded to a scam email or clicked on a link in the email
I responded to a scam phone call
I responded to a scam text message or clicked on a link in the message
I responded to a social media post
My personal information was stolen from my personnel or human resources electronic records at my place of employment
My electronic records containing personal information were stolen from a company or other organization
Obtained in another way (specify)_____

Discussion:

- No Rs received this question.

P10.

For any of the incidents occurring in the last 12 months, how did someone use your personal information to do (this/these things)?

Discussion:

- No Rs received this question.

P11.

How do you think your personal information was obtained to (file a fraudulent tax return/get medical treatment/apply for a job/to provide false information to the police to conceal their identity/provide false information to a government agency/apply for government benefits/misuse your personal information)? (MARK ALL THAT APPLY)
I lost an item that included my personal information
My wallet, checkbook, or purse was stolen
My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device
It was stolen during an online purchase/transaction
Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader
I responded to a scam email or clicked on a link in the email
I responded to a scam phone call
I responded to a scam text message or clicked on a link in the message
I responded to a social media post
My personal information was stolen from my personnel or human resources electronic records at my place of employment
My electronic records containing personal information were stolen from a company or other organization
Obtained in another way (specify)_____

Discussion:

- No Rs received this question.

P12.

I've asked you about different ways someone may have used your personal information. This next question concerns whether someone ever obtained your personal information using any of the following methods. (MARK ALL THAT APPLY)
It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device 01
It was stolen during an online purchase/transaction 02
Someone stole it during an in-person purchase/transaction, including using a skimmer card 03
I responded to a scam email or clicked on a link in the email 04
I responded to a scam phone call 05
I responded to a scam text message or clicked on a link in the message 06
I responded to a social media post 07
My personal information was stolen from my personnel or human resources electronic records at my place of employment 08
My electronic records containing personal information were stolen from a company or other organization 09
None of the above 10

Discussion:

- 10 respondents were asked this question.
- 2 false positives for "It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device":
    - One person (I9) selected this option but upon probing it was determined that She was referring to a data breach from her doctor's office. She selected two other responses as well but likely should not have given the situation she described.
    - One person described an unsuccessful attempt to get their personal information
- 1 false positive for "I responded to a scam email or clicked on a link in the email" (it turned out to be misleading—but otherwise legitimate—marketing, not a scam email)

P13.

Has this happened during the past 12 months, that is from [AUOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?

Answers: Yes (3) No (5)

Discussion:

- No issues with respondents' ability to recall events within the reference period.
- Those who responded "Yes" said they relied on their own record-keeping, recent memory, and landmark events:
    - *"Anybody that call or text me, it's on here. I don't care if it's over 2 years ago. It's saved in my phone - Not only that I take screenshots and print them out. And I keep records. One thing with my training and my professional background—we are taught to keep a paper trail."*
    - *"I mean, it's recent in my memory, so I'm sure it's in the last year."*
    - *"Because it was [this past] Christmas."*
- Those who responded "No" said it happened "years ago" or a long time ago, and seemed sure of the timeframe.

Detailed Notes for Fraud Cognitive Interviews

S1. [Intro item]

In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], did you pay money to receive a prize, grant, inheritance, lottery winning, or sum of money that you were told was yours?

S1b.

For the most recent time this happened how did you first find out about the money or prize?

Answers: Note that some Rs gave more than one response.

- ❖ Someone told me on a phone call (2)*
- ❖ A text message (0)
- ❖ The TV, radio or a newspaper (0)
- ❖ Social media (2)
- ❖ Website (0)
- ❖ Chat application, such as WhatsApp, Telegram or Signal (2)
- ❖ Someone told me in-person (2)
- ❖ From an email I received (4)
- ❖ From material I received in the mail or delivery to my home or business (0)
- ❖ Some other way (Specify: _____) (0)
- ❖ Not Applicable/answered "No" to S1 (15)

*One person was contacted about an inheritance by phone, but they did not end up paying money. The interviewer asked the respondent the probes for this section because the respondent answered "no" for all of the other items.

