Attachment list

Attachment 1: 2021 ITS questionnaire

Attachment 2: Title 34, United States Code, Section 10132 of the Justice Systems Improvement Act of 1979

Attachment 3: 60-day Federal Registry notice

Attachment 4: 30-day Federal Registry notice

Attachment 5: “Identity Theft: What to know, What to Do” brochure

Attachment 6: Assessment of State Identity Theft Laws

Attachment 7: Identity Theft Supplement Secondary Data Analysis, Recommendations, and Next Steps

Attachment 8: Cognitive Interviewing for the National Crime Victimization Survey (NCVS) Identity Theft Supplement (ITS)

Attachment 9: Identity Theft Screener Online Testing: Final Report

2021 Identity Theft Supplement

SECTION A: SCREENER QUESTIONS

INTRO 1: **Now, we are conducting a special supplement on identity theft and I would like to ask you questions. 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. We estimate these questions will take from 5 to 15 minutes depending on your circumstances. The U.S. Census Bureau is required by law to keep your information confidential.**

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.

1. **Have you ever had a checking or savings account in your name through a bank or financial institution?**

YES
NO (Skip to Q5)

2. **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
NO (Skip to Q5)

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

YES
NO (Skip to Q5)

4a**. Did this most recently happen in 2021 or 2020?**

1. 2021
2. 2020

4b**. 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.

5. **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
NO (Skip to Q9)

6. **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
NO (Skip to Q9)

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

YES
NO (Skip to Q9)

8a. **Did this most recently happen in 2021 or 2020?**

1. 2021
2. 2020

8b. **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.

9a. **Have you ever had at least one email account, such as Gmail or Outlook, or social media account such as Facebook or Instagram?**

YES
NO (Skip to Q11)

9b. **Has anyone EVER used your email or social media account without your permission to pretend to be you?**

YES
NO (Skip to Q11)

10a. **Has this happened during the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today?**

YES
NO (Skip to Q11)

Which account was used without your permission…

10b. **Email account, such as Gmail or Outlook?** YES NO

10c. **Social media account, such as Facebook or Instagram?** YES NO

HARD EDIT CHECK: If Q10a is marked "yes" and BOTH Q10b and Q10c are marked "no"

You reported either your email or social media account was misused in Q10a, but didn't identify any of these accounts in Q10b or Q10c. Either Q10a should be changed to reflect that no email or social media accounts were misused in the past 12 months, or either email or social media account should be identified by selecting '1' (yes) to one of the following questions in Q10b or Q10c.

10d. **Please think about the most recent time someone misused [this/one of these] account(s).**

Did this most recently happen in 2021 or 2020?

1. 2021
2. 2020

10e. **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.

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

- **telephone or internet accounts;**
- **utilities accounts, such as cable, gas, or electric;**
- **medical insurance accounts, such as Medicare or a health spending account;**
- **entertainment accounts for music, movies, or games;**
- **online payment accounts like PayPal or Venmo; or**
- **some other accounts?**

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

YES
NO (Skip to Q15)

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

YES
NO (Skip to Q15)

13. **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…**

13a. **Telephone or internet accounts?** YES NO
13b. **Utilities accounts, such as cable, gas, or electric accounts?** YES NO
13c**. Medical insurance accounts, such as Medicare or a health spending account?** YES NO
13d**. Entertainment accounts, such as for movies, music, or games?** YES NO
13e. **Online payment accounts, such as PayPal or Venmo?** YES NO
13f. **Some other type of account?** YES NO
[If yes] **What other types of accounts were misused?** ___________

(If any 13a-13f = yes, ask Q14a; else skip to Q15)

HARD EDIT CHECK: If Q12 is marked “yes” and ALL of Q13a through Q13f are marked “no”

You reported one or more of your existing accounts were misused in Q12, but didn't identify any of these existing accounts in Q13a, Q13b, Q13c, Q13d, Q13e, or Q13f. Either Q12 should be changed to reflect that no existing accounts were misused in the past 12 months or the type of existing account should be identified by selecting '1' (yes) to one or more of the following questions in Q13a, Q13b, Q13c, Q13d, Q13e, or Q13f.

14a**. Please think about the most recent time someone misused [this/one of these] existing accounts.**

Did this most recently happen in 2021 or 2020?

1. 2021
2. 2020

14b. **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.

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

- **checking or savings account;**
- **credit card accounts;**
- **email accounts, such as Gmail or Outlook;**
- **social media accounts, such as Facebook or Instagram;**
- **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
NO (Skip to Q19)

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

YES
NO (Skip to Q19)

17**. With this next question, I'm going to read a list of 11 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…

17a. **New checking or savings accounts?** YES NO
17b. **New credit card accounts?** YES NO
17c. **New email accounts such as Gmail or Outlook?** YES NO
17d. **New social media accounts, such as Facebook or Instagram?** YES NO
17e. **New telephone or internet accounts?** YES NO
17f. **New utilities accounts, such as cable, gas, or electric?** YES NO
17g**. New entertainment accounts, such as for music, movies, or games?** YES NO
17h. **New loans or mortgages?** YES NO
17i. **New insurance policies?** YES NO
17j. **New online payment accounts, such as PayPal or Venmo?** YES NO
17k. **Some other type of new account?** YES NO
[If yes] **What other type of new account was opened?** __________

(If any 17a-17k = yes, ask Q18a; else skip to Q19)

HARD EDIT CHECK - If Q16 is marked "yes" and ALL of Q17a through Q17k are marked "no"

Responses to questions Q17a, Q17b, Q17c, Q17d, Q17e, Q17f, Q17g, Q17h, Q17i, Q17j, and Q17k are inconsistent with answer to Q16 = Yes. Either the response to Q16 is incorrect or one or more of the following questions Q17a, Q17b, Q17c, Q17d, Q17e, Q17f, Q17g, Q17h, Q17i, Q17j, or Q17k should be marked '1' (Yes).

18a. **Please think about the most recent time someone successfully opened [this/one of these] new accounts.**

Did this most recently happen in 2021 or 2020?

1. 2021
2. 2020

18b**. 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.

19. **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
NO (Skip to Check Item A)

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

YES
NO (Skip to Check Item A)

21. **In which of the following ways has someone used your personal information during the past 12 months? Was your personal information used…**

21a. **To file a fraudulent tax return?** YES NO
21b. **To get medical treatment?** YES NO
21c. **To apply for a job?** YES NO
21d. **To provide false information to the police to conceal their identity?** YES NO
21e. **To provide false information to some other government authority such as the Department of Motor Vehicles?** YES NO
21f. **To apply for government benefits?** YES NO
21g. **In some other way not already mentioned?** YES NO
[If yes] **How else was your personal information misused?** __________

(If any 21a-21g = yes, ask Q22a; else skip to Check Item A)

HARD EDIT CHECK: If Q20 is marked “yes” and ALL of Q21a through Q21g are marked “no”

Response to Q20 is inconsistent with responses to Q21a, Q21b, Q21c, Q21d, Q21e, Q21f, and Q21g. Either the response to Q20 is incorrect or one or more of the questions Q21a, Q21b, Q21c, Q21d, Q21e, Q21f, and Q21g should be answered '1' (Yes).

22a. **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 2021 or 2020?

1. 2021
2. 2020

22b. **And in what month?** ____________________________ Month (01-12)

If you don't know, please provide your best estimate.

CHECK ITEM A
Is "no," "don't know," "refused," or "blank" marked for Q2, Q6, Q9b, AND "no," "don't know," or "refused," marked for Q11, Q15, and Q19?
YES – Skip to Section H
NO – Skip to Check Item B

CHECK ITEM B
Is "no," "don't know," "refused," or "out of universe" marked for Q3, Q7, Q10a, Q12, Q16, AND Q20?
YES – Skip to Section G
NO – Skip to Check Item C

CHECK ITEM C
Is only one response marked "yes" from questions Q3, Q7, Q10a, Q12, Q16, AND Q20?
YES – Skip to Q23
NO – Skip to Check Item D

CHECK ITEM D
Is the most recent Month/Year provided more than once in Q4a/b, Q8a/b, Q10d/e, Q14a/b, Q18a/b, and Q22a/b (e.g. if respondent answered 2021, May in both Q4a/b and Q8a/b, select "yes.")?
YES – Skip to Q24
NO – Ask Q23

23**. You said that in <**autofill most recent month/year provided in Q4a/b, Q8a/b, Q10d/e, Q14a/b, Q18a/b OR Q22a/b**> someone <**autofill most recent type of ID theft from Q2, Q6, Q9b, Q11, Q15, OR Q19**>. Was this the result of one related incident or was your personal information misused multiple times in separate unrelated incidents? An incident of identity theft occurs when your information is stolen. A stolen credit card or debit card may be used multiple times but this should be considered a single incident.**

1. Multiple Incidents (Skip to Section B, Intro 1)
2. One related incident (Skip to Section B, Intro 2)

If the respondent states, "I don't know," instruct the respondent to select what they believe to be the best response.

24. **You said that in <**autofill most recent month/year provided in Q4a/b, Q8a/b, Q10d/e, Q14a/b, Q18a/b OR Q22a/b**> someone <**autofill most recent type of ID theft from Q2, Q6, Q9b, Q11, Q15, OR Q19**>. Were these the result of one related incident or was your personal information misused multiple times in separate unrelated incidents? An incident of identity theft occurs when your information is stolen. A stolen credit card or debit card may be used multiple times but this should be considered a single incident.**

1. Multiple Incidents (Ask Q25)
2. One related incident (Skip to Section B, Intro 2)

If the respondent states, "I don't know," instruct the respondent to select what they believe to be the best response.

25**. Which of these misuses of your personal information happened during the most recent incident?**
(Mark all that apply, and only read response items that match autofill "yes" responses from Q2, Q6, Q9b, Q11, Q15, and Q19)

1. **Misuse of an existing checking and/or savings account**
2. **Misuse of an existing credit card account**
3. **Misuse of an existing email or social media account**
4. **Misuse of other types of existing accounts**
5. **Misuse of personal information to open a NEW account**
6. **Misuse of personal information for other fraudulent purpose.**

(Skip to Section B, Intro 1)

SECTION B. HOW/WHEN IDENTITY THEFT DISCOVERED

INTRO 1: *For those with more than one incident*: **I will now ask you to consider only the most recent incident of identity theft that you experienced during the past 12 months.**
For the next series of questions, please think about the [autofill most recent type of ID theft from Q25 or ("yes" response from Q2, Q6, Q9b, Q11, Q15, OR Q19)] **you experienced in** [autofill most recent month/year from Q4a/b, Q8a/b, Q10d/e, Q14a/b, Q18a/b, or Q22a/b]**.**

INTRO 2**:** *For those with a single incident* **For the next series of questions, please think about the** [autofill "yes" responses from (Q2, Q6, Q9b, Q11, Q15, or Q19] **you experienced in** [autofill month/year from Q4a/b, Q8a/b, Q10d/e, Q14a/b, Q18a/b, or Q22a/b]**.**

26. **How did you FIRST find out about the most recent incident of misuse of your personal information?**
(*SELECT A SINGLE RESPONSE*)

DISCOVERED BY RESPONDENT

1. I contacted the credit card company or bank to report a theft and was told that fraudulent charges had already been made.
2. I noticed money missing from my account.
3. I noticed fraudulent charges on my account.
4. I received merchandise or a card that I did not order.
5. I had problems using my card or account because it was declined, closed, or had insufficient funds.
6. I applied for credit, a bank account or loan, utilities such as cable service, employment, or government benefits, etc. and had problems.
7. I checked my credit report.
8. I received a bill that I did not owe.
9. I had a problem filing my income taxes.

NOTIFIED BY FINANCIAL INSTITUTION

10. Credit card company or bank contacted me about suspicious activity on my account.
11. My credit monitoring service contacted me.
12. A collection agency, credit card company, credit bureau, or other financial institution contacted me about late or unpaid bills.

NOTIFIED BY OTHER PARTY

13. A law enforcement agency notified me.
14. A company or agency notified me.

OTHER

15. Discovered in another way - (specify)

27. **In what year and month did you first discover that someone had misused your personal information?**

Enter year: __________

1. **2021**
2. **2020**
3. **2019 or prior**

Enter month: __________ Month (01-12)

SOFT EDIT CHECK: Respondent gave month/year in Q27 that is prior to the most recent month/year of Q4a/b, Q8a/b, Q10d/e, Q14a/b, Q18a/b, or Q22a/b.

Respondent reported that they discovered the most recent incident identity theft prior to the month/year that it occurred. Return to Q27 (WHEN_DISCOVERED_YEAR) to correct the date or accept the inconsistency.

28. **How long had your personal information been misused before you discovered it?**

1. One day or less (1-24 hours)
2. More than a day, but less than a week (more than 24 hours-6 days)
3. At least a week, but less than one month (7-30 days)
4. One month to less than three months
5. Three months to less than six months
6. Six months to less than one year
7. One year or more
8. Don’t know

29. **Do you have any idea HOW your personal information was obtained, even if you are not completely certain?**

YES
NO (Skip to Q31)

30. **How do you think your personal information was obtained?**
(SELECT A SINGLE RESPONSE)

1. I lost an item that included my personal information.
2. My wallet, checkbook, or purse was stolen.
3. My personal information recorded on paper documents was stolen from a place where it was stored or placed such as my office or trash.
4. It was accessed electronically from my work or home computer, cell phone, tablet, or other electronic device.
5. It was stolen during an online purchase/transaction.
6. Someone stole it during an in-person purchase/transaction, including using a skimmer or card reader.
7. I responded to a scam email/phone call.
8. My personal information was stolen from my personnel or human resources files at my place of employment.
9. It was stolen from an office/company such as a financial institution, retailer, service provider, or restaurant.
10. Obtained in another way (specify)_____________

SECTION C. VICTIM RESPONSE

31. **Were you in contact with anyone at a credit card company, bank, credit union, or other financial institution about <the/the most recent> misuse of your personal information**?

YES
NO (Skip to Q35)

32. **Did you contact a credit bureau about the misuse of your personal information?**

YES
NO (Skip to Q35)

33. **At any credit bureau that you contacted, did you...**

a**. Request your credit report?** YES NO
b. **Request corrections to your credit report?** YES NO
c**. Place a fraud alert on your credit report?** YES NO DON'T KNOW

Did you...

d**. Place a freeze on your credit report, which prevents the credit bureaus from sending your credit report to anyone without your permission?** YES NO
e. **Take some other action with the credit bureau?** YES NO
[If yes] **What else did you do when you contacted the credit bureau? __________**

34. **After you told a credit bureau that your personal information had been misused, how satisfied were you with the credit bureau's response? Were you very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?**

1. Very satisfied
2. Somewhat satisfied
3. Somewhat dissatisfied
4. Very dissatisfied
5. Don't know

35. **Did you contact any law enforcement agencies, such as the local police, a sheriff's office or a federal law enforcement agency, to report <the/the most recent> misuse of your personal information?**

YES (Ask Q36)
NO (Skip to Q40)

36. **Did the law enforcement agency take a police report from you about the misuse of your personal information?**

YES (Ask Q37)
NO (Skip to Q38)

37. **Did you receive a copy of that police report?**

YES (Skip to Check Item E)
NO (Skip to Q38)

CHECK ITEM E
Does Q32 = “Yes”?
YES – Ask Q37a
NO – Skip to Q38

37a. **Did you send a copy of that police report to the credit bureau that you contacted?**

YES
NO

38. **How satisfied were you with the law enforcement agency’s response when you reported the misuse of your personal information? Were you very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?** (ENTER A SINGLE RESPONSE)

1. Very satisfied (Skip to Q41)
2. Somewhat satisfied (Skip to Q41)
3. Somewhat dissatisfied (Ask Q39)
4. Very dissatisfied (Ask Q39)
5. Don’t know (Skip to Q41)

39. **Why were you dissatisfied with the law enforcement agency’s response?** (MARK ALL THAT APPLY)

1. Police didn’t or couldn’t do anything
2. Police only filled out a report
3. Police said the crime did not fall in their jurisdiction
4. Police gave me no information on what I should do about the crime
5. Police never got back in contact with me/never learned outcome
6. Didn’t feel my concerns/complaints were taken seriously
7. Police unable to catch the
8. Other (specify) __________

40. **We would like to learn more about why people who experience identity theft do not report it to law enforcement. Why did you decide not to contact a law enforcement agency?** (MARK ALL THAT APPLY)

DIDN'T KNOW I COULD

1. Didn't know that I could report it
2. Didn't think about reporting it
3. Didn't know what agency was responsible for identity theft crimes

NOT IMPORTANT ENOUGH

4. I didn't lose any money
5. Not important enough to report/small loss

HANDLED IT ANOTHER WAY

6. Took care of it myself
7. Credit card company/bank/other organization took care of problem

DIDN'T THINK THE POLICE COULD HELP

8. Didn't think police would do anything
9. Didn't want to bother police
10. Didn't find out about the crime until long after it happened/too late for police to help
11. Couldn't identify the offender or provide much information that would be helpful to the police
12. Occurred in another state or outside of the U.S.

PERSONAL REASONS

13. The person responsible was a friend or family member and I didn't want to get them in trouble
14. Too inconvenient/didn't want to take the time

OTHER

15. Other (specify) ___________

41. **Next, I'm going to read you a list of other people and organizations that someone might contact when their personal information is misused. Which of the following people or organizations, if any, did you contact about <the/the most recent> misuse of your personal information? Did you...**

a. **Contact the business or organization associated with the misuse?** YES NO

b. **Hire a lawyer?** YES NO

c. **Contact a State or local government consumer affairs agency, such as the State Attorney General's office?** YES NO

d. **Contact the Federal Trade Commission?** YES NO

e. **Contact a nongovernment consumer agency, such as the Better Business Bureau or the National Consumer League?** YES NO

f. **Contact a government agency that issues documents like driver's licenses or Social Security cards?** YES NO

g. **Contact a nongovernment agency that issues documents, such as insurance cards?** YES NO

h. **Contact a credit monitoring service or identity theft insurance company?** YES NO

i. **Contact an office or agency – other than the police – that deals with victims of crime?** YES NO

j. **Contact some other group or organization not already mentioned?** YES NO

[If yes] **What other group or organization did you contact?**__________

SECTION D. VICTIM IMPACT

42. **The misuse of personal information affects people in different ways. Next, I would like to ask you some questions about how <the/the most recent> misuse of your personal information may have affected you.**

Did the misuse of your personal information lead you to have significant problems with your job or schoolwork or trouble with your boss, co-workers, or peers?

YES
NO

43. **Did the misuse of your personal information lead you to have significant problems with family members or friends, including getting into more arguments or fights than you did before, not feeling you could trust them as much, or not feeling as close to them as you did before?**

YES
NO

44. **How distressing was the misuse of your personal information to you? Was it not at all distressing, mildly distressing, moderately distressing, or severely distressing?**
(ENTER A SINGLE RESPONSE)

1. Not at all distressing (Skip to Section E)
2. Mildly distressing (Skip to Section E)
3. Moderately distressing (Skip to Check Item F)
4. Severely distressing (Skip to Check Item F)

CHECK ITEM F
Is “yes” marked in Q42 or Q43 or are categories ‘3' or ‘4' marked in Q44?
YES – Ask Q45
NO – Skip to Section E

45. **Did you feel any of the following ways for A MONTH OR MORE because of <the/the most recent> misuse of your personal information?**

a. **Worried or anxious?** YES NO
b. **Angry?** YES NO
c. **Sad or depressed?** YES NO
d. **Vulnerable?** YES NO
e. **Violated?** YES NO
f. **Like you couldn’t trust people?** YES NO
g. **Unsafe?** YES NO
h. **Some other way?** YES NO
[If yes] **What other way did the misuse of your personal information make you feel**? ______

(If any 45a-45h = yes, ask Q46a; else skip to Q47)

46a. **Did you seek any kind of professional help for the feelings you experienced as a result of <the/the most recent> misuse of your personal information?**

YES (Ask Q46b)
NO (Skip to Q47)

46b. **What kind of professional help did you seek?** (MARK ALL THAT APPLY)

1. Counseling/therapy
2. Visited primary care or private physician’s office
3. Visited ER/hospital/walk-in clinic
4. Other specify __________

47. **Did you experience any of the following physical problems caused by <the/the most recent> misuse of your personal information for A MONTH OR MORE? Did you experience...**

a. **Headaches?** YES NO
b. **Trouble sleeping?** YES NO
c. **Changes in your eating or drinking habits?** YES NO
d. **Upset stomach?** YES NO
e. **Fatigue?** YES NO
f. **High blood pressure?** YES NO
g. **Muscle tension or back pain?** YES NO
h. **Some other problem?** YES NO
[If yes] **What other physical problems did you experience for A MONTH OR MORE?** ________

(If any 47a-47h = yes, ask Q48; else skip to Section E)

48. **Did you seek any kind of professional or medical help for the physical problems you just reported?**

YES (Ask Q49)
NO (Skip to Section E)

49. **What kind of professional or medical help did you seek?** (MARK ALL THAT APPLY)

1. Counseling/therapy
2. Visited primary care or private physician's office
3. Visited ER/hospital/walk-in clinic
4. Other specify ___________

SECTION E. OFFENDER

50. **Do you know, or have you learned, anything at all about the person or persons who <most recently> misused your personal information?**

YES (Ask Q51)
NO (Skip to Section F)

51. **How well did you know this person or these people at the time of the incident? For example, was it a family member, friend, acquaintance, salesperson, or somebody else?**

RELATIVE

1. Spouse (ex-spouse)
2. Parent or step-parent
3. Brother or sister or step-brother/step-sister
4. Child or step-child
5. Other relative (specify) __________

NONRELATIVE

6. Boyfriend or girlfriend (ex-boyfriend or ex-girlfriend)
7. Friend or ex-friend
8. Housemate or roommate
9. Neighbor
10. Co-worker (current or former, supervisor or other employee)
11. Someone working in my home (babysitter, housecleaner, etc.)
12. Casual acquaintance
13. Salesperson
14. Food service attendant such as a waiter/waitress, server, or barista
15. Other non-relative (specify) __________

STRANGER

16. Do not recall ever meeting or seeing the person before

SECTION F. FINANCIAL IMPACT

52. **What is the approximate total dollar value of what someone obtained when they misused your personal information <during the most recent incident>? Include the value of goods, services, credit, loans, cash, and anything else the person may have obtained.**
(IF THE RESPONDENT PROVIDES A RANGE, ASK THE RESPONDENT TO PROVIDE THEIR BEST TOTAL DOLLAR VALUE ESTIMATE INSTEAD OF A RANGE)

RECORD THE ESTIMATED AMOUNT. $__________.00 (IF OVER $1,000, PROBE: I just want to verify that the total amount is (INSERT AMOUNT RESPONDENT INDICATED)

If response = $0, skip to Q54b.