Discussion:

- Three respondents did not answer the question as intended.
  - One answered based on how they did not get the money they believed they were promised instead of how they learned about the money or prize.
  - One initially answered based on a scam or debt that they owed. For this reported incident, the money they paid did not have anything to do with a prize, grant, inheritance, lottery winning, or sum of money that you were told was theirs. However, after moving on in the survey, the respondent remembered an incident that did apply to this item.
  - One respondent initially said that their "ex-wife" told them about the prize or money. After reviewing the response options, they chose "in person" as the best fit.
- Seven answered the question as intended; they didn't have any doubts about how they found out about the prize, grant, inheritance, lottery winning, or sum of money that they were told was theirs.
- Of the 7 who answered the question as intended:
  - Response….
    - One was contacted by email and was told they would receive a gift card
    - One was contacted by phone and was told they were receiving an inheritance
    - One was approached in person to purchase a raffle ticket to win a prize
    - One was contacted by email and was told they would receive a vacation trip
    - One was contacted by social media and was told he won a PlayStation 5

        - Two did not specify what they were told they would receive, however one of them was contacted by email and another was contacted in person prize or money.
    - Response Options
        - One respondent said that they were told in a phone call to join a Zoom call. They initially selected "phone" as it fit the best. The respondent changed their response to "chat application" after reviewing the response option list. While they were not familiar with "WhatsApp or Telegram, they didn't see another category where Zoom would fit.
        - One respondent initially selected "social media" but changed their response to "chat application" when they saw "Telegram" was an option.
    - Suggested Response Options:
        - Facetime and or Zoom (video calls)
- Out of the 15 "no" responses to S1, respondents seemed to have an accurate interpretation of the question.

S2. **[Intro item]**

[Not including the time(s) you already reported] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], did you pay money to settle or pay off taxes or a debt, but you found out you were being tricked or lied to and the debt was not real or not yours?

S2a.

For the most recent incident, how did you first find out about the debt you were told you owed?

Answers:

- Someone told me on a phone call (2)
- A text message (0)
- The TV, radio or a newspaper (0)
- Social media (0)
- Website (0)
- Chat application, such as WhatsApp, Telegram or Signal (0)
- Someone told me in-person (0)
- From an email I received (2)
- From material I received in the mail or delivery to my home or business (0)
- Some other way (Specify: _____) (0)
- Not Applicable/answered "No" to S3 (21)

Discussion:

- Three respondents answered question, S2a, as intended.
- One respondent described three different incidents when answering S2a, and for two of these, they did not pay money. The respondent missed the part of the question that asks, "**did you pay money** to settle or pay off taxes or a debt*"* in S2.
- One respondent answered the S2a appropriately ("no") but answered "yes" to this question in the web survey (screener). They clarified that for them the operative word in the question stem was "tricked," insinuating they did not feel tricked into paying money to settle or pay off taxes or debt that they later found out was not real or not theirs.
- Out of the 18 "no" responses to S2, respondents seemed to have an accurate interpretation of the question.

S3. **[Intro item]**

[Not including the time(s) you already reported] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake? Do not include money given to panhandlers on the street.

S3a.

For the most recent time, how did you first find out about the request to donate to a charity or charitable cause that later turned out to be fake or you suspected was fake?

Answers:

- Someone told me on a phone call (0)
- A text message (0)
- The TV, radio or a newspaper (0)
- Social media (2)
- Website (1)
- Chat application, such as WhatsApp, Telegram or Signal (0)
- Someone told me in-person (3)
- From an email I received (0)
- From material I received in the mail or delivery to my home or business (0)
- Some other way (Specify: _____) (1)
- Not Applicable/answered "No" to S3 (19)

Discussion:

- Five of the respondents answered the question as intended. However, one respondent may have answered based on when they found out the charity was fake and not about how they found out about the request to donate to the charity or charitable cause.
- Response Options
  - One respondent, after seeing the response options, wondered if they should have selected "other" because they talked about the incident with their co-workers.
  - One respondent suggested adding docuseries and documentaries as a way of finding out about the fake charity or charitable cause.

S4. **[Intro item]**

[Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you paid money to get a job or get into a business opportunity but were tricked or lied to about how the money would be used or what you would receive in return?

S4a.

How did you first find out about paying the money to get a job or get into a business opportunity?