53**. Of this <autofill: amount of loss from Q52> that was obtained during <the/the most recent> misuse of your personal information, how much of that money did you personally lose? That is, how much did you lose that was not covered or reimbursed by insurance, bank, or credit card company?**

RECORD ESTIMATED AMOUNT. $___________.00 (IF “NONE,” PROBE: Just to confirm, you didn’t personally lose anything?)

HARD EDIT CHECK - If Q53 > Q52

The respondent just reported their personal loss was greater than the total dollar amount obtained. Return to PERSONAL_LOSS and fix the amount or reduce the amount of personal loss so that it doesn't exceed the amount reported in TOTAL_LOSS.

CHECK ITEM G
Is answer to Q53 equal to $0 (the respondent did not lose anything or did not have to pay anything personally)?
YES – Skip to Q54b
NO – Ask Q54a

54a. **Other than the costs you already told me about,** <amount from Q53**>, how much, IF ANY, additional costs did YOU incur as a result of <the/the most recent> misuse of your personal information? Include costs for things such as legal fees, overdraft fees, and any miscellaneous expenses, such as postage, phone calls, or notary fees. Do not include lost wages.**

OR

54b. **How much, IF ANY, costs did YOU incur during <the/the most recent> misuse of your personal information? Include costs for things such as legal fees, overdraft fees, and any miscellaneous expenses, such as postage, phone calls, or notary fees. Do not include lost wages.**

RECORD ESTIMATED AMOUNT. $___________.00 SKIP to Q55
DO NOT INCLUDE COSTS WHICH WERE REIMBURSED.

(IF OVER $1,000, PROBE: I just want to verify that the total amount is (INSERT AMOUNT RESPONDENT INDICATED).

55. **Have you been successful in clearing up all of the financial and credit problems associated with <the/the most recent> misuse of your personal information?**

YES (Ask Q56)
NO (Skip to Q57)
DON'T KNOW (Skip to Q57)

56. **How long did it take you to clear up all of the financial and credit problems associated with the misuse after you discovered it?** (ENTER A SINGLE RESPONSE.)

1. One day or less (1-24 hours)
2. More than a day, but less than a week (more than 24 hours-6 days)
3. At least a week, but less than one month (7-30 days)
4. One month to less than three months
5. Three months to less than six months
6. Six months to less than one year
7. One year or more

57. **How many hours <did you spend/have you spent> clearing up financial or credit problems associated with <the/the most recent> misuse of your personal information? If you don't know, please provide your best estimate.**

__________ Number of hours

58. **Other than anything we have already talked about, have you experienced any of the following problems as a result of <the/the most recent> misuse of your personal information? Have you…**

a. **Had credit related problems, such as having to repeatedly correct the same information on your credit report, being turned down for credit or loans, changes in your credit score, or having to pay higher rates?** YES NO
b. **Had banking problems, such as being turned down for a checking account or having checks bounce?** YES NO
c. **Had debt collectors or collections departments contact you?** YES NO

d. **Had utilities cut off or been denied new service?** YES NO

As a result of the misuse of your personal information, have you...

e**.** **Been turned down for a job or lost a job?** YES NO
f. **Had a lawsuit filed against you?** YES NO
g. **Been the subject of an arrest or criminal proceedings?** YES NO
h. **Had some other type of problems?** YES NO
[If yes] **What other type of problem did you experience**? __________

CHECK ITEM H
Did respondent experience more than one incident of identity theft during the past 12 months (Q23=1 or Q24=1)?
YES – Ask Q59
NO – Skip to Section G

59. **For the next few questions, please think about ALL of the misuses of your personal information during the last year, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR]. Including every incident that occurred over the past 12 months, not just the most recent, what is the approximate total dollar value of what someone obtained while misusing your personal information? Include the value of goods, services, credit, loans, cash, and anything else the person may have obtained.**

(IF THE RESPONDENT PROVIDES A RANGE, ASK THE RESPONDENT TO PROVIDE THEIR BEST TOTAL DOLLAR VALUE ESTIMATE INSTEAD OF A RANGE. THIS INCLUDES "WHAT SOMEONE OBTAINED" REGARDLESS OF WHETHER THE RESPONDENT WAS REIMBURSED.)

RECORD THE ESTIMATED AMOUNT. $__________.00

HARD EDIT CHECK - If Q59 < Q52

The respondent reported less than <the/the most recent> incident of misuse of their personal information, PROBE:

I just want to verify that the total amount is <autofill: amount from Q59>.

The respondent just reported their total dollar value of what the offender obtained from the most recent misuse of their personal information was greater than the total dollar value of what the offender obtained from every incident that occurred over the past 12 months. Return to TOTAL_EVERY_INCIDENT and fix the amount or reduce the amount of TOTAL_LOSS from the most recent misuse of their personal information, so that it doesn't exceed the amount reported in TOTAL_EVERY_INCIDENT.

60. **Not counting the <**autofill: amount from Q59**> dollars that were obtained during ALL incidents of identity theft in the past 12 months, what were the total additional costs, that YOU incurred as a result of the misuses of your personal information? Include costs for things such as legal fees, overdraft fees, and any miscellaneous expenses, such as postage, phone calls, or notary fees. Do not include lost wages.**

RECORD ESTIMATED AMOUNT. $___________.00 DO
NOT INCLUDE COSTS WHICH WERE REIMBURSED.

ANY RESPONSE – Skip to Section G after the following Hard Edits performed

HARD EDIT CHECK - If Q60 < Q54a

The respondent reported less than value of additional costs incurred from <the/the most recent> Incident of misuse of their personal information, PROBE:

I just want to verify that the total amount is <autofill: amount from Q60>.

The respondent just reported the additional costs incurred from the most recent misuse of their personal information was greater than the additional costs incurred from every incident that occurred over the past 12 months. Return to TOTAL_ADD_COSTS and fix the amount or reduce the amount of ADD_COSTS_INCUR from the most recent misuse of their personal information, so that it doesn't exceed the amount reported in TOTAL_ADD_COSTS.

HARD EDIT CHECK - If Q60 < Q54b

The respondent reported less than value of additional costs incurred from <the/the most recent> Incident of misuse of their personal information, PROBE:

I just want to verify that the total amount is <autofill: amount from Q60>.

The respondent just reported the additional cost incurred from the most recent misuse of their personal information was greater than the additional costs incurred from every incident that occurred over the past 12 months. Return to TOTAL_ADD_COSTS and fix the amount or reduce the amount of NO_PERSONAL_LOSS from the most recent misuse of their personal information, so that it doesn't exceed the amount reported in TOTAL_ADD_COSTS.

SECTION G. LONG-TERM VICTIMIZATION AND CONSEQUENCES

INTRO**: Now I'm going to ask you to think about any identity theft that may have occurred more than 12 months ago, that is, any time before [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR].** <*If at least (one or more of Q2, Q6, Q9b, Q11, Q15, or Q19 = 1) AND (one or more of Q3, Q7, Q10a, Q12, Q16, AND Q20 = 1)*, **Don't think about the incident we have just been talking about when you answer the next question.**>
Again, 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.

CHECK ITEM I
Is ("yes" marked for any of Q2, Q6, Q9b, Q11, Q15, or Q19) AND ("yes," "don't know," "refused," or "out of universe" marked for Q3, Q7, Q10a, Q12, Q16, AND Q20)?
YES – Skip to Q61
NO – Skip to Q62

61. **Not including the past 12 months, has anyone EVER, without your permission:**

- **misused one of your existing accounts,**
- **used your personal information to open a new account,**
- **or used your personal information for some other fraudulent purpose, such as getting medical care, a job, government benefits or something else?**

YES
NO (Skip to Section H)

62. **At any point during the past 12 months did you experience credit or other financial problems, legal problems, relationship problems with family or friends, problems at work or school, physical problems, or emotional distress as a result of the identity theft that happened to you more than 12 months ago?**

YES
NO (Skip to Section H)

63. **During the past 12 months, have you experienced any of the following consequences as a result of the identity theft that occurred more than 12 months ago? Have you had…**

a. **Significant problems with your job or schoolwork, or trouble with your boss, co-workers, or peers during the past 12 months?** YES NO

b. **Significant problems during the past 12 months with family members or friends, including getting into more arguments or fights than you did before, not feeling you could trust them as much, or not feeling as close to them as you did before?** YES NO

As a result of the identity theft that occurred more than 12 months ago, have you...

c. **Experienced any of the following feelings for a month or more during the past 12 months: worry, anger, sadness or depression, vulnerability, feeling violated like you couldn't trust people, or feeling that you were unsafe?** YES NO

d. **Had physical problems during the past 12 months resulting from the misuse of your personal information, such as headaches, trouble sleeping, changes in your eating or drinking habits, an upset stomach, high blood pressure or some other physical problem?** YES NO

e. **Had credit related problems during the past 12 months, such as having to repeatedly correct the same information on your credit report, being turned down for credit, loans or having to pay higher rates?** YES NO

f. **Had banking problems during the past 12 months, such as being turned down for a checking account or having checks bounce?** YES NO

As a result of the identity theft that occurred more than 12 months ago, have you...

g. **Had debt collectors or collections departments contact you during the past 12 months?** YES NO

h. **Had utilities cut off or been denied new service during the past 12 months?** YES NO

i. **Been turned down for a job or lost a job during the past 12 months?** YES NO

j. **Had legal problems, such as having a lawsuit filed against you or being the subject of an arrest or criminal proceedings, during the past 12 months?** YES NO

k. **Had some other type of problems during the past 12 months?** YES NO

[If yes] **What other types of problems have occurred during the past 12 months? __________**

SECTION H. PREVENTATIVE BEHAVIORS

64. **Now I'm going to ask you about any actions taken to prevent someone from obtaining your personal information. In the past 12 months, that is since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you:**

a. **Checked your credit report?** YES NO
b. **Changed passwords on any of your financial accounts?** YES NO
c. **Purchased identity theft protection from a company that offers protection services?** YES NO

d. **Purchased credit monitoring or identity theft insurance?** YES NO
e. **Shredded or destroyed documents containing your personal information?** YES NO

f. **Checked your banking or credit card statements for unfamiliar charges?** YES NO

g. **Used security software program on your computer to protect against loss of credit cards/card theft?** YES NO

CHECK ITEM J
If ("yes" for Q64a, Q64b, Q64c, Q64d, Q64e, Q64f, or Q64g) AND ("yes" for Q2, Q6, Q9b, Q11, Q15, or Q19) continue to Q65.
Else, skip to Q67.

65**. You said that during the past 12 months, you** <autofill "yes" responses from 64a, 64b, 64c, 64d, 64e, 64f, 64g>. **Did you take any of these actions as a result of previous misuse of your personal information?**

YES (Ask Q66)

NO (Skip to Q67)

66**. You said that during the past 12 months you: <**autofill "yes" responses from 64a, 64b, 64c, 64d, 64e, 64f, 64g**>. Which actions did you take in direct response to any previous misuse of your personal information?**
(Mark all that apply, and only read response items that match autofill responses in this question)

1. Checked your credit report
2. Changed passwords on any of your financial accounts
3. Purchased identity theft protection from a company that offers protection services
4. Purchased credit monitoring or identity theft insurance
5. Shredded or destroyed documents containing your personal information
6. Checked your banking or credit card statements for unfamiliar charges
7. Used security software program on your computer to protect it against loss of credit cards/card theft

SECTION I. DATA BREACHES

67**. My final questions involve organizations that may have your personal information in their files. During the past 12 months, did a company, government agency, or some other organization that has your personal information:**

a**. Notify you or announce publicly that some or all of their files or data may have been stolen, lost, or posted on a publicly available website?**

YES (Ask Q67b)
NO (Skip to End of Survey)

b. **Did they notify you directly that YOUR personal information may have been stolen, lost, or posted on a publicly available website?**

YES (Ask Q68)
NO (Skip to End of Survey)

68. **Did this personal information include your Social Security number?**

YES
NO
DON'T KNOW

END OF SURVEY

§10132. Bureau of Justice Statistics

(a) Establishment

There is established within the Department of Justice, under the general authority of the Attorney General, a Bureau of Justice Statistics (hereinafter referred to in this subchapter as "Bureau").

(b) Appointment of Director; experience; authority; restrictions

The Bureau shall be headed by a Director appointed by the President. The Director shall have had experience in statistical programs. The Director shall have final authority for all grants, cooperative agreements, and contracts awarded by the Bureau. The Director shall be responsible for the integrity of data and statistics and shall protect against improper or illegal use or disclosure. The Director shall report to the Attorney General through the Assistant Attorney General. The Director shall not engage in any other employment than that of serving as Director; nor shall the Director hold any office in, or act in any capacity for, any organization, agency, or institution with which the Bureau makes any contract or other arrangement under this Act.

(c) Duties and functions of Bureau

The Bureau is authorized to—

(1) make grants to, or enter into cooperative agreements or contracts with public agencies, institutions of higher education, private organizations, or private individuals for purposes related to this subchapter; grants shall be made subject to continuing compliance with standards for gathering justice statistics set forth in rules and regulations promulgated by the Director;

(2) collect and analyze information concerning criminal victimization, including crimes against the elderly, and civil disputes;

(3) collect and analyze data that will serve as a continuous and comparable national social indication of the prevalence, incidence, rates, extent, distribution, and attributes of crime, juvenile delinquency, civil disputes, and other statistical factors related to crime, civil disputes, and juvenile delinquency, in support of national, State, tribal, and local justice policy and decisionmaking;

(4) collect and analyze statistical information, concerning the operations of the criminal justice system at the Federal, State, tribal, and local levels;

(5) collect and analyze statistical information concerning the prevalence, incidence, rates, extent, distribution, and attributes of crime, and juvenile delinquency, at the Federal, State, tribal, and local levels;

(6) analyze the correlates of crime, civil disputes and juvenile delinquency, by the use of statistical information, about criminal and civil justice systems at the Federal, State, tribal, and local levels, and about the extent, distribution and attributes of crime, and juvenile delinquency, in the Nation and at the Federal, State, tribal, and local levels;

(7) compile, collate, analyze, publish, and disseminate uniform national statistics concerning all aspects of criminal justice and related aspects of civil justice, crime, including crimes against the elderly, juvenile delinquency, criminal offenders, juvenile delinquents, and civil disputes in the various States and in Indian country;

(8) recommend national standards for justice statistics and for insuring the reliability and validity of justice statistics supplied pursuant to this chapter;

(9) maintain liaison with the judicial branches of the Federal Government and State and tribal governments in matters relating to justice statistics, and cooperate with the judicial branch in assuring as much uniformity as feasible in statistical systems of the executive and judicial branches;

(10) provide information to the President, the Congress, the judiciary, State, tribal, and local governments, and the general public on justice statistics;

(11) establish or assist in the establishment of a system to provide State, tribal, and local governments with access to Federal informational resources useful in the planning, implementation, and evaluation of programs under this Act;

(12) conduct or support research relating to methods of gathering or analyzing justice statistics;

(13) provide for the development of justice information systems programs and assistance to the States, Indian tribes, and units of local government relating to collection, analysis, or dissemination of justice statistics;

(14) develop and maintain a data processing capability to support the collection, aggregation, analysis and dissemination of information on the incidence of crime and the operation of the criminal justice system;

(15) collect, analyze and disseminate comprehensive Federal justice transaction statistics (including statistics on issues of Federal justice interest such as public fraud and high technology crime) and to provide technical assistance to and work jointly with other Federal agencies to improve the availability and quality of Federal justice data;

(16) provide for the collection, compilation, analysis, publication and dissemination of information and statistics about the prevalence, incidence, rates, extent, distribution and attributes of drug offenses, drug related offenses and drug dependent offenders and further provide for the establishment of a national clearinghouse to maintain and update a comprehensive and timely data base on all criminal justice aspects of the drug crisis and to disseminate such information;

(17) provide for the collection, analysis, dissemination and publication of statistics on the condition and progress of drug control activities at the Federal, State, tribal, and local levels with particular attention to programs and intervention efforts demonstrated to be of value in the overall national anti-drug strategy and to provide for the establishment of a national clearinghouse for the gathering of data generated by Federal, State, tribal, and local criminal justice agencies on their drug enforcement activities;

(18) provide for the development and enhancement of State, tribal, and local criminal justice information systems, and the standardization of data reporting relating to the collection, analysis or dissemination of data and statistics about drug offenses, drug related offenses, or drug dependent offenders;

(19) provide for improvements in the accuracy, quality, timeliness, immediate accessibility, and integration of State and tribal criminal history and related records, support the development and enhancement of national systems of criminal history and related records including the National Instant Criminal Background Check System, the National Incident-Based Reporting System, and the records of the National Crime Information Center, facilitate State and tribal participation in national records and information systems, and support statistical research for critical analysis of the improvement and utilization of criminal history records;

(20) maintain liaison with State, tribal, and local governments and governments of other nations concerning justice statistics;

(21) cooperate in and participate with national and international organizations in the development of uniform justice statistics;

(22) ensure conformance with security and privacy requirement of section 10231 of this title and identify, analyze, and participate in the development and implementation of privacy, security and information policies

which impact on Federal, tribal, and State criminal justice operations and related statistical activities; and

(23) exercise the powers and functions set out in subchapter VII.

(d) Justice statistical collection, analysis, and dissemination

(1) In general

To ensure that all justice statistical collection, analysis, and dissemination is carried out in a coordinated manner, the Director is authorized to—

(A) utilize, with their consent, the services, equipment, records, personnel, information, and facilities of other Federal, State, local, and private agencies and instrumentalities with or without reimbursement therefor, and to enter into agreements with such agencies and instrumentalities for purposes of data collection and analysis;

(B) confer and cooperate with State, municipal, and other local agencies;

(C) request such information, data, and reports from any Federal agency as may be required to carry out the purposes of this chapter;

(D) seek the cooperation of the judicial branch of the Federal Government in gathering data from criminal justice records;

(E) encourage replication, coordination and sharing among justice agencies regarding information systems, information policy, and data; and

(F) confer and cooperate with Federal statistical agencies as needed to carry out the purposes of this subchapter, including by entering into cooperative data sharing agreements in conformity with all laws and regulations applicable to the disclosure and use of data.

(2) Consultation with Indian tribes

The Director, acting jointly with the Assistant Secretary for Indian Affairs (acting through the Office of Justice Services) and the Director of the Federal Bureau of Investigation, shall work with Indian tribes and tribal law enforcement agencies to establish and implement such tribal data collection systems as the Director determines to be necessary to achieve the purposes of this section.

(e) Furnishing of information, data, or reports by Federal agencies

Federal agencies requested to furnish information, data, or reports pursuant to subsection (d)(1)(C) shall provide such information to the Bureau as is required to carry out the purposes of this section.

(f) Consultation with representatives of State, tribal, and local government and judiciary

In recommending standards for gathering justice statistics under this section, the Director shall consult with representatives of State, tribal, and local government, including, where appropriate, representatives of the judiciary.

(g) Reports

Not later than 1 year after July 29, 2010, and annually thereafter, the Director shall submit to Congress a report describing the data collected and analyzed under this section relating to crimes in Indian country.