Answers:

- ❖ Someone told me on a phone call (0)
- ❖ A text message (0)
- ❖ The TV, radio or a newspaper (1)
- ❖ Social media (0)
- ❖ Website (0)
- ❖ Chat application, such as WhatsApp, Telegram or Signal (1)
- ❖ Someone told me in-person (1)
- ❖ From an email I received (1)
- ❖ From material I received in the mail or delivery to my home or business (0)
- ❖ Some other way (Specify: _____) (0)
- ❖ Not Applicable/answered "No" to S4 (21)

Discussion:

- Two respondents answered S4a as intended.
- Two respondents did not answer S4a as intended. The first selected "WhatsApp, Telegram or Signal" but they received an email with a link to WhatsApp where they went to find out more. The second was reporting an experience that happened to their sister and not a personal experience for themselves.

S5. **[Intro item]**

[Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you invested money with a person or company that tricked you or lied to you about what you would receive, such as promising a guaranteed return on your investment or that you would not lose any money?

S5b.

How did you first find out about investing with the person or company?

Answers:

- ❖ Someone told me on a phone call (0)
- ❖ A text message (0)
- ❖ The TV, radio or a newspaper (0)
- ❖ Social media (1)
- ❖ Website (0)
- ❖ Chat application, such as WhatsApp, Telegram or Signal (0)
- ❖ Someone told me in-person (0)
- ❖ From an email I received (0)
- ❖ From material I received in the mail or delivery to my home or business (0)
- ❖ Some other way (Specify: __Google_____) (1)
- ❖ Not Applicable/answered "No" to S5 (23)

Discussion:

- One of the respondents answered the question (S5b) as intended and did not have any doubts about knowing how they found out about the investment opportunity.
    - They described the incident:

"A business associate from… work… had a startup opportunity and was soliciting angel investor funds for the startup… I gave him a little bit of money, kind of risk versus reward, if you will. And then I found out that there was nothing behind the start up."

- The respondent did not express any confusion about the response options, and they did not have any problems fitting their answer into a category. When asked if a category was missing from the list, the respondent said

  "I think… Yes, in a way. We do a lot of angel investment seminars. They're seminars where people present their ideas…. They're in-person. They're not done via Zoom, or anything like that."

  However, the option of "in-person" would fit for this scenario.

S6. **[Intro item]**

[Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you paid for any products or services that you NEVER received or that turned out to be a SCAM?

R answered S6 by saying "not something that turned out to be a scam that something that wasn't above aboard" and then described a situation with an extended warranty for a car. He paid $300 for this until he learned that this was accepted in his state. R said he got an email from him

S6b.

How did you first find out about purchasing the product or service?

Answers:

- ❖ Someone told me on a phone call (1)
- ❖ A text message (0)
- ❖ The TV, radio or a newspaper (0)
- ❖ Social media (4)
- ❖ Website (5)
- ❖ Chat application, such as WhatsApp, Telegram or Signal (0)
- ❖ Someone told me in-person (1)
- ❖ From an email I received (3)
- ❖ From material I received in the mail or delivery to my home or business (0)
- ❖ Some other way (Specify: ____App_____) (2)
- ❖ Not Applicable/answered "No" to S6 (10)

Discussion:

- A few respondents had issues selecting how they first found out about purchasing the product or service for S6a.
    - Two respondents saw a product on social media that had a link that took them to a website. They were not sure if they should select social media or website as their answer.
    - A third respondent found out about a product while watching an advertisement in an app they were using. They expressed confusion because they were not sure what category to select. They first said, "social media" and then decided on "some other way" as their answer.
- Two respondents did not answer the question (S6a) but rather told their personal story about the incident. Their response to the item came later after the interviewer showed the response categories or probed for an answer.
- Nine respondents answered the question S6a as intended and did not express doubts about know how they first found out about purchasing the product or service.
    - Two described the email they received.
        - "Email that followed closely on a purchase from a brick-and-mortar business. and an email from the same business showed up. It turned out to be a scam. It looked very real."
        - The respondent thought they were purchasing garden sized gnomes, but they were only 3 inches tall. "It was just one of those things where the product was unique, and it caught my eye, and I didn't really investigate the company."