(Pub. L. 90–351, title I, §302, as added Pub. L. 96–157, §2, Dec. 27, 1979, 93 Stat. 1176; amended Pub. L. 98–473, title II, §605(b), Oct. 12, 1984, 98 Stat. 2079; Pub. L. 100–690, title VI, §6092(a), Nov. 18, 1988, 102 Stat. 4339; Pub. L. 103–322, title XXXIII, §330001(h)(2), Sept. 13, 1994, 108 Stat. 2139; Pub. L. 109–162, title XI, §1115(a), Jan. 5, 2006, 119 Stat. 3103; Pub. L. 111–211, title II, §251(b), July 29, 2010, 124 Stat. 2297; Pub. L. 112–166, §2(h)(1), Aug. 10, 2012, 126 Stat. 1285.)

References in Text

This Act, referred to in subsecs. (b) and (c)(11), is Pub. L. 90–351, June 19, 1968, 82 Stat. 197, known as the Omnibus Crime Control and Safe Streets Act of 1968. For complete classification of this Act to the Code, see Short Title of 1968 Act note set out under section 10101 of this title and Tables.

Codification

Section was formerly classified to section 3732 of Title 42, The Public Health and Welfare, prior to editorial reclassification and renumbering as this section.

Prior Provisions

A prior section 302 of Pub. L. 90–351, title I, June 19, 1968, 82 Stat. 200; Pub. L. 93–83, §2, Aug. 6, 1973, 87 Stat. 201; Pub. L. 94–503, title I, §110, Oct. 15, 1976, 90 Stat. 2412, related to establishment of State planning agencies to develop comprehensive State plans for grants for law enforcement and criminal justice purposes, prior to the general amendment of this chapter by Pub. L. 96–157.

Amendments

2012—Subsec. (b). Pub. L. 112–166 struck out ", by and with the advice and consent of the Senate" before period at end of first sentence.

2010—Subsec. (c)(3) to (6). Pub. L. 111–211, §251(b)(1)(A), inserted "tribal," after "State," wherever appearing.

Subsec. (c)(7). Pub. L. 111–211, §251(b)(1)(B), inserted "and in Indian country" after "States".

Subsec. (c)(9). Pub. L. 111–211, §251(b)(1)(C), substituted "Federal Government and State and tribal governments" for "Federal and State Governments".

Subsec. (c)(10), (11). Pub. L. 111–211, §251(b)(1)(D), inserted ", tribal," after "State".

Subsec. (c)(13). Pub. L. 111–211, §251(b)(1)(E), inserted ", Indian tribes," after "States".

Subsec. (c)(17). Pub. L. 111–211, §251(b)(1)(F), substituted "activities at the Federal, State, tribal, and local" for "activities at the Federal, State and local" and "generated by Federal, State, tribal, and local" for "generated by Federal, State, and local".

Subsec. (c)(18). Pub. L. 111–211, §251(b)(1)(G), substituted "State, tribal, and local" for "State and local".

Subsec. (c)(19). Pub. L. 111–211, §251(b)(1)(H), inserted "and tribal" after "State" in two places.

Subsec. (c)(20). Pub. L. 111–211, §251(b)(1)(I), inserted ", tribal," after "State".

Subsec. (c)(22). Pub. L. 111–211, §251(b)(1)(J), inserted ", tribal," after "Federal".

Subsec. (d). Pub. L. 111–211, §251(b)(2), designated existing provisions as par. (1), inserted par. (1) heading, substituted "To ensure" for "To insure", redesignated former pars. (1) to (6) as subpars. (A) to (F), respectively, of par. (1), realigned margins, and added par. (2).

Subsec. (e). Pub. L. 111–211, §251(b)(3), substituted "subsection (d)(1)(C)" for "subsection (d)(3)".

Subsec. (f). Pub. L. 111–211, §251(b)(4)(B), inserted ", tribal," after "State".

Pub. L. 111–211, §251(b)(4)(A), which directed insertion of ", tribal," after "State" in heading, was executed editorially but could not be executed in original because heading had been editorially supplied.

Subsec. (g). Pub. L. 111–211, §251(b)(5), added subsec. (g).

2006—Subsec. (b). Pub. L. 109–162, §1115(a)(1), inserted after third sentence "The Director shall be responsible for the integrity of data and statistics and shall protect against improper or illegal use or disclosure."

Subsec. (c)(19). Pub. L. 109–162, §1115(a)(2), amended par. (19) generally. Prior to amendment, par. (19) read as follows: "provide for research and improvements in the accuracy, completeness, and inclusiveness of criminal history record information, information systems, arrest warrant, and stolen vehicle record information and information systems and support research concerning the accuracy, completeness, and inclusiveness of other criminal justice record information;".

Subsec. (d)(6). Pub. L. 109–162, §1115(a)(3), added par. (6).

1994—Subsec. (c)(19). Pub. L. 103–322 substituted a semicolon for period at end.

1988—Subsec. (c)(16) to (23). Pub. L. 100–690 added pars. (16) to (19) and redesignated former pars. (16) to (19) as (20) to (23), respectively.

1984—Subsec. (b). Pub. L. 98–473, §605(b)(1), inserted provision requiring Director to report to Attorney General through Assistant Attorney General.

Subsec. (c)(13). Pub. L. 98–473, §605(b)(2)(A), (C), added par. (13) and struck out former par. (13) relating to provision of financial and technical assistance to States and units of local government relating to collection, analysis, or dissemination of justice statistics.

Subsec. (c)(14), (15). Pub. L. 98–473, §605(b)(2)(C), added pars. (14) and (15). Former pars. (14) and (15) redesignated (16) and (17), respectively.

Subsec. (c)(16). Pub. L. 98–473, §605(b)(2)(A), (B), redesignated par. (14) as (16) and struck out former par. (16) relating to insuring conformance with security and privacy regulations issued under section 10231 of this title.

Subsec. (c)(17). Pub. L. 98–473, §605(b)(2)(B), redesignated par. (15) as (17). Former par. (17) redesignated (19).

Subsec. (c)(18). Pub. L. 98–473, §605(b)(2)(D), added par. (18).

Subsec. (c)(19). Pub. L. 98–473, §605(b)(2)(B), redesignated former par. (17) as (19).

Subsec. (d)(1). Pub. L. 98–473, §605(b)(3)(A), inserted ", and to enter into agreements with such agencies and instrumentalities for purposes of data collection and analysis".

Subsec. (d)(5). Pub. L. 98–473, §605(b)(3)(B)–(D), added par. (5).

Effective Date of 2012 Amendment

Amendment by Pub. L. 112–166 effective 60 days after Aug. 10, 2012, and applicable to appointments made on and after that effective date, including any nomination pending in the Senate on that date, see section 6(a) of Pub. L. 112–166, set out as a note under section 113 of Title 6, Domestic Security.

Effective Date of 1984 Amendment

Amendment by Pub. L. 98–473 effective Oct. 12, 1984, see section 609AA(a) of Pub. L. 98–473, set out as an Effective Date note under section 10101 of this title.

Construction of 2010 Amendment

Pub. L. 111–211, title II, §251(c), July 29, 2010, 124 Stat. 2298, provided that: "Nothing in this section [amending this section and section 41507 of this title] or any amendment made by this section—

"(1) allows the grant to be made to, or used by, an entity for law enforcement activities that the entity lacks jurisdiction to perform; or

"(2) has any effect other than to authorize, award, or deny a grant of funds to a federally recognized Indian tribe for the purposes described in the relevant grant program."

[For definition of "Indian tribe" as used in section 251(c) of Pub. L. 111–211, set out above, see section 203(a) of Pub. L. 111–211, set out as a note under section 2801 of Title 25, Indians.]

Data Collection

Pub. L. 115–391, title VI, §610, Dec. 21, 2018, 132 Stat. 5245, provided that:

"(a) National Prisoner Statistics Program.—Beginning not later than 1 year after the date of enactment of this Act [Dec. 21, 2018], and annually thereafter, pursuant to the authority under section 302 of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3732) [now 34 U.S.C. 10132], the Director of the Bureau of Justice Statistics, with information that shall be provided by the Director of the Bureau of Prisons, shall include in the National Prisoner Statistics Program the following:

"(1) The number of prisoners (as such term is defined in section 3635 of title 18, United States Code, as added by section 101(a) of this Act) who are veterans of the Armed Forces of the United States.

"(2) The number of prisoners who have been placed in solitary confinement at any time during the previous year.

"(3) The number of female prisoners known by the Bureau of Prisons to be pregnant, as well as the outcomes of such pregnancies, including information on pregnancies that result in live birth, stillbirth, miscarriage, abortion, ectopic pregnancy, maternal death, neonatal death, and preterm birth.

"(4) The number of prisoners who volunteered to participate in a substance abuse treatment program, and the number of prisoners who have participated in such a program.

"(5) The number of prisoners provided medication-assisted treatment with medication approved by the Food and Drug Administration while in custody in order to treat substance use disorder.

"(6) The number of prisoners who were receiving medication-assisted treatment with medication approved by the Food and Drug Administration prior to the commencement of their term of imprisonment.

"(7) The number of prisoners who are the parent or guardian of a minor child.

"(8) The number of prisoners who are single, married, or otherwise in a committed relationship.

"(9) The number of prisoners who have not achieved a GED, high school diploma, or equivalent prior to entering prison.

"(10) The number of prisoners who, during the previous year, received their GED or other equivalent certificate while incarcerated.

"(11) The numbers of prisoners for whom English is a second language.

"(12) The number of incidents, during the previous year, in which restraints were used on a female prisoner during pregnancy, labor, or postpartum recovery, as well as information relating to the type of restraints used, and the circumstances under which each incident occurred.

"(13) The vacancy rate for medical and healthcare staff positions, and average length of such a vacancy.

"(14) The number of facilities that operated, at any time during the previous year, without at least 1 clinical nurse, certified paramedic, or licensed physician on site.

"(15) The number of facilities that during the previous year were accredited by the American Correctional Association.

"(16) The number and type of recidivism reduction partnerships described in section 3621(h)(5) of title 18, United States Code, as added by section 102(a) of this Act, entered into by each facility.

"(17) The number of facilities with remote learning capabilities.

"(18) The number of facilities that offer prisoners video conferencing.

"(19) Any changes in costs related to legal phone calls and visits following implementation of section 3632(d)(1) of title 18, United States Code, as added by section 101(a) of this Act.

"(20) The number of aliens in prison during the previous year.

"(21) For each Bureau of Prisons facility, the total number of violations that resulted in reductions in rewards, incentives, or time credits, the number of such violations for each category of violation, and the demographic breakdown of the prisoners who have received such reductions.

"(22) The number of assaults on Bureau of Prisons staff by prisoners and the number of criminal prosecutions of prisoners for assaulting Bureau of Prisons staff.

"(23) The capacity of each recidivism reduction program and productive activity to accommodate eligible inmates at each Bureau of Prisons facility.

"(24) The number of volunteers who were certified to volunteer in a Bureau of Prisons facility, broken down by level (level I and level II), and by each Bureau of Prisons facility.

"(25) The number of prisoners enrolled in recidivism reduction programs and productive activities at each Bureau of Prisons facility, broken down by risk level and by program, and the number of those enrolled prisoners who successfully completed each program.

"(26) The breakdown of prisoners classified at each risk level by demographic characteristics, including age, sex, race, and the length of the sentence imposed.

"(b) Report to Judiciary Committees.—Beginning not later than 1 year after the date of enactment of this Act [Dec. 21, 2018], and annually thereafter for a period of 7 years, the Director of the Bureau of Justice Statistics shall submit a report containing the information described in paragraphs (1) through (26) of subsection (a) to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives."

Inclusion of Honor Violence in National Crime Victimization Survey

Pub. L. 113–235, div. B, title II, Dec. 16, 2014, 128 Stat. 2191, provided in part: "That beginning not later than 2 years after the date of enactment of this Act [div. B of Pub. L. 113–235, Dec. 16, 2014], as part of each National Crime Victimization Survey, the Attorney General shall include statistics relating to honor violence".

Study of Crimes Against Seniors

Pub. L. 106–534, §5, Nov. 22, 2000, 114 Stat. 2557, provided that:

"(a) In General.—The Attorney General shall conduct a study relating to crimes against seniors, in order to assist in developing new strategies to prevent and otherwise reduce the incidence of those crimes.

"(b) Issues Addressed.—The study conducted under this section shall include an analysis of—

"(1) the nature and type of crimes perpetrated against seniors, with special focus on—

"(A) the most common types of crimes that affect seniors;

"(B) the nature and extent of telemarketing, sweepstakes, and repair fraud against seniors; and

"(C) the nature and extent of financial and material fraud targeted at seniors;

"(2) the risk factors associated with seniors who have been victimized;

"(3) the manner in which the Federal and State criminal justice systems respond to crimes against seniors;

"(4) the feasibility of States establishing and maintaining a centralized computer database on the incidence of crimes against seniors that will promote the uniform identification and reporting of such crimes;

"(5) the effectiveness of damage awards in court actions and other means by which seniors receive reimbursement and other damages after fraud has been established; and

"(6) other effective ways to prevent or reduce the occurrence of crimes against seniors."

Inclusion of Seniors in National Crime Victimization Survey

Pub. L. 106–534, §6, Nov. 22, 2000, 114 Stat. 2557, provided that: "Beginning not later than 2 years after the date of enactment of this Act [Nov. 22, 2000], as part of each National Crime Victimization Survey, the Attorney General shall include statistics relating to—

"(1) crimes targeting or disproportionately affecting seniors;

"(2) crime risk factors for seniors, including the times and locations at which crimes victimizing seniors are most likely to occur; and

"(3) specific characteristics of the victims of crimes who are seniors, including age, gender, race or ethnicity, and socioeconomic status."

Crime Victims With Disabilities Awareness

Pub. L. 105–301, Oct. 27, 1998, 112 Stat. 2838, as amended by Pub. L. 106–402, title IV, §401(b)(10), Oct. 30, 2000, 114 Stat. 1739, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'Crime Victims With Disabilities Awareness Act'.

"SEC. 2. FINDINGS; PURPOSES.

"(a) Findings.—Congress finds that—

"(1) although research conducted abroad demonstrates that individuals with developmental disabilities are at a 4 to 10 times higher risk of becoming crime victims than those without disabilities, there have been no significant studies on this subject conducted in the United States;

"(2) in fact, the National Crime Victim's Survey, conducted annually by the Bureau of Justice Statistics of the Department of Justice, does not specifically collect data relating to crimes against individuals with developmental disabilities;

"(3) studies in Canada, Australia, and Great Britain consistently show that victims with developmental disabilities suffer repeated victimization because so few of the crimes against them are reported, and even when they are, there is sometimes a reluctance by police, prosecutors, and judges to rely on the testimony of a disabled individual, making individuals with developmental disabilities a target for criminal predators;

"(4) research in the United States needs to be done to—

"(A) understand the nature and extent of crimes against individuals with developmental disabilities;

"(B) describe the manner in which the justice system responds to crimes against individuals with developmental disabilities; and

"(C) identify programs, policies, or laws that hold promises for making the justice system more responsive to crimes against individuals with developmental disabilities; and

"(5) the National Academy of Science Committee on Law and Justice of the National Research Council is a premier research institution with unique experience in developing seminal, multidisciplinary studies to establish a strong research base from which to make public policy.

"(b) Purposes.—The purposes of this Act are—

"(1) to increase public awareness of the plight of victims of crime who are individuals with developmental disabilities;

"(2) to collect data to measure the extent of the problem of crimes against individuals with developmental disabilities; and

"(3) to develop a basis to find new strategies to address the safety and justice needs of victims of crime who are individuals with developmental disabilities.

"SEC. 3. DEFINITION OF DEVELOPMENTAL DISABILITY.

"In this Act, the term 'developmental disability' has the meaning given the term in section 102 of the Developmental Disabilities Assistance and Bill of Rights Act of 2000 [42 U.S.C. 15002].

"SEC. 4. STUDY.

"(a) In General.—The Attorney General shall conduct a study to increase knowledge and information about crimes against individuals with developmental disabilities that will be useful in developing new strategies to reduce the incidence of crimes against those individuals.

"(b) Issues Addressed.—The study conducted under this section shall address such issues as—

"(1) the nature and extent of crimes against individuals with developmental disabilities;

"(2) the risk factors associated with victimization of individuals with developmental disabilities;

"(3) the manner in which the justice system responds to crimes against individuals with developmental disabilities; and

"(4) the means by which States may establish and maintain a centralized computer database on the incidence of crimes against individuals with disabilities within a State.

"(c) National Academy of Sciences.—In carrying out this section, the Attorney General shall consider contracting with the Committee on Law and Justice of the National Research Council of the National Academy of Sciences to provide research for the study conducted under this section.

"(d) Report.—Not later than 18 months after the date of enactment of this Act [Oct. 27, 1998], the Attorney General shall submit to the Committees on the Judiciary of the Senate and the House of Representatives a report describing the results of the study conducted under this section.

"SEC. 5. NATIONAL CRIME VICTIM'S SURVEY.

"Not later than 2 years after the date of enactment of this Act, as part of each National Crime Victim's Survey, the Attorney General shall include statistics relating to—

"(1) the nature of crimes against individuals with developmental disabilities; and

"(2) the specific characteristics of the victims of those crimes."

DATES: Comments are encouraged and will be accepted for 30 days until March 4, 2021.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain.* Find this particular information collection by selecting ''Currently under 30-day Review—Open for Public Comments'' or by using the search function.

SUPPLEMENTARY INFORMATION: Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address one or more of the following four points:

—Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Bureau of Justice Statistics, including whether the information will have practical utility;

—Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

—Evaluate whether and if so how the quality, utility, and clarity of the information to be collected can be enhanced; and

—Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* Revision of a currently collection approved collection. The 2020 survey instrument is being revised to include new questions and remove others.

(2) *The Title of the Form/Collection:* 2018–2020 Survey of State Criminal History Information Systems (SSCHIS).

(3) *The agency form number, if any, and the applicable component of the Department sponsoring the collection:* The form number is N/A. The applicable component within the Department of Justice is the Bureau of Justice Statistics, in the Office of Justice Programs.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Respondents are state government agencies, primarily state criminal history record repositories. The SSCHIS report, the most comprehensive data available on the collection and maintenance of information by state criminal history record systems, describes the status of such systems and record repositories on a biennial basis. Data collected from state record repositories serves as the basis for estimating the percentage of total state records that are immediately available through the FBI's Interstate Identification Index (III), and the percentage of arrest records that include dispositions. Other data presented include the number of records maintained by each state, the percentage of automated records in the system, and the number of states participating in the National Fingerprint File and the National Crime Prevention and Privacy Compact which authorizes the interstate exchange of criminal history records for noncriminal justice purposes. The SSCHIS also contains information regarding the timeliness and completeness of data in state record systems and procedures employed to improve data quality.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* The total number of respondents is 56. The average length of time per respondent is 6.5 hours. This estimate is based on the average amount of time reported by five states that reviewed the survey.

(6) *An estimate of the total public burden (in hours) associated with the collection:* The total burden associated with this collection is estimated to be 364 hours.

If additional information is required contact: Melody Braswell, Department Clearance Officer, United States Department of Justice, Justice Management Division, Policy and Planning Staff, Two Constitution Square, 145 N Street NE, 3E.405A, Washington, DC 20530.

Dated: January 27, 2021.

Melody Braswell,

Department Clearance Officer for PRA, U.S. Department of Justice.

[FR Doc. 2021–02129 Filed 2–1–21; 8:45 am]

BILLING CODE 4410–18–P

DEPARTMENT OF JUSTICE

[OMB Number 1121–0317]

Agency Information Collection Activities; Proposed eCollection eComments Requested; Reinstatement, With Change, of a Previously Approved Collection for Which Approval Has Expired: 2021 Identity Theft Supplement (ITS)

AGENCY: Bureau of Justice Statistics, Department of Justice.

ACTION: 60-Day notice.

SUMMARY: The Department of Justice (DOJ), Office of Justice Programs, Bureau of Justice Statistics, will be submitting the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted for 60 days until April 5, 2021.

FOR FURTHER INFORMATION CONTACT: If you have additional comments especially on the estimated public burden or associated response time, suggestions, or need a copy of the proposed information collection instrument with instructions or additional information, please contact Erika Harrell, Statistician, Bureau of Justice Statistics, 810 Seventh Street NW, Washington, DC 20531 (email: *Erika.Harrell@usdoj.gov;* telephone: 202–307–0758).

SUPPLEMENTARY INFORMATION: Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address one or more of the following four points:

—Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Bureau of Justice Statistics, including whether the information will have practical utility;

—Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

—Evaluate whether and if so how the quality, utility, and clarity of the information to be collected can be enhanced; and

—Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* Reinstatement of the Identity Theft Supplement, with changes, a previously approved collection for which approval has expired.

(2) *The Title of the Form/Collection:* 2021 Identity Theft Supplement.