- Four suggestions were made concerning the response options for S6b. Three respondents made suggestions for additional response categories.
    - One suggested the response option list was too narrow as it didn't include using Amazon's chat bot. They had used the chat bot as part of the purchase experience.
    - Two made a suggestion to add "app" as a response option.
    - Utilizing "select all that apply" was suggested by one respondent who felt they had more than one way of finding out. This particular respondent had been told in-person by someone she knew to go to a website for a product. The respondent wanted to select "website" and "someone told me in-person".

Recommendation:
Consider adding "app" as a response option.
Consider revising the response option "Chat application, such as WhatsApp, Telegram or Signal" to include "chat bot".

S7. **[Intro item]**

[Not including the time(s) you already told me about] In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you donated, sent, or otherwise given money to someone who PRETENDED to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be?

S7a.

Which ONE of the following BEST DESCRIBES how you were first contacted by this person?
Answers:

- ❖ Through a chat application, such as WhatsApp, Telegram or Signal (0)
- ❖ Through a dating app (0)
- ❖ Through social media such as Facebook, TikTok, Instagram, or LinkedIn (0)
- ❖ Someone told me on a phone call (0)
- ❖ Through a website (0)
- ❖ In an email (1)
- ❖ By a text message (0)
- ❖ By a phone call (0)
- ❖ Some other way (Specify: _____) (0)
- ❖ Not Applicable/answered "No" to S7 (24)

Discussion:

- One respondent answered "yes" to item S7.
  - The respondent answered S7a as intended and did not show doubts about their answer.
  - The email they received asking for money appeared to come from the respondent's mother's nonprofit hospice healthcare provider. They said,
    "The deceptive part of it was the money did not go to the hospice organization. It went to another organization."
- Three respondents indicated that they had received inquiries for this type of incident but they didn't "fall" for it.

Cryptocurrency

Did you provide the money using cryptocurrency?

YES 01
NO 02

Discussion:
Respondents had varying ideas of how cryptocurrency was developed and works. A few expressed that they did not use it or were afraid to use it. The following are the major categories of responses concerning what cryptocurrency meant to them. Quotes are provided when available.

- Two respondents reported paying with cryptocurrencies across all modules.
  - One said it is a different way to pay, every transaction is visible, but your identity is unknow.
  - Another respondent said that it is a way of controlling your finances, investing, and a mode to transmitting a digital form of money.
- Twenty-one respondents reported that they did not pay using cryptocurrencies. [Some respondents had more than one response that was categorized below.]
  - (2) Never took interest in cryptocurrencies/Do not use
  - (1) A way to manage money
    - "Trendy way to manage money if you will."
  - (1) For the wealthy
    - "That's for the rich people who can do those things and maneuver in that arena where us regular, everyday people, it's not something that's sitting at the front of our mind."

- (2) Blockchain
  - "It's usually a numerical value placed on a blockchain algorithm that it's not physical currency. It's a digital type of currency. That's like, I said, it's based on blockchain algorithm that is locked up. So, I mean, I've dabbled in crypto here and there, like I've had one base accounts, and but nothing big."
  - "Cryptocurrency is a form of decentralized money that is basically an agreed upon value. That's set by a blockchain. A blockchain obviously, is where you record all the transactions… I'm speaking particularly about… Bitcoin. So that's what a cryptocurrency is – a decentralized platform for finance and exchange of goods."
  - "To me, it's just digital money. So, in terms of Bitcoin, Ethereum. I know there's a bunch of them out there. I've never bought any of it. But it's all, as far as I know, digital currency that they somehow mine from a computer. I'm not exactly sure."
- (3) Not real money
  - "I'm not sure about cryptocurrency. I think a fake money, but I mean, I guess people can use it."
  - "Digital money that I'm afraid of." It's not tangible, it sounds like a game of back and forth with money, but it's not real money."
  - "If I can't spend it or touch it, it's not money…. cryptocurrency is kind of a mystery. It's hard to explain to people and it's hard for people to explain to you."
- (5) Bitcoin/Form of money
  - "I think cryptocurrency… It's another form of cash. But it's different, because, like Bitcoin. So that's like their modern way of being able to pay for something."
  - "It is an online representation of capital.. represented by tokens."
- (9) Digital currency you buy, and it fluctuates in value like an investment depending on the market
  - "To me. It's electronic value. it's difficult to measure, because it's always changing… Sure, on paper you can make a lot of whatever unit that is, but more difficult to spend, more difficult to track way too volatile."
  - "It is an investment opportunity, but it is one that needs to be handled very carefully, because there's been so much controversy over it."