(3) *The agency form number, if any, and the applicable component of the Department sponsoring the collection:* The form number for the questionnaire is ITS–1. The applicable component within the Department of Justice is the Bureau of Justice Statistics, in the Office of Justice Programs.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Respondents will be persons 16 years or older living in households located throughout the United States sampled for the National Crime Victimization Survey (NCVS). The ITS will be conducted as a supplement to the NCVS in all sample households for a six (6) month period. The ITS is primarily an effort to measure the prevalence of identity theft among persons, the characteristics of identity theft victims, and patterns of reporting to the police, credit bureaus, and other authorities. The ITS was also designed to collect important characteristics of identity theft such as how the victim's personal information was obtained; the physical, emotional and financial impact on victims; offender information; and the measures people take to avoid or minimize their risk of becoming an identity theft victim. BJS plans to publish this information in reports and reference it when responding to queries from the U.S. Congress, Executive Office of the President, the U.S. Supreme Court, state officials, international organizations, researchers, students, the media, and others interested in criminal justice statistics.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* An estimate of the total number of respondents is 104,910. An estimated 90.2% of respondents (94,630) will have no identity theft and will complete the short interview with an average burden of eight minutes. Among the 9.8% of respondents (10,280) who experience at least one incident of identity theft, the time to ask the detailed questions regarding the aspects of the most recent incident of identity theft is estimated to take an average of fifteen minutes. Respondents will be asked to respond to this survey only once during the six-month period. The burden estimate is based on actual interview times from the 2018 ITS, an analysis of the 2021 ITS questionnaire changes, and mock interviews done with the 2021 questionnaire.

(6) *An estimate of the total public burden (in hours) associated with the collection:* There are an estimated 15,185 total burden hours associated with this collection.

If additional information is required contact: Melody Braswell, Department Clearance Officer, United States Department of Justice, Justice Management Division, Policy and Planning Staff, Two Constitution Square, 145 N Street NE, 3E.405A, Washington, DC 20530.

Dated: January 27, 2021.

Melody Braswell,

Department Clearance Officer for PRA, U.S. Department of Justice.

[FR Doc. 2021–02125 Filed 2–1–21; 8:45 am]

BILLING CODE 4410–18–P

DEPARTMENT OF LABOR

Agency Information Collection Activities; Submission for OMB Review; Comment Request; Apprenticeship Evidence-Building Portfolio, New Collection

AGENCY: Office of the Assistant Secretary for Policy, Chief Evaluation Office, Department of Labor.

ACTION: Notice of information collection; request for comment.

SUMMARY: The Department of Labor (DOL), as part of its continuing effort to reduce paperwork and respondent burden, conducts a preclearance consultation program to provide the general public and federal agencies with an opportunity to comment on proposed and/or continuing collections of information in accordance with the Paperwork Reduction Act of 1995 (PRA95). This program helps to ensure that requested data can be provided in the desired format, reporting burden (time and financial resources) is minimized, collection instruments are clearly understood, and the impact of collection requirements on respondents is properly assessed. Currently, the Department of Labor is soliciting comments concerning the collection of data about the Apprenticeship Evidence-Building Portfolio. A copy of the proposed Information Collection Request (ICR) can be obtained by contacting the office listed below in the addressee section of this notice.

DATES: Written comments must be submitted to the office listed in the addressee section below on or before April 5, 2021.

ADDRESSES: You may submit comments by either one of the following methods: *Email: ChiefEvaluationOffice@dol.gov; Mail or Courier:* Janet Javar, Chief Evaluation Office, OASP, U.S. Department of Labor, Room S–2312, 200 Constitution Avenue NW, Washington, DC 20210. *Instructions:* Please submit one copy of your comments by only one method. All submissions received must include the agency name and OMB Control Number identified above for this information collection. Comments, including any personal information provided, become a matter of public record. They will also be summarized and/or included in the request for OMB approval of the information collection request.

FOR FURTHER INFORMATION CONTACT: Janet Javar by email at *ChiefEvaluationOffice@dol.gov* or by phone at (202) 693–5954.

SUPPLEMENTARY INFORMATION:

I. *Background:* The Chief Evaluation Office (CEO) of the U.S. Department of Labor (DOL) intends to design and conduct evaluations of DOL-funded apprenticeship initiatives through the Apprenticeship Evidence-Building Portfolio. The portfolio of initiatives includes the *Scaling Apprenticeship Through Sector-Based Strategies* grants, *Closing the Skills Gap* grants, *Youth Apprenticeship Readiness* grants, and other DOL investments. The goal of this five-year study is to build evidence on apprenticeship models, practices, and partnership strategies in high-growth occupations and industries. The overall study is comprised of several components: (1) An implementation study of the *Scaling Apprenticeship* and *Closing the Skills Gap* grants to develop typologies of apprenticeship models and practices, identify promising strategies across the portfolio, and to better understand the implementation of models to help interpret impact evaluation findings; (2) a study of registered apprenticeship state systems and partnerships to assess their capacity to develop, design, modify, implement, replicate, sustain, expand/scale up, and evaluate apprenticeship strategies and models; and (3) an implementation evaluation of the *Youth Apprenticeship Readiness* grant program to understand service delivery design and implementation, challenges, and promising practices. DOL will submit additional ICRs for future data collection requests for this overall study.

This **Federal Register** Notice provides the opportunity to comment on nine

Dated: April 21, 2021.

Melody Braswell,

Department Clearance Officer for PRA, U.S. Department of Justice.

[FR Doc. 2021–08587 Filed 4–23–21; 8:45 am]

BILLING CODE 4410–18–P

DEPARTMENT OF JUSTICE

Office of Justice Programs

[OMB Number 1121–0317]

Agency Information Collection Activities; Proposed eCollection eComments Requested; Reinstatement, With Change, of a Previously Approved Collection for Which Approval has Expired: 2021 Identity Theft Supplement (ITS)

AGENCY: Bureau of Justice Statistics, Office of Justice Programs, Department of Justice.

ACTION: 30-Day notice.

SUMMARY: The Bureau of Justice Statistics, Office of Justice Programs, Department of Justice (DOJ), will be submitting the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995. The proposed information collection was previously published in the **Federal Register**. Following publication of the 60-day notice, the Bureau of Justice Statistics received no requests for the survey instrument and two communications containing suggestions for revisions to the collection of data and regarding the administration of the instrument, which are addressed in Supporting Statement Part A.

DATES: Comments are encouraged and will be accepted for 30 days until May 26, 2021.

FOR FURTHER INFORMATION CONTACT: If you have additional comments especially on the estimated public burden or associated response time, suggestions, or need a copy of the proposed information collection instrument with instructions or additional information, please contact Erika Harrell, Statistician, Bureau of Justice Statistics, 810 Seventh Street NW, Washington, DC 20531 (email: *Erika.Harrell@usdoj.gov;* telephone: 202–307–0758).

SUPPLEMENTARY INFORMATION: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain.* Find this particular information collection by selecting ''Currently under 30-day Review—Open for Public Comments'' or by using the search function. Your comments should address one or more of the following four points:

—Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Bureau of Justice Statistics, including whether the information will have practical utility;

—Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

—Evaluate whether and if so how the quality, utility, and clarity of the information to be collected can be enhanced; and

—Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* Reinstatement of the Identity Theft Supplement, with changes, a previously approved collection for which approval has expired.

(2) *The Title of the Form/Collection:* 2021 Identity Theft Supplement.

(3) *The agency form number, if any, and the applicable component of the Department sponsoring the collection:* The form number for the questionnaire is ITS–1. The applicable component within the Department of Justice is the Bureau of Justice Statistics, in the Office of Justice Programs.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Respondents will be persons 16 years or older living in households located throughout the United States sampled for the National Crime Victimization Survey (NCVS). The ITS will be conducted as a supplement to the NCVS in all sample households for a six (6) month period. The ITS is primarily an effort to measure the prevalence of identity theft among persons, the characteristics of identity theft victims, and patterns of reporting to the police, credit bureaus, and other authorities. The ITS was also designed to collect important characteristics of identity theft such as how the victim's personal information was obtained; the physical, emotional and financial impact on victims; offender information; and the measures people take to avoid or minimize their risk of becoming an identity theft victim. BJS plans to publish this information in reports and reference it when responding to queries from the U.S. Congress, Executive Office of the President, the U.S. Supreme Court, state officials, international organizations, researchers, students, the media, and others interested in criminal justice statistics.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* An estimate of the total number of respondents is 104,910. An estimated 90.2% of respondents (94,630) are estimated to report no identity theft and will complete the ITS screener and follow-up questions with an average burden of about eight minutes. Among the 9.8% of respondents (10,280) who are expected to experience at least one incident of identity theft during the reference period, the time to ask the screener, incident, and follow-up questions of identity theft is estimated to take an average of fifteen minutes. Respondents will be asked to respond to this survey only once during the six-month period. The burden estimate is based on data from actual interview times from the 2018 ITS, an analysis of the 2021 ITS questionnaire changes and mock interviews done with the 2021 questionnaire.

(6) *An estimate of the total public burden (in hours) associated with the collection:* There are an estimated 15,185 total burden hours associated with this collection.

If additional information is required contact: Melody Braswell, Department Clearance Officer, United States Department of Justice, Justice Management Division, Policy and Planning Staff, Two Constitution Square, 145 N Street NE, 3E.405A, Washington, DC 20530.

Dated: April 21, 2021.

Melody Braswell,

Department Clearance Officer for PRA, U.S. Department of Justice.

[FR Doc. 2021–08584 Filed 4–23–21; 8:45 am]

BILLING CODE 4410–18–P

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

[Notice: (21–026)]

Notice of Intent To Grant an Exclusive, Co-Exclusive or Partially Exclusive Patent License

AGENCY: National Aeronautics and Space Administration.

Identity Theft

What to know, What to do

FEDERAL TRADE COMMISSION
IdentityTheft.gov

Is someone using your personal or financial information to make purchases, get benefits, file taxes, or commit fraud? That's identity theft.

Visit IdentityTheft.gov to report identity theft and get a personal recovery plan.

The site provides detailed advice to help you fix problems caused by identity theft, along with the ability to:

- get a **personal recovery plan** that walks you through each step
- update your plan and track your progress
- print pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors

Go to **IdentityTheft.gov** and click "**Get Started**."

There's detailed advice for **tax**, **medical**, and **child identity theft** – plus over thirty other types of identity theft. No matter what type of identity theft you've experienced, the next page tells you what to do right away. You'll find these steps – and a whole lot more – at **IdentityTheft.gov**.

What To Do Right Away

Step 1: Call the companies where you know fraud occurred.

□ Call the fraud department. Explain that someone stole your identity. Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.

□ Change logins, passwords, and PINs for your accounts.

Step 2: Place a fraud alert and get your credit reports.

□ To place a free fraud alert, contact one of the three credit bureaus. That company must tell the other two.

- **Experian.com/help**
  888-EXPERIAN (888-397-3742)
- **TransUnion.com/credit-help**
  888-909-8872
- **Equifax.com/personal/credit-report-services**
  1-800-685-1111

A fraud alert lasts one year. It will make it harder for someone to open new accounts in your name.

Get updates at **IdentityTheft.gov/creditbureaucontacts**.

□ Get your free credit reports from Equifax, Experian, and TransUnion. Go to **annualcreditreport.com** or call 1-877-322-8228.

□ Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.

Step 3: Report identity theft to the FTC.

□ Go to **IdentityTheft.gov**, and include as many details as possible.

Based on the information you enter, **IdentityTheft.gov** will create your Identity Theft Report and recovery plan.

Go to IdentityTheft.gov for next steps.

Your next step might be closing accounts opened in your name, or reporting fraudulent charges to your credit card company.

IdentityTheft.gov can help – no matter what your specific identity theft situation is.

FEDERAL TRADE COMMISSION
IdentityTheft.gov
September 2018

Assessment of State Identity Theft Laws

1. Introduction

All 50 states and the District of Columbia have criminalized the act of identity theft. For the purpose of understanding how well the current definition of identity theft used in the Identity Theft Supplement (ITS) aligns with these state laws, we examined similarities and variations in the legal elements of identity theft across all 50 states and DC. The key elements of the laws that were examined were:

- How personally identifiable information (PII) is defined – this directly impacts the breadth and depth of the identity theft laws
- How PII is misused – whether the law focuses on just financial gain or nonfinancial uses as well
- The severity of punishments for identity theft – what are the thresholds for felony versus misdemeanor acts of identity theft
- The statute of limitations for charging identity theft offenders

This paper presents findings from the assessment, walking through each of the four key elements. The findings show that any commonalities in the laws are at a high-level. For example, all states recognize the misuse of PII for financial gain as a criminal offense. However, the laws vary widely in how explicitly they define PII, whether nonfinancial misuses of PII are also considered identity theft, whether the level of financial gain makes it a misdemeanor or felony offense, and how long the statute of limitations is. Because of these variations, we do not recommend any changes to the ITS. The ITS screener is broad enough to be aligned with the most expansive of state identity theft definitions, yet the elements collected on the instrument allow the data to be restricted to align with the specific elements of each of the state laws.

Determining which state statutes to include in the assessment

From one state to the next, a wide range of terminology is used in statutes related to identity theft. This is demonstrated in the titles of the statutes. In Arkansas code, identity theft falls under the titles of ‘financial identity fraud’ and ‘nonfinancial identity fraud;’ in Wyoming, under ‘unauthorized use of personal identifying information; in Kentucky, ‘theft of identity;’ and in Nevada, under “Obtaining and using personal identifying information of another person to harm or impersonate person, to obtain certain nonpublic records or for other unlawful purpose.” Other states simply use the terms ‘identity theft’ or ‘identity fraud’ but these terms are also used differently across different states. In Rhode Island, for example, the identity theft statute focuses largely on consumer fraud, whereas the identity fraud statute prohibits the misuse of personally identifiable information (PII). To further add complexity to the assessment of state identity theft laws, some states have a single statute that captures a broad range of identity theft-related offenses, whereas others have a series of separate statutes for identity theft, impersonation, trafficking in identifying information, possessing or manufacturing fraudulent identifying documents, serving as an accomplice in the commission of identity theft, and giving false information to a police officer. Because of this wide variation in how states label and classify identity theft, it was necessary to set guidelines about which statutes to use to best enable across state comparisons and to capture information most relevant to the Identity Theft Supplement.

A trained legal expert identified and compiled the state-level laws that are presented here by applying Boolean search strings in the LexisNexis database for all 50 states and D.C. Primary legal research was conducted in each state's statutory and administrative code databases. Boolean search strings included both keywords and searches based on the main numerical citations of each state's current identity theft laws. The laws included in the assessment specifically included the terms 'identity theft,' 'identity fraud,' 'theft of identity,' or 'misuse of identification' and intentionally focused on acts of identity theft committed against individuals. The assessment excluded laws related to identity theft that were focused on businesses as the victim, such as hacking; statutes focused on the trafficking of identifying information, since victims are unlikely to know that their information is being shopped around, until the point that an offender purchases and uses it; and laws focused on the possession or manufacture of false identifying information, which often encompass incidents in which the false information is entirely fabricated, rather than belonging to a living person.

In addition to the identity theft laws that were the focus of this assessment, all 50 states and DC also have independent credit card fraud statutes. Credit card fraud laws primarily focus on the unlawful obtaining and misuse of a victim's credit or debit card and the monetary harm that may occur from making unauthorized purchases. For example, the Iowa credit card fraud statute uses similar language as many of the other states:

> "A person commits the offense of fraudulent use of a credit card or debit card, if with purpose to defraud, he or she uses a credit card, credit card account number, debit card, or debit card account number to obtain property or a service with knowledge that:
>
> (1) The credit card, credit card account number, debit card, or debit card account number is stolen;
>
> (2) The credit card, credit card account number, debit card, or debit card account number has been revoked or cancelled;
>
> (3) The credit card, credit card account number, debit card, or debit card account number is forged; or
>
> (4)For any other reason his or her use of the credit card, credit card account number, debit card, or debit card account number is unauthorized by either the issuer or the person to whom the credit card or debit card is issued" (AR 5-37-207).

By contrast, states' identity theft laws apply much more broadly to the unlawful obtaining and use of a variety of different types of PII, including but not limited to, the victim's credit or debit card. Although the Iowa identity theft statute covers a broader spectrum of PII and actions, the law also states that "A person commits the offense of identity theft if the person fraudulently uses or attempts to fraudulently use identification information of another person, with the intent to obtain credit, property, services, or other benefit" (Iowa Code § 715A.8), which would include making charges on a credit card that one is not authorized to use.

Most states appear to have similar overlap in their statutes. A handful of states (less than 10) do not explicitly include credit or debit card numbers as a form of PII, presumably to make a clearer distinction between identity theft and credit card theft offenses. Kentucky is the only state for which the identity theft statute specifically notes, “This section does not apply to credit or debit card fraud under KRS 434.550 to 434.730” ((KRS § 514.160).

The identity theft laws often carry a higher maximum sentencing classification, but in 48 states, credit card fraud can also be a felony offense. Among these states, the monetary threshold for when an incident rises from a misdemeanor to felony offense is typically the same for both identity theft and credit card fraud.

The remainder of the assessment focuses only on those identity theft statutes that met the criteria for inclusion.

2. The Key Elements of States’ Identity Theft Laws

In all states, identity theft is legally defined by two key components 1) what constitutes PII; and 2) the types of illegal activities involving a victim’s PII that constitute identity theft. In addition to these key definitional components, identity theft laws specify the severity of the crime in that state - in terms of the level punishment assessed against an individual who has committed identity theft - and how long an offender can be charged with identity theft after the commission or discovery of the crime.

To examine the details of these four key elements, the assessment relied on Boolean search strings to capture and code explicit mentions to different types of PII and identity theft activities. Other details, such as the length of the statute of limitations were captured through manual text review. It should be noted that although a state statute may not specifically identify a particular activity or type of PII as constituting the misuse of identifying information, that activity may still be prosecutable under the general terms of the statute. For this assessment, however, we focused on explicit references to the legal details described below.

Specific Types of Information Defined as PII

One of the key factors determining the breadth of an identity theft statute is the range of information included under the umbrella of PII. Table 1 presents the states that utilize a broader definition of PII and those that are more specific about the pieces of information that constitute PII. About 35% of states use a specific PII definition, meaning that the statute provides an explicit and finite list of discrete items that can be classified as PII. These statutes do not reference broad categories of PII, such as ‘biometric data’ or ‘financial data,’ and do not include language allowing for the inclusion of other items not specified in the list. Delaware’s definition of “personal identifying information” is representative of this type of explicit definition:

> "(c) For the purposes of this section, ***“personal identifying information” includes*** name, address, birth date, Social Security number, driver’s license number, telephone number, financial services account number, savings account number, checking account number, payment card number, identification document or false identification document, electronic identification number, educational record, health care record, financial record, credit record, employment record, e-

> mail address, computer system password, mother's maiden name or similar personal number, record or information" (emphasis added). (11 Del. C. § 854).

The majority of states (65%) more broadly define PII, presenting examples of the types of information that are classified as PII, as well as a broader "catch-all" category that covers other types of information not specified in the list. The District of Columbia's law is representative of this broader definition:

> "DC Code § 22-3227.01. (3) "Personal identifying information" ***includes, but is not limited to***, the following:
> (A) Name, address, telephone number, date of birth, or mother's maiden name;
> (B) Driver's license or driver's license number, or non-driver's license or non-driver's license number;
> (C) Savings, checking, or other financial account number;
> (D) Social security number or tax identification number;
> (E) Passport or passport number;
> (F) Citizenship status, visa, or alien registration card or number;
> (G) Birth certificate or a facsimile of a birth certificate;
> (H) Credit or debit card, or credit or debit card number;
> (I) Credit history or credit rating;
> (J) Signature;
> (K) Personal identification number, electronic identification number, password, access code or device, electronic address, electronic identification number, routing information or code, digital signature, or telecommunication identifying information;
> (L) ***Biometric data***, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
> (M) Place of employment, employment history, or employee identification number; and
> (N) ***Any other numbers or information that can be used to access*** a person's financial resources, access medical information, obtain identification, act as identification, or obtain property (emphasis added)"

Table 1. List of states with a broad legal definition of PII and those with an explicit definition, 2020

Broader PII Definition	**Explicit PII Definition**
AL	AK
AZ	AR
CO	CA
CT	DE
DC	GA
FL	KY
HI	LA
IA	MA
ID	MI
IL	MN

IN	MS
KS	NE
MD	OH
ME	OR
MO	PA
MT	SC
NC	VT
ND	WV
NH	
NJ	
NM	
NV	
NY	
OK	
RI	
SD	
TN	
TX	
UT	
VA	
WA	
WI	
WY	

In terms of the specific types of PII that are covered by the state statutes, over 90% of states specifically identify a victim’s name as PII. Over 80% of states consider a victim’s payment card (i.e. credit, debit, Electronic Benefit Transfer) number to be PII. Three of the states that do not identify payment card numbers as PII in the identity theft statute, use a broad definition of PII that would include payment card numbers but does not specifically list them (e.g. Missouri - “’Means of identification’, anything used by a person as a means to uniquely distinguish himself or herself" (§ 570.010 R.S.Mo.). Half (50%) of all states specifically include a payment card number’s PIN number as PII and about 40% of states include the victim’s e-mail address and account passwords as types of PII. However, it should be noted that some states also have separate crimes pertaining to unlawfully obtaining personal information through a computer.