For the questions on how the fraud was first communicated (S1b, S2a, S3a, S4a, S5b, S6b. S7a) respondents were asked about their interpretation of key terms, including Social Media, Websites and Chat applications. Below provides the results across these questions.

What does Social Media mean?

- (1) A virtual message board with closed and open environments
- (1) A source of communication that is not always accurate
    - "Social media is a source of communication available to virtually everybody. There's no way to confirm the validity of social media… You can't take it as an accurate source of news or communication, unless you know the individuals that are posting personally, and you can validate for yourself that the information is accurate."
- (2) Entertainment
    - "Entertainment by YouTube or Facebook. I don't consider it business."
- (5) A way to communicate with friends and family or groups of people
    - "An online forum where you connect with others through a profile."
- (13) Social media platforms such as, Myspace, Facebook, TikTok, X, LinkedIn, Instagram where people connect [Please note that most comments for this category were not direct quotes. The Interviewers listed out the types of platforms mentioned.]
    - "It's a Facebook, anything you can communicate socially." "For me personally, I think of, you know, TikTok, Instagram, X, Twitter, YouTube. That's what I consider social media."

What did social media mean when answering this question?

The following are the major categories of responses concerning what social media meant to respondents when answering a specific module question.

- (8) Social media platforms such as Myspace, Facebook, TikTok, X, LinkedIn, Instagram where people connect and share information with others
    - "I mean, yeah, I guess it's kind of a broad term, because to me it's usually any place where people interact with each other. I would say, the main ones being Facebook, Twitter, or X. Now Instagram, Snapchat, and YouTube are the main ones."
    - "Social interaction with friends and family."
- (1) A place to buy or sell products
    - Occasionally buying products or dealing with vendors and companies. You know, posting information."
- (1) Entertainment
- (1) A place to warn others about experiences about a company
- (1) A way of providing warnings about scams
    - "[If] Facebook had knowledge of the scams that were going on, it might have made me feel better that the next time, I would watch out for things like that."

- (1) Social media platforms such as Myspace, Facebook, TikTok, X, LinkedIn, Instagram
    - "Well, my 1st thinking is, oh, anything online. But then I think, well, social media would be, probably we're more like Facebook and TikTok."
- (1) Social media is not always factual
    - "Discretionary when you are [using it]." R said she uses discretion as people can take a positive topic and give it a negative spin or vice versa.
- (2) Social media platforms such as Myspace, Facebook, TikTok, X, LinkedIn, Instagram
    - Respondent said "Instagram… Defining parts of the feed and the profile aspects."

In general - How is social media different from websites or other Internet applications?

- (1) Social media is something you have to belong to in order to use it
    - "Applications are broad spectrum. Anybody can access [it]. In a social media application, you have to belong to that group and log in. So, it's closed loop."
- (1) Social media is less formal
    - "I feel like it is less formal, and there's more you can do in terms of individual expression. People might be more willing to say something on social media, their opinions, than you would on an employment website." Employment websites "are more professional, in my opinion. It's more, you know, business polished."
- (1) Social media can be a dangerous place, you do not know who you are talking to while a website is more transparent
- (1) Social media is a way to get information, such as news stories, more quickly
- (1) Social media sites are easier to understand or use
- (1) Ownership by the people vs a specific organization
    - "To me, the website is the property of an entity… whereas social media is pretty much open to everyone"
- (1) Social media provides differing views on a topic
    - Well, generally social media platforms that I look on. If I click on the topic at hand, it'll show me differentiating views of that topic because it's tagged in each of the videos like positive and negatives this side and that side. So I feel like I get a more rounded view of it, on social media."
- (3) Social media is not regulated by facts
    - "It has been researched, and nobody has proved it correct. It is just out there." The respondent was referring to the content. She said people don't take responsibility or make sure things like punctuation is correct.
    - "Social media is a source of communication available to virtually everybody. There's no way to confirm the validity of social media… You can't take it as an accurate source of news or communication, unless you know the individuals that are posting personally, and you can validate for yourself that the information is accurate."
    - "There's no fact checking, it's like a free-for-all where a website is usually made by a company or a person so they can promote themselves, or you can find information about what they're offering."
- (4) Social media is interactive between users while websites are company or product related and information is more direct

    - “Other website applications is generally…. more of a one way stream of information, in my opinion… basic information that's coming one way like a new source or something that you're reading, that it's not really back and forth as much as it is this one way."
    - "I'm the receiver reading what was posted" - there's no way to interact with it. Social media is two-way, receiving and giving information.
- (8) Websites are for specific topics/goods/services/business or standard to everyone, while social media covers an array of topics and is a place to connect with friends and family, or groups of people
    - "The website provides information where whereas social media is just like where people can just hop on and just be on there."

What does Chat application mean?

- (1) A link is shared to a group of people who can type or video message each other (Messenger/WhatsApp)
- (1) Private conversations between two people that are not leaked to others
- (2) Don’t know or not familiar with Chat applications
    - "I don't have any of those. I've heard of WhatsApp but not Telegram or Signal."
- (3) Sharing information on social media or messaging with typed or video messaging
    - "A chat. Application is like how I would share on social media or like the SMS messaging"
    - "You can chat with video on Facebook facetime. There's WhatsApp, there's iChat, iMessage."
- (5) Types of AI, such as WhatsApp, Gemini or ChatGPT, that are used for entertainment, business, research, conversations, games
    - A chat application means an AI chat bot. "When I'm interacting with an artificial agent, I don't use WhatsApp, Telegram, or Signal for security purposes.
    - Chat box on a website for "Putting [things] on your resume, or asking about careers…"
- (6) Typed conversations with another individual online using a tablet, cell phone or computer.
    - "Chat is just another way to get something without sending a formal email a little more quickly."

- (6) An App
    - "I would classify most of them as Apps.. those that come to mind are WhatsApp, Facebook Messenger App, potentially IMessage, but that is between [being] texting and a chat app."
    - A phone application where you can see when people are active and looking at the conversation.
    - Chat application is something that happens on an iPhone, like WhatsApp. The respondent continued by clarifying chat applications have "security features like Session, Telegram… You can message with people."
    - "I would think any type of like messenger type service like WhatsApp, Facebook Messenger, SMS, or iChat those type of apps that are specifically designed just for chatting that don't have any other inherent value like, how YouTube has videos or Facebook has posts, or Instagram or Snapchat has pictures that goes with."
    - Respondent reported that it was the apps that were listed. They see them as international hangouts for scam artists, and they are suspicious if someone gives them a WhatsApp number.

Detailed Notes for Bias-Motivated Crime Cognitive Interviews

The next question is about why the offender may have targeted you. The reason may have been prejudice or bigotry toward those with your characteristics or religious beliefs, even if the offender mistakenly thought you had those characteristics or beliefs. This kind of reason is different from just being angry or wanting to get something from you.

Do you think the offender was targeting you because of prejudice or bigotry toward your race/ethnic background, your religion, your disability, your sexual orientation, your sex or any other of your personal characteristic?

Responses: **No (12) Yes (7)**

Discussion:

- **Out of the 7 "yes" responses:**
    - One respondent (a fraud victim) reported being targeted because he was perceived as belonging to a vulnerable group "*I tend to be targeted for these kind of scams or mlms [multi-level marketing scam], for example. I guess it's because of the economic disparity that they see. And they think, you know, we tend to be easier targets*."
    - One respondent (a victim of a serious violent assault – possibly sexual attack) said she was targeted because she was a female (but she did not think of it as a hate crime).
    - A third respondent was a stalking victim where offender is an ex.
    - The fourth respondent. "*I would say, because I am a Christian and I think that he I think he like kind of fed off of that meaning in the sense of like me being very nice and welcoming and so I think he, I think he thought that I was naive, maybe and that I just would kind of go with the flow*."
    - Of the remaining three:
        - One believes she was targeted because of her race – she described online bullying.
        - Another thought she was targeted due to her religion by her ex husband. "*I just think it was because religion..because we were going to the same church before, and he quit going there and then he keeps calling me witch and stuff.*"
        - And the final respondent (a fraud victim) said she thinks she was targeted because her name is the capital of a foreign country and people may think she belongs to a certain ethnic group and perhaps an easier target (for scams).