Specific Types of Activities that Constitute Identity Theft

A victim’s PII could be misused for the purpose of financial gain or for a host of nonfinancial reasons. All state identity theft statutes specify that the use of someone’s PII for financial gain - to obtain property or services or engage in a financial transaction - constitutes identity theft. However, a smaller proportion of state statutes identify nonfinancial misuses of information. The most common type of nonfinancial misuse identified in the statutes is the misuse of PII to obtain or maintain employment. About a quarter of states explicitly include language related to using a person’s PII to obtain employment. Less than 10 state statutes specify that identity theft occurs when someone uses a victim's PII to A. obtain false documents, B. open accounts, C. get or maintain employment, D. conceal the commission of a crime, or E. to avoid arrest or prosecution. This does not necessarily mean that these acts would not be prosecutable identity theft offenses, but simply that the law does not explicitly identity these activities as forms of identity theft.

The vast majority (about 75%) of states' identity theft statutes also explicitly make it a crime to unlawfully possess a victim's PII, even if the offender took no further action and the victim did not suffer any actual harm. Over 60% of states make it a crime to attempt to use a victim's PII or to give, sell or transfer a victim's PII to someone else.

Classifying the Severity of Identity Theft

Just over half of states classify identity theft as a felony-level offense only (i.e., identity theft is never a misdemeanor).[1] The other half of the states have both felony- and misdemeanor-level identity theft offenses. This includes states such as Louisiana and New Jersey that do not formally use the terms "felony" or "misdemeanor" but have state-level criminal codes that assess more severe penalties for certain types of identity theft acts.[2] State laws establish the severity of different types of identity theft by either presenting a tiered classification of offenses or by specifying punishment enhancements for offenses with certain characteristics. There is a great deal of variation in terms of how the 50 states and the District of Columbia assess whether an act of identity theft is a felony- or misdemeanor-level offense.[3] About a quarter of states utilize a grading system of offenses. These states specifically assign certain acts of identity theft involving a specific dollar amount or that involve other specific factors as a 1st degree, 2nd degree, or 3rd degree offense, or as a "Class [B, C, D, E] felony or misdemeanor."

Among the states that have both misdemeanor and felony offense, the thresholds for when an incident rises from the level of a misdemeanor to a felony are primarily based on financial losses or monetary gains. The monetary threshold for when the incident rises from a misdemeanor to a felony ranges from $75 in Alaska up to $2,000 in Pennsylvania. Some identity theft laws additionally consider the number of identity theft victims or pieces of identifying information misused, or the specific type of PII that was unlawfully used. Several of the states with misdemeanor offenses specifically note that PII used for a purpose other than financial gain, including to commit a crime or avoid arrest or prosecution, is a

[1] It should be noted that although credit card fraud laws were not specifically included in this assessment, in 48 states, credit card fraud can be classified as a felony offense.

[2] Louisiana classifies a crime that carries a sentence of "hard labor" as a felony-level penalty (La. R.S. § 14:67.16). "'Felony" is any crime for which an offender may be sentenced to death or imprisonment at hard labor." (La. R.S. § 14:2). New Jersey classifies misdemeanor-level crimes as acts that constitute a "disorderly conduct-level offense:" "A person who violates subsection a. of this section is guilty of a crime as follows: (1) If the actor obtains a benefit or deprives another of a benefit in an amount less than $500 and the offense involves the identity of one victim, the actor shall be guilty of a crime of the fourth degree except that a second or subsequent conviction for such an offense constitutes a crime of the third degree; or (2) If the actor obtains a benefit or deprives another of a benefit in an amount of at least $500 but less than $75,000, or the offense involves the identity of at least two but less than five victims, the actor shall be guilty of a crime of the third degree; or (3) If the actor obtains a benefit or deprives another of a benefit in the amount of $75,000 or more, or the offense involves the identity of five or more victims, the actor shall be guilty of a crime of the second degree. (N.J. Stat. § 2C:21-17).

[3] For example, Pennsylvania classifies an act of identity theft involving property with a value of $2000 or less as a misdemeanor of the first degree, while an offense involving property worth $2000 or more is classified as a felony of the third degree. (18 Pa.C.S. § 4120). In Alaska, fraudulent use of an identification document is a class B felony if the value of the property or services obtained is $25,000 or more; a class C felony if the value of the property or services obtained is $75 or more but less than $25,000; and a class A misdemeanor if the value of the property or services obtained is less than $75."

misdemeanor offense. Less than five state statutes include language that the length of time a victim's PII is used or the type of PII used have bearing on the severity of the offense. About 30% of the statutes include punishment enhancements if the offense involves an elder victim and about 15% include punishment enhancements if the offense involves a child victim.

Beyond financial losses, in about half of states, the identity theft laws take into consideration the damage that has been done to the victim's credit rating or financial reputation. These harms do not directly impact the classification of offense severity. Rather, states have articulated the laws provide specific remedies that are available to help the victim mitigate or offset this damage, separately and apart from the consideration of the severity of penalties.

Statute of Limitations

Just as the particular elements of identity theft crimes vary widely across the states, so too do the statute of limitations that establish the time limit in which the criminal punishment of an act of identity theft can be initiated. The states of Kentucky, North Carolina, South Carolina, West Virginia, and Wyoming do not place any time constraints on when the prosecution of identity theft must be initiated. This means that a prosecutor in these states could bring charges of identity theft against a suspected offender 5 months, 5 years, or even 50 years after the commission of identity theft. In all other states, the statute of limitations ranges from 1 year (Idaho only) to 7 years.

About 70% of states start the clock for the purposes of the statute of limitations time period from the date on which the act of identity theft was committed. The other 30% of states establish the beginning of the statute of limitations as the date on which the act of identity theft was first *discovered.* For example, in Connecticut, legal action may occur up to 3 years after the victim has discovered the identity theft (Conn. Gen. Stat. § 52-571h), North Dakota grants up to 6 years "after discovery by the victim" (ND Cent Code 12.1-23-11.), and New Mexico allows for up to 5 years after the time of discovery. (N.M. Stat. 30-1-8).

The District of Columbia is the only jurisdiction that starts the clock after the act(s) of identity theft "has been completed or terminated" (DC Code § 22-3227.07). This formula recognizes that an individual may be victimized multiple times. Some states offer two different statutes of limitations: one-time frame that dates back to the commission of the offense, and a different timeframe that first applies from the date of discovery that identity theft has occurred. For example, Florida requires a criminal prosecution of identity theft to occur within 3 years after the commission of the act, *or* "within 1 year after discovery of the offense by an aggrieved party, or by a person who has a legal duty to represent the aggrieved party and who is not a party to the offense, if such prosecution is commenced within 5 years after the violation occurred" (Fla Stat § 817.568). Virginia similarly allows a criminal action to be initiated within 5 years of the commission of the offense, or within 1 year "after the existence of the illegal act and the identity of the offender are discovered by the Commonwealth, by the owner, or by anyone else who is damaged by such violation" (VA Code Section 19.2-8).

3. Methodology and Limitations

State-level identity theft laws in all 50 states and D.C. were identified through primary legal research conducted by a legal researcher. First, identity theft laws were identified using two secondary sources:

1) The National Conference of State Legislature's "Identity Theft" database:
http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx; and
2) Identity Theft and Credit Card Fraud Laws available on FindLaw's website:
https://criminal.findlaw.com/criminal-charges/identity-theft.html;
https://criminal.findlaw.com/criminal-charges/credit-debit-card-fraud.html. Once the main identity theft laws in each state were identified, targeted Boolean search strings were created and applied within the subscription-based LexisNexis legal database to identify any additional, relevant state identity theft laws.

The Boolean search strings were created and laws were intentionally included or excluded based on 2 main criteria: 1) whether a state's law explicitly mentioned the word "identity" within five words of "fraud" or "theft."; or 2) whether a state law specifically referenced and included the numerical citation of the main identity theft law. For example, California's main identity theft law is Penal Code 530.5 and California laws that referenced this statute were eligible for inclusion.

This task did not include the following types of state-level laws: identity theft involving a business or organizational entity; general consumer fraud law; general theft offenses, such as burglary; laws that focus on cyber-hacking, or the infiltration of information housed within a computer network; the crime of producing or using a fake identification for the purposes of enabling a minor to obtain tobacco, alcohol, or other substances; laws that criminalize fraudulent access or use of access device

Some states have enacted additional laws that specifically criminalize certain aspects of identity fraud. In order to maintain internal consistency within each of the categories for the purposes of meaningful comparison, these narrow examples were not systematically captured. The following types of narrower state law examples were not captured: the crime of "vital records identity fraud" (e.g., Ala. Code § 31-13-14); the crime of impersonation of a police officer (e.g., NH Rev Stat 381:12); the crime of extortion, in which identifying information or property of specific value is threatened (e.g., VA Code Section 18.2-59); or the crime of committing identity theft in the context of an "immigration matter" (e.g., (S.C. Code Ann. § 14-7-1630).

Once a state's relevant identity theft laws were identified, these laws were then analyzed to determine if a state explicitly mentioned and regulated certain key elements, based on the established inclusion criteria of each key element. For example, the following keyword-based Boolean search strings was applied to determine if a state's crime of identity theft includes or requires that an individual suffered monetary loss:

- unanno(offense or felony or crime /50 (identity or "identifying information" or fraud! /9 misrepresent! or fraud! or identi! or decept!) or (theft /9 financial! or information! or identif!))

Similarly, the following Boolean search string was applied in LexisNexis to determine if a state separately criminalized the sole act of unlawfully possessing an individual's PII, even if no further action was taken to obtain the individual's property, or anything of value.

- unanno("identity theft" or "theft of identity" or "identity fraud" or "misuse of identification" or (misappropriation or taking or personal! or obtain! Or theft /7 identity or identifying /4 another or information or person or individual)) /30 (possess! /9 unlawful! or identify! or obtain! or personal! or information! /5 identity or identify! or information or document))

4. Recommendations

The ITS uses a screener that is broad enough to capture the full range of identity theft incidents reflected in state statutes and sufficient incident-level data that allows for further restriction of the incidents examined based on criteria of interest. For example, a data user in Kentucky interested in benchmarking Kentucky data to the nation, could exclude data on debit and credit card misuse from any analysis to be more aligned with their identity theft statute. Likewise, a data user in Nebraska who wanted to focus on incidents that would be felonies in Nebraska could limit the data to examine the consequences of identity theft incidents resulting in a loss of $1,500 or more.

Further narrowing the screener would eliminate incidents that could be classified as identity theft based on at least some of the state statutes. Making the screener broader to capture other offenses related to identity theft, such as possession or trafficking of stolen PII, would also be problematic because victims may not be aware that these activities are going on and the data would lack reliability. Therefore, based on this analysis, we do not recommend any changes to the BJS definition of identity theft currently operationalized in the ITS.

Identity Theft Supplement Secondary Data Analysis, Recommendations, and Next Steps

Introduction

In keeping with the Assessing the Measurement of Identity Theft Proposal, agreed upon by RTI and BJS in December 2019, this document presents findings and recommendations from the secondary analysis of Identity Theft Supplement (ITS) data. Using existing ITS data, RTI proposed to examine several key measurement issues that impact the definition and prevalence of identity theft: 1. The reference point used for determining whether an incident is within the survey reference period; 2. the unbounded nature of the ITS and the potential for respondents to 'telescope' incidents into the reference period; and 3. the inclusion of attempted incidents in the definition of identity theft. This document walks through these three measurement issues and presents the analysis and resulting recommendations. Key recommendations are as follows:

- Continue to use most recent occurrence[1] of misuse as the reference point in an identity theft incident that determines whether the incident is in scope; ask respondents to provide a month and year of most recent known occurrence to ensure that incidents are within the 12-month survey reference period.
- Consider using a duel reference period in the screener to reduce the likelihood of respondents telescoping incidents into the 12-month reference period. The first question would ask about experiences with a particular type of identity during an extended period of time (TBD), with a follow up question asking the respondent to date the most recent occurrence of that misuse. As noted above, the date of most recent occurrence would be used to determine whether the incident was within the reference period.
- Ask respondents to focus on successfully completed incidents of identity theft when answering detailed follow-up questions about the most recent incident. This will create more consistency in the incidents that are described in detail without impacting trends in overall prevalence rates.

The last section of the document proposes next steps that incorporate all three sets of recommendations.

Reference points

Measurement challenges: Most crimes are discrete events that can be pinpointed to a particular date on which the incident occurred. Because identity theft is episodic and often occurs without the victim's immediate, direct knowledge, dating an identity theft incident and determining whether it falls within the reference period of the survey is more complicated. There are several key points in an identity theft incident that could be used for the purpose of dating and determining whether the incident is within the reference period, including:

[1] The word 'occurrence' is used rather than 'incident' because we're talking about reference points *within* an incident – when it started, when it was discovered and the most recent time it happened/occurred (since an incident could be episodic with multiple occurrences of misuse happening in one incident). In many instances, there is only one occurrence of misuse in an incident so these terms refer to the same thing, but there are situations where the offender misuses the victim's information multiple times and we want to make sure we're capturing that as well.

1. When the offender first started misusing the victim's information (start);[2]
2. When the victim discovered that his or her information was being misused (discovery);
3. The last occurrence of misuse (occurrence); and
4. When the victim resolved all financial and credit problems related to the identity theft (resolution).

Although number 4 is critical for understanding the severity and harms of identity theft, using it to date an incident is akin to dating an assault based on when the victim was released from the hospital. Additionally, for the purpose of determining whether an incident is in the reference period, dating an incident based on when all financial and credit problems were resolved would mean that victims with unresolved problems at the time of the interview would technically not be eligible for inclusion. For these reasons, we focus on points 1 through 3 for the purpose of understanding dating and when an incident is within the reference period.

Current approach: The reference period for the current instrument is loosely framed around occurrences of misuse, with the screener asking if personal information has been misused in the prior 12 months. However, there is an inherent assumption in the current ITS instrument that reference points 2 and 3 (discovery and most recent occurrence of misuse) are one in the same. The survey asks victims the month and year they first discovered the misuse and how long the offender had been using their information when they discovered it, but there is no question about the date of the last occasion in which the offender used their information.

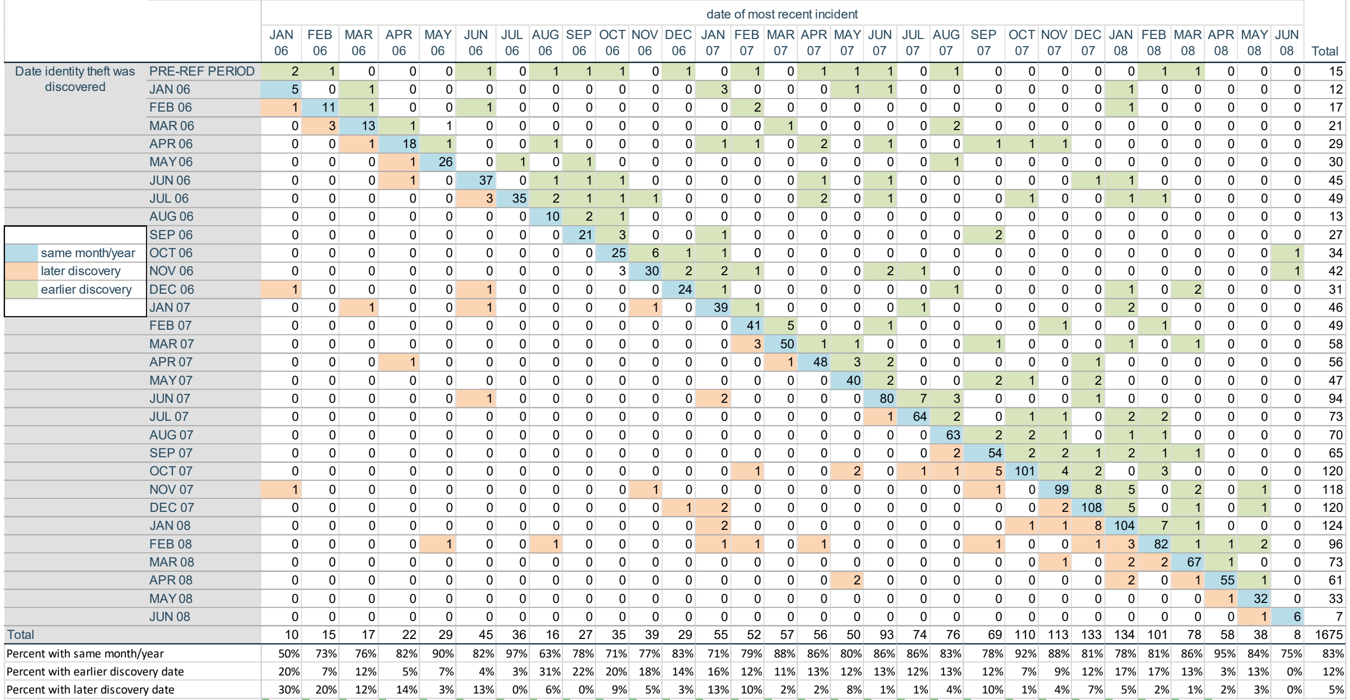
Part of the rational for not asking about the most recent or last occurrence of misuse was due to the challenge in defining an occurrence of misuse. For incidents involving the misuse of an existing account, an occurrence is easily defined as a charge made on the account without the victim's permission. With the use of personal information to open a new account or engage in other acts of misuse, occurrence is a more difficult concept. The last occurrence may not be the most recent time an offender made a financial charge to an account in the victim's name, but rather the date on which an account (that the offender opened using the victim's information) was closed or the victim's social security number was frozen to prevent the offender from using it.

Logically, it also makes sense to assume that as soon as a victim discovers the identity theft, he or she will take immediate steps to stop the offender, assuming the misuse has not already stopped. This logic was demonstrated in the 2008 ITS, which had a two-year reference period and asked victims both about the date of discovery and the date of the most recent misuse. Despite the fact that victims were not asked to focus on a single incident and could have been reporting on different episodes when offering the date of discovery and the date of occurrence, the large majority of victims (83%) who were able to provide dates for both points, offered the same month and year for discovery and most recent occurrence, as shown in figure 1. About 12% of victims provided a discovery date that was earlier than the date of the most recent occurrence, with less than 1% providing a discovery date that was outside of the two-year reference period. About 5% of victims provided a discovery date that was later than the date of the most recent occurrence, suggesting that they discovered the identity theft after it appeared to have stopped. It is important to note, however, that these percentages are based on the

[2] When the offender obtained the victim's personal information is not considered here because in some instances the act of taking the information could be considered a theft and would be measured separately. In other cases, the victim's information may be something that the offender legally has access to as a friend, family member, employer, etc.

approximately 60% of respondents who were able to provide month and year information for both the date of discovery and the date of most recent occurrence. About 40% of victims could not provide one or more of these pieces of information. Unfortunately, because the 2008 instrument did not ask the respondent to focus on a specific incident of identity theft when completing the questions about dates, it is not possible to determine whether these percentages differ by type of identity theft.

Figure 1. Date identity theft was discovered and date of most recent identity theft occurrence, 2008

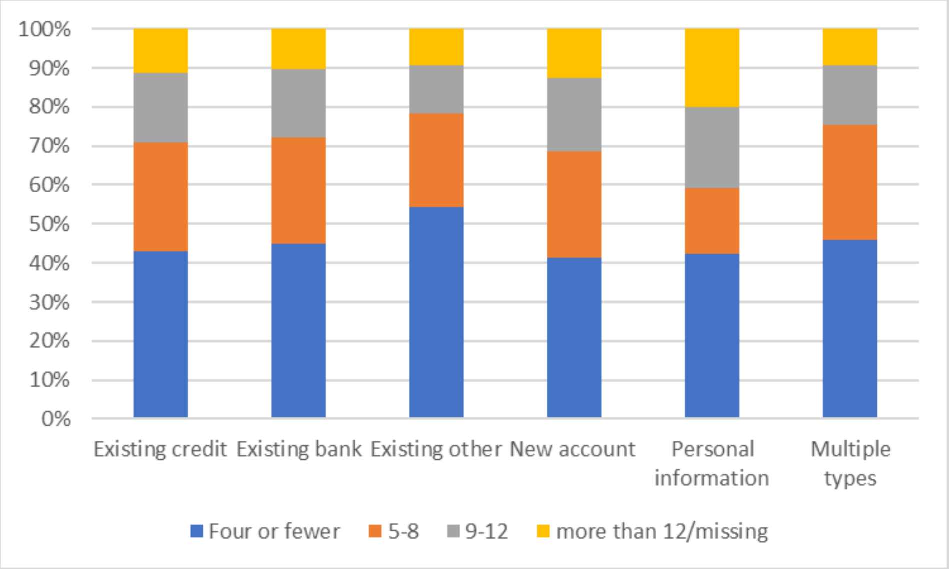


		date of most recent incident																													
		JAN 06	FEB 06	MAR 06	APR 06	MAY 06	JUN 06	JUL 06	AUG 06	SEP 06	OCT 06	NOV 06	DEC 06	JAN 07	FEB 07	MAR 07	APR 07	MAY 07	JUN 07	JUL 07	AUG 07	SEP 07	OCT 07	NOV 07	DEC 07	JAN 08	FEB 08	MAR 08	APR 08	MAY 08	JUN 08	Total
Date identity theft was discovered	PRE-REF PERIOD	2	1	0	0	0	1	0	1	1	1	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	0	0	0	15
	JAN 06	5	0	1	0	0	0	0	0	0	0	0	0	3	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	12
	FEB 06	1	11	1	0	0	1	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	17
	MAR 06	0	3	13	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	21
	APR 06	0	0	1	18	1	0	0	1	0	0	0	0	1	1	0	2	0	1	0	0	1	1	1	0	0	0	0	0	0	0	29
	MAY 06	0	0	0	1	26	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	30
	JUN 06	0	0	0	1	0	37	0	1	1	1	0	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0	45
	JUL 06	0	0	0	0	0	3	35	2	1	1	1	0	0	0	0	2	0	1	0	0	0	1	0	0	1	1	0	0	0	0	49
	AUG 06	0	0	0	0	0	0	0	10	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13
	SEP 06	0	0	0	0	0	0	0	0	21	3	0	0	1	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	27
🟦 same month/year	OCT 06	0	0	0	0	0	0	0	0	0	25	6	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	34
🟧 later discovery	NOV 06	0	0	0	0	0	0	0	0	0	3	30	2	2	1	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	1	42
🟩 earlier discovery	DEC 06	1	0	0	0	0	1	0	0	0	0	0	24	1	0	0	0	0	0	0	1	0	0	0	0	1	0	2	0	0	0	31
	JAN 07	0	0	1	0	0	1	0	0	0	0	1	0	39	1	0	0	0	0	1	0	0	0	0	0	2	0	0	0	0	0	46
	FEB 07	0	0	0	0	0	0	0	0	0	0	0	0	0	41	5	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0	49
	MAR 07	0	0	0	0	0	0	0	0	0	0	0	0	0	3	50	1	1	0	0	0	1	0	0	0	1	0	1	0	0	0	58
	APR 07	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	48	3	2	0	0	0	0	0	1	0	0	0	0	0	0	56
	MAY 07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	40	2	0	0	2	1	0	2	0	0	0	0	0	0	47
	JUN 07	0	0	0	0	0	1	0	0	0	0	0	0	2	0	0	0	0	80	7	3	0	0	0	1	0	0	0	0	0	0	94
	JUL 07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	64	2	0	1	1	0	2	2	0	0	0	0	73
	AUG 07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	63	2	2	1	0	1	1	0	0	0	0	70
	SEP 07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	54	2	2	1	2	1	1	0	0	0	65
	OCT 07	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2	0	1	1	5	101	4	2	0	3	0	0	0	0	120
	NOV 07	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	99	8	5	0	2	0	1	0	118
	DEC 07	0	0	0	0	0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	0	0	0	2	108	5	0	1	0	1	0	120
	JAN 08	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	1	1	8	104	7	1	0	0	0	124
	FEB 08	0	0	0	0	1	0	0	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	0	1	3	82	1	1	2	0	96
	MAR 08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	2	67	1	0	0	73
	APR 08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	2	0	1	55	1	0	61
	MAY 08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	32	0	33
	JUN 08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	6	7
Total		10	15	17	22	29	45	36	16	27	35	39	29	55	52	57	56	50	93	74	76	69	110	113	133	134	101	78	58	38	8	1675
Percent with same month/year		50%	73%	76%	82%	90%	82%	97%	63%	78%	71%	77%	83%	71%	79%	88%	86%	80%	86%	86%	83%	78%	92%	88%	81%	78%	81%	86%	95%	84%	75%	83%
Percent with earlier discovery date		20%	7%	12%	5%	7%	4%	3%	31%	22%	20%	18%	14%	16%	12%	11%	13%	12%	13%	12%	13%	12%	7%	9%	12%	17%	17%	13%	3%	13%	0%	12%
Percent with later discovery date		30%	20%	12%	14%	3%	13%	0%	6%	0%	9%	5%	3%	13%	10%	2%	2%	8%	1%	1%	4%	10%	1%	4%	7%	5%	2%	1%	2%	3%	0%	5%

Figure 2, which is based on 2018 data, shows the passage of time (number of months) from the month and year when the victim discovered the most recent incident of identity theft to the date of the ITS interview. Overall, less than 5% of victims provided a discovery date that was more than 12 months prior to the interview date and that held true across almost all types of identity theft. The exception was the misuse of personal information for purposes besides opening a new account. About 14% of these victims provided a date of discovery that was outside of the 12-month reference period. This may suggest that these victims are telescoping their experiences into the reference period or that this type of identity theft is more difficult to stop, and that, after the discovery, occurrences of the misuse continued into the reference period. Since the instrument does not ask when the actual misuse stopped, it is difficult to ascertain which explanation is more likely or prevalent.

For all types of identity theft, except for personal information misuse, about 90% of victims provided a discovery date that was within the 12-month reference period.

Figure 2. Months from discovery of identity theft to interview, by type of identity theft, 2018

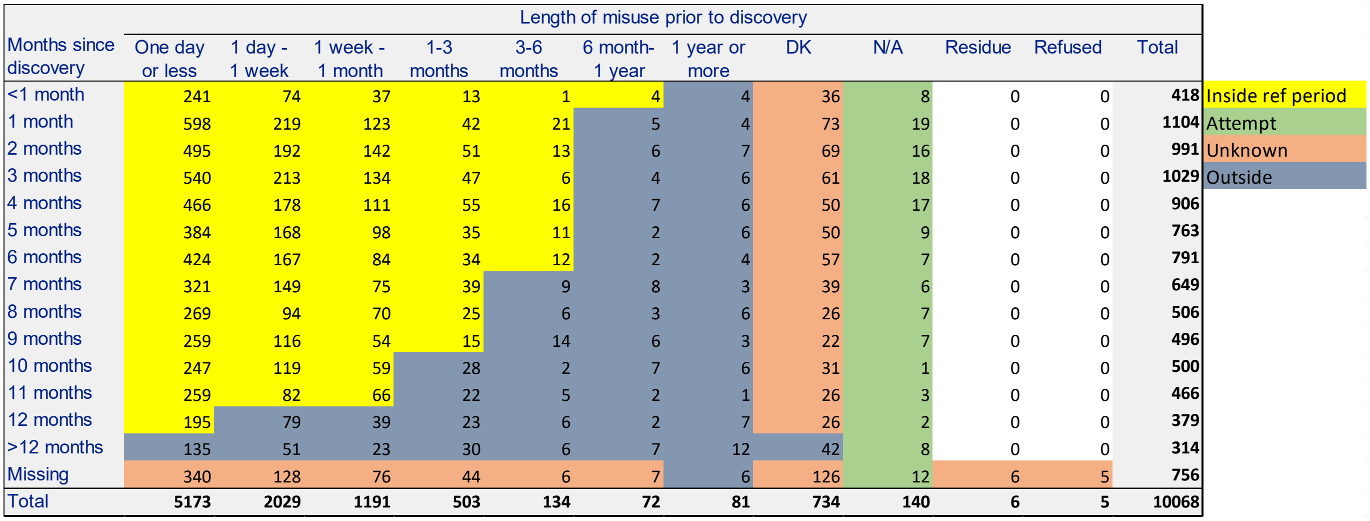


For about half of identity theft victims, reference points 1 and 2 (start and discovery of the misuse) also occurred on the same date. In 2018, 53% of victims discovered the most recent incident of identity theft one day or less after the misuse started.[3] When the analysis is limiting to just those victims who were not missing data about when the misuse started, that percentage increases to 58%.

Figure 3 shows the relationship between when the incident was discovered and whether the start of the incident is within the 12-month reference period. The determination on whether the start was within the reference period is based on the number of months from discovery to interview, plus the length of misuse prior to discovery. If the victim provided a date of discovery that was three months prior to the interview and then he or she responded that the start of misuse was three to six months prior to discovery, both the discovery date and the start date are within the reference period since we know that the start date was no more than nine months prior to the interview. For this analysis, we erred on the side of classifying incidents as outside the reference period rather than inside. In other words, if the victim said the start of misuse was three to six months prior to discovery, we assumed six months rather than three months.

[3] Includes victims who stated that their information was not actually misused.

Figure 3. Relationship between number of months from discovery to interview and whether the misuse started inside or outside of the reference period, 2018



	Length of misuse prior to discovery												
Months since discovery	One day or less	1 day - 1 week	1 week - 1 month	1-3 months	3-6 months	6 month- 1 year	1 year or more	DK	N/A	Residue	Refused	Total	
<1 month	241	74	37	13	1	4	4	36	8	0	0	**418**	Inside ref period
1 month	598	219	123	42	21	5	4	73	19	0	0	**1104**	Attempt
2 months	495	192	142	51	13	6	7	69	16	0	0	**991**	Unknown
3 months	540	213	134	47	6	4	6	61	18	0	0	**1029**	Outside
4 months	466	178	111	55	16	7	6	50	17	0	0	**906**	
5 months	384	168	98	35	11	2	6	50	9	0	0	**763**	
6 months	424	167	84	34	12	2	4	57	7	0	0	**791**	
7 months	321	149	75	39	9	8	3	39	6	0	0	**649**	
8 months	269	94	70	25	6	3	6	26	7	0	0	**506**	
9 months	259	116	54	15	14	6	3	22	7	0	0	**496**	
10 months	247	119	59	28	2	7	6	31	1	0	0	**500**	
11 months	259	82	66	22	5	2	1	26	3	0	0	**466**	
12 months	195	79	39	23	6	2	7	26	2	0	0	**379**	
>12 months	135	51	23	30	6	7	12	42	8	0	0	**314**	
Missing	340	128	76	44	6	7	6	126	12	6	5	**756**	
Total	**5173**	**2029**	**1191**	**503**	**134**	**72**	**81**	**734**	**140**	**6**	**5**	**10068**	

Based on the classification in the above figure, table 1 shows the relationship between whether the discovery was inside the reference period and whether the start of misuse was inside the reference period, based on weighted data. Overall, 79% of victims reported that the incident started and was discovered within the 12-month reference period. Another 14% did not know how long the misuse had been happening before it was discovered, and 2% said their information was not actually misused (attempted misuse). This leaves about 6% of victims for whom the start of the misuse was known to be outside of the reference period.

Table 1. Incidents for which the start of misuse was inside or outside the 12-month reference period, by number of months from discovery to interview, 2018

			Start of misuse							
Number of months since first discovery	Total		Inside reference period		Outside reference period		No actual misuse (attempt)		Unknown	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Total	23,901,317	100.00	18,767,613	78.52	1,498,363	6.27	364,437	1.52	3,270,904	13.69
Four or fewer	10,655,320	100.00	9,612,513	90.21	110,410	1.04	209,123	1.96	723,274	6.79
5-8	6,490,174	100.00	5,859,084	90.28	117,851	1.82	76,814	1.18	436,425	6.72
9-12	4,118,240	100.00	3,296,016	80.03	522,903	12.70	37,095	0.90	262,226	6.37
More than 12	759,213	100.00	0	0.00	739,053	97.34	20,160	2.66	0	0.00
Missing	1,878,370	100.00	0	0.00	8,147	0.43	21,244	1.13	1,848,979	98.44

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

Looking by type of identity theft, the percentage of misuse that started outside the reference period was less than 10% for victims of existing account misuse, 17% for the use of personal information to open a new account, and 24% for the use of personal information for other purposes (table 2). About 30% of victims of new account misuse and 40% of victims of personal information misuse did not know when the misuse started.

Table 2. Incidents for which the start of misuse was inside or outside the 12-month reference period, by type of identity theft, 2018

	Start of misuse										
	Inside reference period			Outside reference period			Attempt			Unknown	
Type of identity theft	Number	Percent		Number	Percent		Number	Percent		Number	Percent
Total	18,767,613	78.52	%	1,498,363	6.27		364,437	1.52		3,270,904	13.69
Existing credit	7,151,350	81.96	%	467,355	5.36		133,645	1.53		973,254	11.15
Existing bank	8,079,130	81.84	%	394,585	4.00		100,822	1.02		1,297,134	13.14
Existing other	1,218,654	75.85	%	139,052	8.65		47,579	2.96		201,475	12.54
New account	512,505	49.64	%	172,061	16.67		42,396	4.11		305,442	29.59
Personal information	237,028	33.06	%	172,320	24.03		23,895	3.33		283,813	39.58
Multiple types	1,568,946	80.55	%	152,991	7.85		16,100	0.83		209,787	10.77

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

Table 3 shows the impact on prevalence rates of excluding victims for whom the either the discovery or start of the most recent incident were unknown or outside the reference period. Not surprisingly, the shift in reference point appears to have the greatest impact on the misuse of personal information for other purposes, reducing the number of victims by about 45%.

Table 3. Change in identity theft prevalence rate if reference period was based on incident discovery date or start date, 2018

	Prevalence			Prevalence based on discovery date/a			Prevalence based on start of misuse/b	
Type of most recent incident	Count	Percent		Count	Percent		Count	Percent
Total	23,901,317	9.26	%	21,973,099	8.51	%	20,366,053	7.89
Existing credit	9,871,671	3.82		9,169,064	3.55		8,795,433	3.41
Existing bank	8,725,603	3.38		7,906,740	3.06		7,439,153	2.88
Existing other	1,606,759	0.62		1,514,020	0.59		1,393,279	0.54
New account	1,032,405	0.40		965,748	0.37		707,301	0.27
Other personal	717,056	0.28		616,813	0.24		393,586	0.15
Multiple	1,947,824	0.75		1,800,715	0.70		1,637,302	0.63

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

a/Excludes victims who experienced a single incident during the reference period and for whom the discovery date of that incident was unknown or more than 12 months prior to the interview.

b/Excludes victims who experienced a single incident during the refernece period and for whom the start of the misuse was unknown or more than 12 months prior to the interview.

Recommendations: In order to maintain trends in the prevalence of identity theft and not make major changes to the screener questions, BJS should continue to use date of occurrence – the last time the misuse happened - as the reference point for determining whether an incident is within the reference period. For the vast majority of victims, the date of occurrence and discovery will be one in the same or within a month of each other. Similarly, for the vast majority of victims, the start of the incident will also be within the one-year reference period.

In order to ensure that victims are not mixing up actual occurrences of misuse and unresolved financial and credit problems and reporting incidents that should be included in the long-term consequences section (misuse ended prior to the reference period but associated problems were still being resolved during the reference period), BJS should consider adding a question to capture the date of the most recent known occurrence of misuse, in addition to date of discovery. If a respondent provides a date of most recent occurrence that is outside of the reference period, he or she would be skipped to questions asking about long-term consequences, rather than going through all of the questions about the nature and characteristics of the most recent incident.

We propose that the new question would be asked in the screener section of the instrument (see more detailed recommendations under *Respondent Telescoping*). Cognitive testing will be needed to ensure that respondents are able to understand the distinctions between start, discovery, most recent occurrence, and resolving all associated financial and credit problems, and to ensure the proper ordering of these questions for maximum clarity. Additionally, because the concept of an occurrence differs among the different types of identity theft, cognitive testing will also be important for determining whether additional clarifying language is needed to help respondents understand the concept of the most recent occurrence of misuse.

The benefit to this approach is improved data reliability. Forcing respondents to think about the date of the most recent occurrence should reduce the likelihood that respondents will accidentally report incidents that should have been out of scope and should reduce potential respondent confusion about how to place episode in time. The drawback to this change is that it could impact the comparability of findings to the prior years. However, evidence from this assessment suggests that, putting aside potential issues with telescoping, the vast majority of victims do not have challenges with identifying incidents that occurred within the reference period, even without asking more specific dating questions.

Respondent telescoping

Measurement challenges: Unlike the core NCVS for which interviews 2-7 are bounded by the prior interview, the ITS and other NCVS supplements are completely unbounded. Because the ITS is administered every two years, in any given ITS administration, the majority of respondents are receiving the survey for the first time. For the relatively small portion of respondents who are receiving it for the second time, it will have been two years since they last took it and the reference period of the survey goes back one year from the time of the interview. This means that respondents could be telescoping identity theft incidents into the reference periods without survey administrators having any way of recognizing it.

Telescoping could occur for several different reasons: 1. It could be intentional, which occurs in situations where the respondent wants to talk about his or her experiences even though they are outside of the reference period; 2. It could occur because of recall issues if the respondent is not sure about the date of the incident and places it more recently in time than it actually occurred; and 3. It could be related to aforementioned issues around the various reference points associated with an incident. Specifically, if the misuse has stopped but the respondent is still resolving problems related to the incident, he or she may think of that incident as ongoing and being within the reference period; particularly, if the survey questions do not provide clear guidance about the relevant reference point.

Unless the respondent provides a date for the incident that is outside of the reference period, is difficult to determine concretely whether a respondent has telescoped. As discussed previously, the ITS does not currently ask respondents to date the most recent occurrence of misuse. It asks about date of discovery, but based on data from 2008, it is possible that some incidents are discovered well before the misuse can be stopped, so the available survey dates cannot alone be used to make this determination. There are two other potential ways to identify telescoped incidents: 1. If a respondent who completes two iterations of the ITS reports the same incident the second time completing the survey, and 2. If a respondent appears to report the same incident in the long-term consequences section of the survey instrument that he or she reported as being within the reference period. This might be evidence that the respondent was confused about the survey reference period; reported an incident in the main body of the survey that should have been out of scope; and then rereported it in the long-term consequences section after realizing that it should have been reported there in the first place.

Reports of the same incident across two survey waves. About 10% (19,687) of eligible respondents to the 2014 ITS were also eligible to complete the 2016 ITS. Of these, 66% (13,117) completed both of their ITS interviews. Among those who completed both interviews, 1,220 were victims of identity theft in 2014; 1,153 were victims in 2016; and 212 were victims in both years. Although it is possible that victims who experienced identity theft in one year or the other engaged in telescoping, there is no way to determine whether it actually occurred. Thus, we examine the 212 victims who experienced identity theft in both years in order to determine whether the incidents reported in 2016 were similar to the incidents reported in 2014.

Of the 212 victims who reported identity theft in both periods, 120 (57%) reported experiencing the same type of incident in 2016 as in 2014. The majority experienced the misuse of an existing account, with 80 victims experiencing existing credit card misuse in both periods and 34 experiencing the misuse of an existing bank account in both periods. Six victims experienced multiple types of identity theft during the same incident in both periods, but none reported the use of personal information to open a new account or for other purposes across both periods.

Table 4 shows a comparison of the characteristics of the most recent incident among victims who reported the same type of incident during both interviews. It presents unweighted counts since 2014 and 2016 use different weights, which would impact the comparability. For most questions, very few respondents provided substantive responses that were consistent across both interview waves. One exception is reporting to police where most respondents said ‘no’ across both interview waves. This cannot be taken as indication of telescoping, however, since reporting identity theft to police is relatively rare in the first place. None of the victims provided the same responses to all the questions examined in table 4 (not shown), which suggests that they are not likely reporting on the same incident across both waves.

Table 4. Characteristics of identity theft incidents among victims who experienced the same type of identity theft in 2014 and 2016

	Existing credit card	Existing bank account
Total	34	80
How personal information was obtained		
Same reason given	2	3
Both unknown	17	51
Different reason given	15	26
Reported to law enforcement		
Both yes	1	1
Both no	28	75
Different responses	5	4
How distressing was the incident		
Same response	8	28
Different responses	26	52
Amount of direct loss		
Both $0	3	6
Both unknown	1	1
Same $ amount	2	4
Different $ amount	28	69
Amount of out-of-pocket loss		
Both $0	15	40
Both unknown	4	10
Same $ amount	0	0
Different $ amount	15	30

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2014 and 2016.

It should be noted that the lack of evidence of telescoping across the two interview waves does not mean that respondents are not telescoping; just that we did not identify telescoping through this analysis. It could be that respondents tend to telescope in incidents that happened less than a year outside of the reference period and that the amount of time between the two incidents is too long to effectively identify telescoping.

Reports of the same incident within the same interview. The Long-Term Consequences section of the ITS asks respondents whether, outside of the past 12 months, they have EVER experienced identity theft. To examine whether any of the incidents reported in the long-term consequences section of instrument appear to be the same as those reported as in scope, we start by examining whether victims whose most recent incident was discovered outside of the reference period are more likely to report long-term identity theft, particular long-term incidents for which they are still experiencing problems. For this analysis we use 2018 data because of the more specific dating of when the incident was discovered. Table 4 shows that overall about 1.3% of respondents were still experiencing problems at the time of the interview from an identity theft that occurred outside of the 12-month reference period. Among respondents who reported in their most recent incident as having been discovered more than 12 months prior to the interview, that percentage increased to 4.2%. This apparent increased propensity among these respondents may suggest that at least some of them are reporting the incident again in the long-term consequences section, recognizing that it is applicable.