- **Respondents who answered "no" generally had a rationale for not thinking they were targeted due to prejudice or bigotry:**
    - The majority of respondents (n=10) were victims of scams (or attempted scams) and while some thought they may have been targeted due to their demographics, it was because they belong to a group thought to be vulnerable/easy targets. Some examples of respondent comments include:
        - *"I just feel like at that time I was just an easy target, meaning that I'm not a naive person. I can pick up on things pretty pretty quickly. But I think that during that time I had gotten an email. It looked legitimate."*
        - *"I was preyed upon because, I was a family friend. This individual preyed on friends and family predominantly for his Ponzi scheme to embezzle other people's money."*
        - *"No, unless they thought I was just stupid. You know that maybe they thought they had the edge over somebody, but outside of that no, I don't think it was because of race my sex orientation I think they just blanket everybody, and who they can get is who they can get."*
    - One described stalking behavior by an ex-partner but the respondent did not believe they were targeted due to prejudice or bigotry). *"He fixated on me, and then my cat. He just called about a week ago again. But it's all about this cat from a year ago, and then I talked to his, this woman that he's been living with. And she said, he's paranoid, delusional, schizophrenic."*
    - A final respondent had been harassed online (about a false claim of inappropriate contact with a student). *"If you look at it in this particular school situation, there's no way for this these young people to know in any of those things, for sure, right. I mean, they don't know my religion. They don't know. I mean, certainly they know my gender. They don't know my ethnic background, my racial background, although they could speculate."*

IF YES: What leads you to believe you were targeted in this way?

- **When asked what made them believe they think they were targeted in this way, only a few responses to this probe were clear:**
    - One woman was bullied on an online forum. She said her "avatar" is African American and this is the only black avatar on the forum. She thinks this is the reason she has been targeted.
    - *"Because when he saw me he looked me up and down more than he needed to. It took too long to load the bike into the. He was paying too much attention to me and not his job. The job was to get me home. That's not what he wanted to do, but I still had no clue. It would end up the way it did." "He wanted to attack a female that the impression I've gotten I felt, and I still feel that way. After the incident."* [this is the victim of violent assault – note that this respondent did NOT feel that this was a hate crime, but she did answer "yes" to the original question]
    - One woman said her ex-husband targets her because of her church attendance.
    - Another woman believes she was targeted due to her religion but not due to prejudice, but rather as a way to target/hook her: "his demeanor, his his whole persona. Everything was shifty…He was tending to to ask a lot of questions for Christianity …He was trying to

use that to kind of befriend us and befriend me, and he would always seem to know if my husband went to work."

- **Other responses were too vague to assess:**
  - *"it's just from my own research that I've kind of seen, and, you know, start to put together, you know, with these kinds of scams. From my own experience"*
  - *"The way they responded. And how, they added other people based on my own insecurities to try to get me to react."*
- **For those who answer 'no' respondents said their understanding of the question generally aligned with the intent of the question, although most of the respondents did not use the words "prejudice," "bigotry" or "hate" in their responses - examples:**
  - *"If it had anything to do with my race who I am, what I'm about. The color of my skin."*
  - *"an aspect of my identity, or you know, like a belief of mine, whether that be like I don't know, like religious or political"*
  - *"Targeted against someone of a particular race like Asian or African, American or Latino or Caucasian maybe even possibly An income bracket"*
  - *"asking about- were you targeted because of your beliefs or religion or your disability"*
- **Three of the twelve respondents specifically mentioned "prejudice," "bigotry" or "hate" in their responses:**
  - *"I would think of it as being an individual who is experiencing hate crime, in practice."*
  - *"because of having prejudiced against their religious beliefs, or or where they're from"*
  - A final respondent described a former coworker who faced prejudicial treatment due to obesity.
- **For those who said 'no' to the question, responses on what 'targeting you because of prejudice or bigotry' mean?**
  - *"It means that if any individual …has a hatred or a prejudice towards a certain group. They're looking to prey upon those people and punish them, or feel like they are getting something over on a group of people that they dislike distrust or have any ill feelings towards."*
  - *"prejudice would be being against my nationality, my race, my color, who I am, my gender."*
  - One said the probe triggered memories from life, of events such as what happened in 2020 with George Floyd.
  - *"my understanding of like prejudice would be like some kind of I guess, like vendetta against you for… like an aspect of your identity or you know some like outward yeah, I guess like piece of identity. That is something that like offender, I guess could easily latch onto"*
- **Some were focused more on the "why targeted":**
  - *"It means that you're the specific one that they want to target because of your personality, your race, your religion, or your disability, because they think they can take advantage of you."*
  - *"It means that they don't like me, and that they want to bother me."*
  - *"somebody doesn't like somebody, you know, or has an issue with somebody just based on their genetic background"*
- **One listed different subpopulations but did not attend to the words "prejudice/bigotry":**