Table 4. Number of months since discovery of most recent incident by whether victim reported experiences with identity theft outside of the prior 12 months, 2018

	ID theft outside of prior 12 months			
		Yes		
Number of months since first discovery	No	Total	Still experiencing problems	Experienced problems during past 12 months
Total	88.3 %	11.5 %	0.49 %	0.61 %
No identity theft	89.5	10.3	0.40	0.51
Four or fewer	77.2	22.3	1.30	1.65
5-8	76.9	22.6	1.10	1.30
9-12	74.8	24.8	1.30	1.54
more than 12	78.0	20.7	4.20	4.86
missing	78.0	18.8	0.90	1.00

Note: Details may not sum to 100% due to missing data.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

Similarly, table 5 shows that the percentage of victims still experiencing problems from an incident that occurred outside of the 12-month reference period appears higher among those for whom the most recent incident started outside the reference period compared to inside the reference period.

Table 5. Whether most recent incident started inside or outside the reference period by whether victim reported experiences with identity theft outside of the prior 12 months, 2018

	Id theft outside of prior 12 months			
		Yes		
Start of most recent ID theft and type	No	Total	Still experiencing problems	Experienced problems during past 12 months
Total	88.3 %	11.5 %	0.49 %	0.61 %
No identity theft	89.5	10.3	0.40	0.51
Started inside reference period	76.2	23.3	1.1	1.3
Started outside reference period	75.8	22.8	2.9	3.6
Attempt	83.6	15.3	0.0	1.1
Unknown	79.4	18.3	2.0	2.1

Note: Details may not sum to 100% due to missing data.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

To assess whether victims may be reporting the same incident in both the most recent and long-term consequences sections of the instrument, we examine the type of identity theft reported in both sections, among those victims whose most recent incident either started or was discovered outside the reference period. Table 6 shows that there does appear to be a relationship in the types of identity theft that these victims reported in each section. For example, among those who experienced existing credit card misuse as the most recent incident, 18% reported also experiencing existing credit card misuse in the long-term consequences section of the instrument, while only 5% reported existing bank account misuse in the long-term consequences section, and less than 1% reported other types of identity theft in the long-term consequences section. Among those whose most recent incident was the misuse of personal information to open a new account, which was dated outside of the reference period, 15% also reported the misuse of personal information to open a new account in the long-term consequences section. In comparison, less than 5% of victims who experienced other types of identity theft during the most recent incident and dated them outside of the reference period, reported the misuse of personal information to open a new account in the long-term consequences section.

Table 6. Types of identity theft reported inside and outside the reference period, among those for whom the start or discovery of the most recent incident was outside the reference period, 2018

	Identity theft experienced outside of prior 12 months						
Most recent identity theft that started or was discovered outside of reference period	Existing credit		Existing bank	Other existing	New account	Other fraudulent purpose	No identity theft
Existing credit card	18.1	%	4.9	0.0	0.7	0.9	75.7
Existing bank account	2.6	%	11.2	0.5	3.0	0.4	82.3
Other existing	7.6	%	5.8	6.2	3.3	6.4	74.8
New account	12.0	%	10.1	5.5	15.5	8.8	73.0
Other fraudulent purpose	8.7	%	2.0	0.0	4.4	9.0	81.1
Multiple types	22.5	%	5.9	2.5	8.6	12.0	59.6

Note: Details may not sum to 100% due to missing data and victims who reported multiple types of identity theft experienced outside of the prior 12 months.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

Despite this apparent relationship, of the 81 unweighted victims whose most recent incident was the same type as the identity theft experienced outside of the prior 12 months, none of the victims reported the same amount of indirect loss (the only question about monetary losses asked in both sections).[4] Part of this may be due to differences in how the questions about indirect losses are presented in the two sections (in the long-term consequences section, the question does not follow the questions about direct and out-of-pocket losses, as it does in the main body of the instrument).

Both sections of the instrument also asked victims a series of questions about problems they experienced as a result of the identity theft. Table 7 shows the congruity in responses among the 81 unweighted victims whose most recent incident was the same type as that experienced outside of the reference period. Of the 81 victims, 69 of the respondents screened out of the long-term consequences section because they said they had not experienced problems during the year, and for the purpose of analysis, these victims are treated as though they gave ‘no’ responses to the individual questions. The vast majority of victims also gave ‘no’ responses to these questions when asked about the most recent incident. Therefore, there is a high degree of congruity in the responses in that most victims said they did not experience the different types of problems for either of the incidents. Unfortunately, because the problems are relatively rare in the first place, this cannot be taken as conclusive evidence that the victims were reporting on the same incident in both sections.

[4] The response options to the long-term consequences indirect loss question are categorical, presenting different ranges of monetary loss. In contrast, the indirect loss question in the most recent incident section allows the victim to provide a specific monetary value. For this analysis we compared whether the monetary value provided in the most recent incident section was within the range selected in the long-term consequences section.

Table 7. Types of problems experienced as a result of most recent and long-term identity theft incidents, 2018

Types of problems	Unweighted count
Total	81
Problems with job or school	
Both yes	0
Both no	76
Problem with family or friends	
Both yes	3
Both no	74
Credit problems	
Both yes	4
Both no	69
Banking problems	
Both yes	1
Both no	75
Dealing with debt collectors	
Both yes	2
Both no	69
Utilities cut off	
Both yes	0
Both no	78
Turned down for job	
Both yes	0
Both no	79
Legal problems	
Both yes	1
Both no	77

Note: Includes victims who reported the same type of incident in both section of the instrument and for whom the start date or discovery date were outside of the reference period.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

Recommendations: Using existing variables on the ITS survey instrument, it is difficult to find conclusive evidence that respondents are telescoping identity theft incidents into the one-year reference period. However, given evidence of telescoping on the core NCVS and the potential for respondent confusion regarding the different reference points in an identity theft incident, we recommend further analysis. As noted in the original proposal, we recommend building on the findings from prior research that a dual reference period can be useful at controlling telescoping (see for example, Loftus et al., 1990). Prohaska and colleagues (1998) additionally found that asking people to provide a specific date for when an incident occurred rather than answer a yes/no question about whether something happened during a particular period can help to control telescoping. Thus, we propose testing two different approaches to controlling telescoping in the ITS (which could potentially be applied to other supplements as well). The approaches would differ in the length of the initially presented reference period (lifetime vs. five years), but would otherwise flow like this:

1. Do you currently have or have you ever had at least one active checking or savings account through a bank or financial institution?

YES
NO (skip to credit_lifetime)

2. Has someone EVER, without your permission, used your existing checking or savings account, including any debit or ATM cards?

YES
NO (skip to credit_lifetime)

3. In what year, did this misuse most recently occur? _______________

EARLIER THAN 2020 (skip to credit_lifetime)
DON'T KNOW (ask 3a)

3a. Do you think the misuse happened in the past 12 months, that is since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR]?

YES
NO
(all responses, skip to credit_lifetime)

4. In what month did this misuse most recently occur? ________________

DON'T KNOW (ask 4a)

4a. Do you think the misuse happened in the past 12 months, that is since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR]?

YES
NO

The survey would continue asking this sequence of questions for the other types of identity theft. If respondents did not report any identity theft incidents in the screener, the survey would end. If the only incidents reported were outside of the 12-month reference period, the respondents would be skipped immediately into the long-term consequences section, which would ask whether the respondent was still experiencing credit and financial problems as a result of the experience. As with the current instrument, if respondents reported incidents occurring during the prior 12 months, they would be asked the detailed follow-up questions about the most recent incident.

Research has shown that asking about a longer reference period, followed by the shorter period of interest, reduces forward telescoping by conveying to respondents that the dates of the events are important and forcing them to think about dating in more detail. Additionally, respondents' social desirability concerns can lead them to want to provide useful information in response to survey questions. A dual reference period enables events outside of the reference period to still be reported (Loftus et al., 1990; Sudman et al. 1984), while not impacting estimates from the period of interest. Although researchers have found that natural sequence is key for internal bounding and that asking a shorter or more recent reference period followed by a longer or later period is not effective at controlling telescoping, there is no research to suggest the optimal length of reference periods, since this is largely contingent on the phenomenon of interest. The studies that have tested the effectiveness of the dual reference period used considerably shorter reference periods than the ITS. For instance, Loftus and colleagues (1990) experimented with reference periods of two months followed by six months; six months followed by two months; and the prior month followed by the prior two months.

Several federal data collections ask about multiple reference periods within the same reference period, yet methodological descriptions and articles about these collections are largely void of discussion related to bounding and telescoping. Surveys, such as the National Survey of Family Growth and the National Survey of Drug Use and Health (NSDUH) ask questions about both lifetime experiences and experiences and experiences in the prior 12-months. For instance, many of the sections of NSDUH on substance use begin with questions about whether the respondent used the drug in their lifetime, including age at first use, followed by questions about use in the prior 12-months and use in the prior month, if they answer the lifetime question affirmatively. The Substance Abuse and Mental Health Services Administration (SAMSHA) reports NSDUH estimates based on each of these reference periods when possible. Although several studies (see, for example, Johnson et al., 1997; Johnson et al., 2005) have examined the potential for forward telescoping in NSDUH and its predecessor survey, particularly in reference to the age-at -first-use questions, the role of the dual reference period in reducing telescoping has received limited attention. In 2004, however, SAMSHA discontinued the long-term measures of pain reliever use in NSDUH because of the discovery of underestimation bias in the lifetime measures (Gfroerer, 2018).

One federal study, the National Intimate Partner and Sexual Violence Survey (NISVS), asks respondents questions about lifetime, three-year, and one-year experiences with a range of different types of victimizations. However, we are unaware of any research assessing whether the use of multiple reference periods helps to control telescoping. This may be due to the fact that the multiple reference periods are not intended to identify incidents that occurred within a certain reference period, but rather to help cue respondents to think about all of the things that different offenders may have done to them.

Given the limited available guidance on the most effective use of dual reference periods for internal bounding, we propose testing the effectiveness of a lifetime reference period followed by the 12-month reference period, as well as a five-year reference period followed by the 12-month reference period. The benefit of starting with a lifetime reference period is that the ITS already asks questions about lifetime experiences with identity theft and these estimates can be useful for understanding the stock of victims. Although asking lifetime questions first should serve to reduce any forward telescoping due to respondent desires to participate in the survey and talk about their experiences, it may not be as effective at getting them to focus on the exercise of dating. Thus, we propose to test whether a five-year reference period is more effective for reducing telescoping by forcing respondents to think about more concrete periods of time.

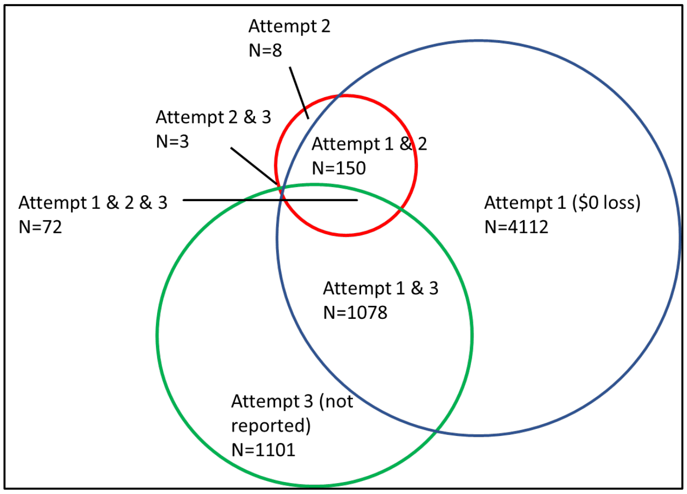
If the testing were done using an online survey panel, we could efficiently and affordably recruit a sufficient number of respondents to determine statistically significant differences in one-year prevalence estimates generated through the two experimental approaches and the control group (current approach). We propose in-person cognitive testing of the proposed changes prior to web-based testing to ensure that the added reference period is not overly complicated or challenging for respondents to follow

Attempts

Measurement challenges: Current screener questions ask respondents to think about the ‘use or attempted use’ of their identifying information without permission. Recent BJS reports have not distinguished between attempted and completed incidents, in part because of challenges with defining attempted versus completed incidents. There are three possible ways of identifying an attempted incident with the current survey instrument: 1. The distinction could be based on whether the offender was able to obtain something of value (money, products, services, benefits) from the victim.[5] If the offender was not able to obtain anything from the misuse, we assume it was an attempt that was stopped through third party intervention. However, this distinction works for existing account misuse but is more challenging when a victim's personal information is used to open a new account or for other fraudulent purposes. For instance, if the offender opens a new account in the victim's name, whether he or she makes any charges on the account, it would still be considered a completed incident of identity theft. Likewise, if the offender falsely provided the victim's information to law enforcement or the courts, this would be a completed incident of identity theft, but would not necessarily have a monetary value attached to it; 2. The survey asks respondents (Q10) how long their information was misused before they discovered it and one of the response options is 'not applicable – it was not actually misused.' A potential issue with this definition is that respondents are not given guidance on what it means for their information to be 'not actually misused;' 3. If a victim did not report the incident to law enforcement, one reason he or she could give for not reporting was that 'I did not lose any money/it was an attempt.' An obvious challenge with using this item to make the distinction is that attempted identity theft could be reported to police or not reported to police for a separate reason and would not be identifiable.

Figure 4 uses data from 2014 and 2016 to show the relationship between incidents that would be defined as attempts based on at least one of the three measurement approaches. As the figure shows, about 72 of 6,542 potential attempts (1.1%) met all three definitions.

Figure 4. Venn diagram of identity theft incidents that met at least one of three potential definitions of an attempt, 2014 and 2016.



Focusing just on incidents involving the misuse of an existing account further demonstrates the complexities of defining attempts. In 2014 and 2016 combined, there were 4,335 incidents of existing account identity theft with $0 in direct loss, suggesting that the offender was prevented from actually making a charge on the account. One would assume that among these types of identity theft, this would

[5] This analysis focuses on whether the offender successfully obtained products or services regardless of whether the victim was reimbursed for any financial losses. A victim may be reimbursed by a financial institution but that does not change whether the offender successfully carried out the identity theft.

be the most straightforward measure. However, examination of the responses to the questions aligning with the other two indicators of an attempt, demonstrates the lack of consistency in responses (table 8. About 23% of victims who experienced $0 in losses from existing account misuse said that they did not report to police because it was an attempt, and 4% said their information was not actually misused. It makes sense that some victims who experienced attempted identity theft may report to police or have other reasons for not reporting, and that there would not be perfect overlap between these two categories. However, it is harder to reconcile that a respondent who experienced an attempt would say that their information was used for more than a day or even a day before they discovered it.

In 2014 and 2016, there were 2,029 incidents of existing account misuse that were not reported to police because the victim did not suffer a loss or because the incident was an attempt. However, nearly half of these victims reported direct losses of $1 or more, suggesting that respondents may be selecting this reason for not reporting when their direct losses have been reimbursed by a financial institution in addition to when there were no direct losses.

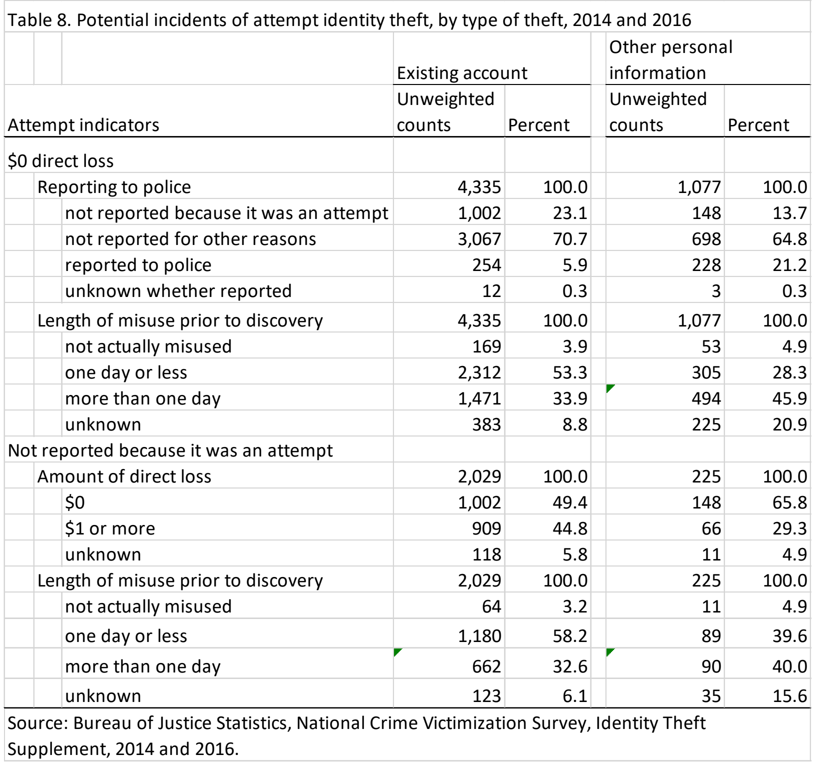


Table 8. Potential incidents of attempt identity theft, by type of theft, 2014 and 2016

	Existing account		Other personal information	
Attempt indicators	Unweighted counts	Percent	Unweighted counts	Percent
$0 direct loss				
Reporting to police	4,335	100.0	1,077	100.0
not reported because it was an attempt	1,002	23.1	148	13.7
not reported for other reasons	3,067	70.7	698	64.8
reported to police	254	5.9	228	21.2
unknown whether reported	12	0.3	3	0.3
Length of misuse prior to discovery	4,335	100.0	1,077	100.0
not actually misused	169	3.9	53	4.9
one day or less	2,312	53.3	305	28.3
more than one day	1,471	33.9	494	45.9
unknown	383	8.8	225	20.9
Not reported because it was an attempt				
Amount of direct loss	2,029	100.0	225	100.0
$0	1,002	49.4	148	65.8
$1 or more	909	44.8	66	29.3
unknown	118	5.8	11	4.9
Length of misuse prior to discovery	2,029	100.0	225	100.0
not actually misused	64	3.2	11	4.9
one day or less	1,180	58.2	89	39.6
more than one day	662	32.6	90	40.0
unknown	123	6.1	35	15.6

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2014 and 2016.

Other Potential Issues with Measuring Attempts: Although virtually impossible to measure, it is also possible that victims may fail to report attempts to the survey due to:

- Recall failure – victims may be less likely to remember attempted incidents, meaning a higher risk of false negative error due when attempts are included.
- Lack of awareness – if an offender is not successful in using the victim’s information, the victim may never be aware that an attempt occurred.

Table 9 compares the nature of incidents and victim experiences across successful incidents and attempts. Attempts are measured in three ways, reflecting a more to less conservative approach: 1. Victims who answered Q10 (how long was your information misused before you discovered it) with the response ‘not applicable – it was not actually misused;’ 2. Victims of any type of identity theft who experienced $0 in direct losses AND either did not report to police because it was an attempt OR responded to Q10 that it was not actually misused (meets 2 of 3 criteria); 3. All victims of existing account misuse who experienced $0 in direct losses and for victims of new account or other personal information misuse, those who met any 2 of the 3 criteria. On the flip side, the completed incident counts associated with attempts 1 include any victims who did not select response option 9 in Q10. The completed incident counts associated with attempts 2 include a. victims who lost $1 or more and b. victims who lost $0 AND did not select either option 9 in Q10 OR ‘it was an attempt’ as a reason for not reporting to police (includes those who did report to police). Finally, the completed incident counts associated with attempts 3 include a. victims of existing account misuse with losses of $1 or more; b. victims of new account or personal information misuse with losses of $1 or more and c. victims of new account or personal information misuse with losses of $0 who did not select response option 9 in Q10 AND did not select ‘it was an attempt’ as a reason for not reporting to police.

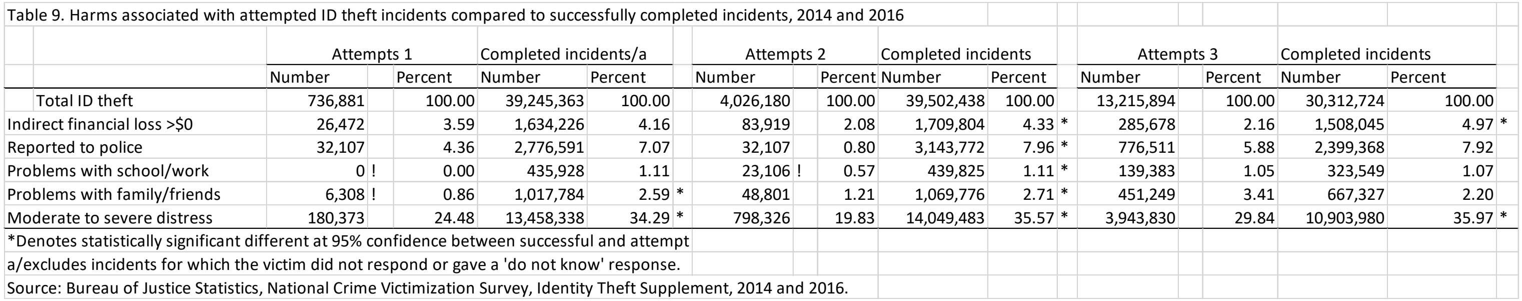


Table 9. Harms associated with attempted ID theft incidents compared to successfully completed incidents, 2014 and 2016

	Attempts 1		Completed incidents/a		Attempts 2		Completed incidents		Attempts 3		Completed incidents	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Total ID theft	736,881	100.00	39,245,363	100.00	4,026,180	100.00	39,502,438	100.00	13,215,894	100.00	30,312,724	100.00
Indirect financial loss >$0	26,472	3.59	1,634,226	4.16	83,919	2.08	1,709,804	4.33 *	285,678	2.16	1,508,045	4.97 *
Reported to police	32,107	4.36	2,776,591	7.07	32,107	0.80	3,143,772	7.96 *	776,511	5.88	2,399,368	7.92
Problems with school/work	0 !	0.00	435,928	1.11	23,106 !	0.57	439,825	1.11 *	139,383	1.05	323,549	1.07
Problems with family/friends	6,308 !	0.86	1,017,784	2.59 *	48,801	1.21	1,069,776	2.71 *	451,249	3.41	667,327	2.20
Moderate to severe distress	180,373	24.48	13,458,338	34.29 *	798,326	19.83	14,049,483	35.57 *	3,943,830	29.84	10,903,980	35.97 *

*Denotes statistically significant different at 95% confidence between successful and attempt

a/excludes incidents for which the victim did not respond or gave a 'do not know' response.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2014 and 2016.