- *"I think in terms of first, probably race. I think, in terms of culture and sexual orientation. I even think in terms of income level, you know, not just not just what we can visibly see, but what we also perceive about that person"*

- **Examples of how respondents would know they were targeted (among the 'no' respondents) – "language" seems to be the only common theme:**
  - *"anything from verbal statements, body language, you know, avoidance things that you know may maybe you know rumor innuendo give me"*
  - *"using offensive language"*
  - *"how they communicate with you"*
  - *"I think if if the person would maybe possibly keep asking, I would think personally like racial questions like, are you African American?"*
- **One respondent said their own feelings would drive whether they felt they were being targeted:**
  - *"If you feel offended by it, I think then you could, you know, reasonably be reasonably assume you're being targeted like, I was saying, if it's something that you know, that you posters like a clear part of your identity, or who you are, what you believe in. I think then you could. You could assume that you're being targeted"*

- **One respondent said that if law enforcement identified a pattern they would know they had been targeted:**
    - *"I don't think the individual would know. but I do think that it would become apparent if you could trace back to all the persons that they've reached out to. If we're talking about a scam situation where the FBI or the police or CIA had access to their information. And was it consistent throughout? Did they target particular people who were black, who were Hispanic, who were at a certain income level, a certain age, a certain religion."*
- **There was a wide variety of answers when asked what targeting because of their sex means. Most included both gender and sexual orientation in their responses:**
    - *"That means to me if someone identifies as male, female or non-binary."*
    - *"If we're talking about targeting somebody, I think of females. And I would also throw in there the probably gays as well, not males, but because, again. if it's a prejudiced response, then they're going to be targeting somebody they believe is going against their norm."*
    - *"That means if you target somebody because they're either homosexual or transgender or you know, heterosexual. You target a particular person who is of that particular sexual orientation because you did not like them or believe what they're doing like you don't believe that gays should be married and you target them"*
    - *"I would think of it as like gender I mean targeting somebody due to their gender, whether that be the gender they were assigned at birth, or their like current gender identity."*
- **Only three respondents mentioned male/female without also bringing in gender or sexual orientation.**
- **Most respondents were able to come up with "other" examples when asked what 'other personal characteristics' means:**
    - Appearance including weight, tattoos, piercings, eye color, hair color.
    - Socio economic/ income status.
    - Age (elderly).
    - Speech impediments.
    - Low Intelligence.
    - Behaviors such as smoking, drug use.

Appendix I

Reviewers Consulted on the Cybercrime Questionnaires

Appendix I
Reviewers Consulted on the Cybercrime Questionnaires

Lynn A. Addington, Ph.D.
Professor of Justice, Law, and Criminology
American University

Erica R. Fissel, Ph.D.
Research and Evaluation Manager
ICF

Thomas Holt, Ph.D.
Professor, School of Criminal Justice
Michigan State University

Jin Ree Lee, Ph.D.
Assistant Professor, Department of Criminology, Law and Society
George Mason University

Marie-Hellen Maras, DPhil
Professor in the Center for Cybercrime Studies
John Jay College of Criminal Justice