Even with the most inclusive definition of attempts (attempt 3), these incidents account for less than half of the most recent incidents experienced by victims. There is no way of knowing what the actual percentage of attempts is, but with the technology put in place by the financial institutions alone, one would expect that more identity theft is prevented than what successfully occurs. As noted previously, it may be the case that victims are not made aware of or do not remember these attempted incidents, or it may be that victims report about attempts in the screener questions, but choose to report about a different incident when they’re asked to think about the most recent incident of identity theft. Either way, the relatively low number of attempts compared to completed incidents likely suggests that attempts are not being fully enumerated through the NCVS.

Differences in victim experiences: When attempted incidents are reported by victims, combining these with completed incidents may serve to dilute the negative impact of completed identity theft. Although victims of attempted identity theft may experience negative impacts, one would expect those harms to be less prevalence and less severe than for victims of completed identity theft.

Table 9 (above) also shows that based on all three definitions, a smaller proportion of attempted victims experience harms than victims of completed identity theft. Using the attempt 2 definition, all of the differences between the victims of completed and attempted incidents were statistically significant. It is important to note though, regardless of how attempts are defined, there are still victims of attempted incidents of identity theft who experience negative consequences, including indirect financial losses and moderate to severe distress, and some of these incidents are reported to police.

Impact of excluding attempts on prevalence estimates. Using the three definitions of an attempt, we computed the prevalence of identity theft if attempts were removed (table 10). A victim whose most recent incident was an attempt could have experienced a completed incident earlier in the reference period, so those victims who experienced multiple incidents were not excluded from the prevalence rate, regardless of whether they experienced an attempt during the most recent incident. Regardless of the definition or year, about three-fourths of victims who experienced an attempt during the most recent incident had only that one incident.

Table 10. Change in identity theft prevalence rate with removal of attempted incidents, 2014 and 2016

	2014								
	Original prevalence		Prevalence minus attempts (definition 1)		Prevalence minus attempts (definition 2)		Prevalence minus attempts (definition 3)		
Most recent ID theft	Number	Percent	Number	Percent	Number	Percent	Number	Percent	
Any	17,576,205	7.05	17,276,940	6.93	15,959,215	6.40	13,184,329	5.29	*
Existing credit card account	7,329,114	2.94	7,241,245	2.90	6,651,886	2.67	5,530,828	2.22	*
Existing bank account	6,735,809	2.70	6,629,041	2.66	6,151,199	2.47	6,285,591	2.52	
Other existing account	980,281	0.39	927,518	0.37	831,895	0.33	530,063	0.21	
New account	683,309	0.27	661,262	0.27	578,782	0.23	578,782	0.23	
Personal information	546,424	0.22	534,478	0.21	519,270	0.21	519,270	0.21	
Multiple types	1,301,268	0.52	1,283,396	0.51	1,226,183	0.49	1,226,183	0.49	
	2016								
	Original prevalence		Prevalence minus attempts (definition 1)		Prevalence minus attempts (definition 2)		Prevalence minus attempts (definition 3)		
Most recent ID theft	Number	Percent	Number	Percent	Number	Percent	Number	Percent	
Any	25,952,409	10.18	25,637,514	10.06	24,413,614	9.58	20,495,285	8.04	*
Existing credit card account	11,077,632	4.35	10,979,806	4.31	10,533,100	4.13	8,840,147	3.47	*
Existing bank account	9,828,567	3.86	9,732,318	3.82	9,280,199	3.64	7,462,653	2.93	*
Other existing account	1,272,948	0.50	1,232,193	0.48	1,098,327	0.43	690,497	0.27	*
New account	873,366	0.34	831,618	0.33	760,931	0.30	760,931	0.30	
Personal information	838,602	0.33	815,053	0.32	785,452	0.31	785,452	0.31	
Multiple types	2,061,294	0.81	2,046,526	0.80	1,955,605	0.77	1,955,605	0.77	

Note: Victims who experienced an attempt during their most recent incident, but experienced other incidents of identity theft during the reference period are not subtracted from the prevalence rate.

*New prevalence rate was significantly different from original prevalence rate at 95% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2014 and 2016.

Based on data from both 2014 and 2016, removing attempts based on definitions 1 and 2 would not have a statistically significant impact on the prevalence rates for any of the types of identity theft. The removal of attempts based on the attempt 3 definition would significantly reduce the prevalence of identity theft. However, based on findings from table 2, it appears likely that attempt 2 is a more accurate reflection of attempts captured in the survey than attempt 3.

Though not statistically significant, the removal of attempts based on any of the three definitions appears to have a larger impact on the prevalence of existing account misuse than on the misuse of personal information to open a new account or for other fraudulent purposes.

Recommendations: Based on the likelihood that attempts are underestimated in the NCVS and the current inability to confidently separate attempts from completed incidents, which may result in an underestimation of the harms associated with completed identity theft, we suggest one of the following options for improving measurement.

1. *Exclude attempts completely*.
    - Change the language of the screener questions to remove the phrase ‘attempted to use.’ The questions would then read, for example, “Has someone, without your permission, made charges on or deducted money from your existing checking or savings account, including any debit or ATM cards?
    - In addition, for those who respond affirmatively to any of the three screener questions about existing account misuse, add a question after the screener to ask ‘at any point was someone successful in making charges on your account, regardless of whether you were reimbursed.’ If the respondent says ‘no’ he or she would be treated the same way as a respondent who said ‘no’ to the initial screener. In other words, if he or she does not report any other types of identity theft, they would be treated as a nonvictim, with the survey ending after the screener. If the respondent says ‘yes,’ when he or she is prompted to think about the most recent incident, there would also be an instruction to exclude any incidents in which the offender was not successful in obtaining money, goods, or services.

2. *Ask respondents to provide detailed information about successful incidents only.*
    - Screener questions remain the same as they are currently, with respondents asked to think about both the use and attempted use of personal information.
    - For those who respond affirmatively to any of the three screener questions about existing account misuse, add a question after the screener to ask ‘at any point was someone successful in making charges on your account, regardless of whether you were reimbursed.’ If the respondent says ‘no’ he or she would be treated the same way as a respondent who said ‘no’ to the initial screener. In other words, if he or she does not report any other types of identity theft, they would be treated as a nonvictim, with the survey ending after the screener. If the respondent says ‘yes,’ when he or she is prompted to think about the most recent incident, there would also be an instruction to exclude any incidents in which the offender was not successful in obtaining money, goods, or services.

Given BJS’s interest in maintaining high-level trends over time, we recommend approach number 2. Under this approach, respondents would be screened in as victims if they experienced existing account misuse AND said that the offender had successfully made charges on their account OR if they answered affirmatively to the screener questions about the misuse of personal information to open a new account or for other fraudulent purposes. This approach would allow BJS to maintain continuity in terms of reporting overall prevalence rates by type of identity theft. It would also allow BJS the flexibility to exclude attempted incidents of existing account misuse, the type of identity theft for which attempts are easiest to identify and most commonly reported. Finally, it would create more consistency in the types of incidents that are described when respondents report on the nature of and harms associated with the most recent incident. The drawback to this approach is that about 1% of victims who would have previously answered questions about their most recent incident, would be skipped out of these questions.[6] This might impact BJS’ ability to compare trends over time in the nature of and victim

[6] The 1% estimate is based on the reduction in cases when attempt definition 2 was used.

responses to identity and would slightly limit the sample sizes available for analysis of the characteristics of the most recent incident. For context, in 2018, there were 10,068 unweighted persons who experienced identity theft. Losing about 1% would still leave a sample size of just under 10,000.

Cognitive testing would be needed to ensure that respondents are consistently interpreting and correctly understanding the screener follow-up questions and the language used to focus respondents on the most recent completed incident.

Time in Sample

In a panel design survey like the NCVS, respondent fatigue can impact survey estimates and data quality.[7] Fatigue may result in sample members not participating in later interview waves, thus creating the potential for a biased sample. Fatigue could also cause respondents to break off prior to the administration of the supplement if they have already spent considerable time on the core NCVS.

BJS is interested in understanding whether ITS response rates and prevalence rates are impacted by how many NCVS interviews the respondent has participated in. For the purpose of understanding the potential impact of respondent fatigue, this analysis is focused on person time-in-sample (TIS) (1-7) and person interview number (1-7), rather than household or address TIS. Table 10 examines 2018 ITS response and prevalence rates, dividing up respondents by whether they reported an incident in the core NCVS.

Among eligible ITS respondents - those age 16 or older who completed the NCVS interview themselves (non-proxy) – there was not much variation in response rates by TIS or interview number. Regardless of whether an NCVS incident was reported, the vast majority of eligible respondents who completed the core survey, also completed the supplement. Across TIS, for instance, the overall response rates ranged from 91% among those in TIS 3 to 94% among those in TIS 6 and TIS 7.

Prevalence rates in the ITS were significantly higher among respondents who had reported an NCVS incident (17.3%) compared to those who had not (8.9%). With the exception of respondents in TIS 7, this was true across all TIS groups.

Among respondents who did not report an NCVS victimization, identity theft prevalence rates were significantly higher for persons in TIS 1 compared to persons in TIS 2-7. However, this pattern did not hold true among persons who had reported an NCVS victimization. Research suggests that social desirability concerns may lead respondents to want to provide useful responses to surveys, which can result in telescoping. These findings may suggest that in TIS 1 respondents are more likely to engage in forward telescoping in the ITS if they did not have anything to report in the core survey. In later interview waves, these social desirability concerns are no longer present because they have participated in the core survey multiple times.

Table 11 shows 2018 prevalence rates by most recent type identity theft and TIS. Rates of existing bank account misuse were higher in TIS 1 than TIS 2-7 and rates of persons experiencing multiple types of identity theft during the same incident were higher in TIS 1 than TIS 3-7. Otherwise there were no clear patterns in prevalence rates by TIS.

[7] Additional information about the NCVS panel design is available in the survey's technical documentation: https://www.bjs.gov/content/pub/pdf/ncvstd16.pdf.

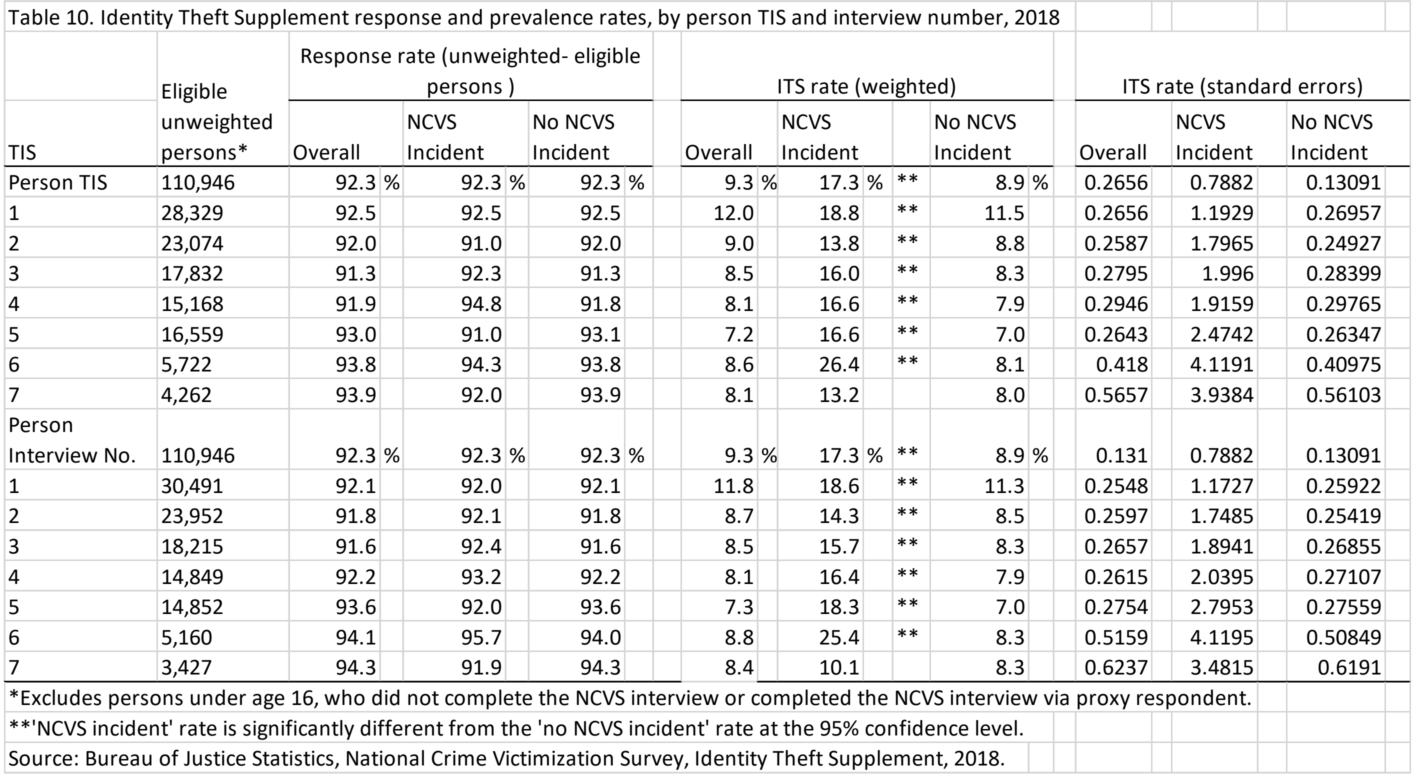


Table 10. Identity Theft Supplement response and prevalence rates, by person TIS and interview number, 2018

	Eligible	Response rate (unweighted- eligible persons)			ITS rate (weighted)				ITS rate (standard errors)		
TIS	unweighted persons*	Overall	NCVS Incident	No NCVS Incident	Overall	NCVS Incident		No NCVS Incident	Overall	NCVS Incident	No NCVS Incident
Person TIS	110,946	92.3 %	92.3 %	92.3 %	9.3 %	17.3 %	**	8.9 %	0.2656	0.7882	0.13091
1	28,329	92.5	92.5	92.5	12.0	18.8	**	11.5	0.2656	1.1929	0.26957
2	23,074	92.0	91.0	92.0	9.0	13.8	**	8.8	0.2587	1.7965	0.24927
3	17,832	91.3	92.3	91.3	8.5	16.0	**	8.3	0.2795	1.996	0.28399
4	15,168	91.9	94.8	91.8	8.1	16.6	**	7.9	0.2946	1.9159	0.29765
5	16,559	93.0	91.0	93.1	7.2	16.6	**	7.0	0.2643	2.4742	0.26347
6	5,722	93.8	94.3	93.8	8.6	26.4	**	8.1	0.418	4.1191	0.40975
7	4,262	93.9	92.0	93.9	8.1	13.2		8.0	0.5657	3.9384	0.56103
Person Interview No.	110,946	92.3 %	92.3 %	92.3 %	9.3 %	17.3 %	**	8.9 %	0.131	0.7882	0.13091
1	30,491	92.1	92.0	92.1	11.8	18.6	**	11.3	0.2548	1.1727	0.25922
2	23,952	91.8	92.1	91.8	8.7	14.3	**	8.5	0.2597	1.7485	0.25419
3	18,215	91.6	92.4	91.6	8.5	15.7	**	8.3	0.2657	1.8941	0.26855
4	14,849	92.2	93.2	92.2	8.1	16.4	**	7.9	0.2615	2.0395	0.27107
5	14,852	93.6	92.0	93.6	7.3	18.3	**	7.0	0.2754	2.7953	0.27559
6	5,160	94.1	95.7	94.0	8.8	25.4	**	8.3	0.5159	4.1195	0.50849
7	3,427	94.3	91.9	94.3	8.4	10.1		8.3	0.6237	3.4815	0.6191

*Excludes persons under age 16, who did not complete the NCVS interview or completed the NCVS interview via proxy respondent.

**'NCVS incident' rate is significantly different from the 'no NCVS incident' rate at the 95% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

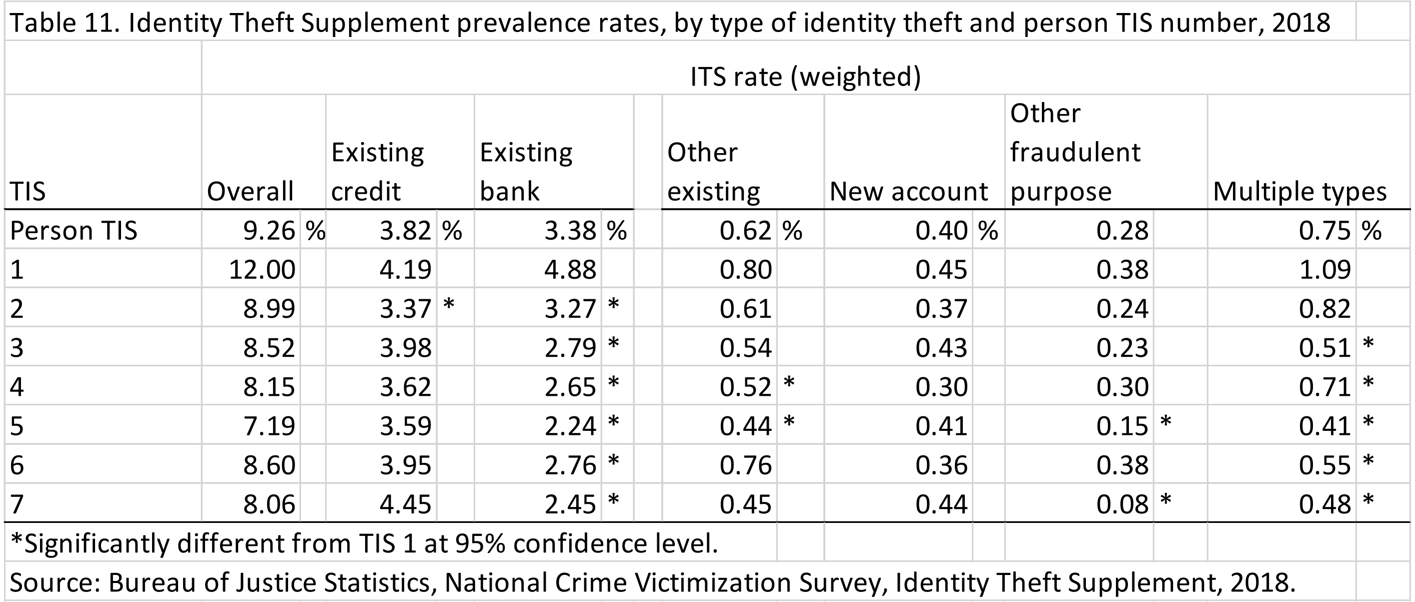


Table 11. Identity Theft Supplement prevalence rates, by type of identity theft and person TIS number, 2018

	ITS rate (weighted)						
TIS	Overall	Existing credit	Existing bank	Other existing	New account	Other fraudulent purpose	Multiple types
Person TIS	9.26 %	3.82 %	3.38 %	0.62 %	0.40 %	0.28	0.75 %
1	12.00	4.19	4.88	0.80	0.45	0.38	1.09
2	8.99	3.37 *	3.27 *	0.61	0.37	0.24	0.82
3	8.52	3.98	2.79 *	0.54	0.43	0.23	0.51 *
4	8.15	3.62	2.65 *	0.52 *	0.30	0.30	0.71 *
5	7.19	3.59	2.24 *	0.44 *	0.41	0.15 *	0.41 *
6	8.60	3.95	2.76 *	0.76	0.36	0.38	0.55 *
7	8.06	4.45	2.45 *	0.45	0.44	0.08 *	0.48 *

*Significantly different from TIS 1 at 95% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

Next steps

If BJS agrees with the findings and resulting recommendations provided in this document, the next step is for RTI to develop several versions of a revised instrument screener and a testing plan Following BJS review of the drafts, we propose to conduct approximately 30 in-person interviews with respondents who experienced each of the three major types of identity theft (existing account misuse, use of personal information to open a new account, and use of personal information for other purposes). Once changes to the instrument have been agreed upon, we propose 2 online tests to compare the ability of the different versions of the instrument to control telescoping and to assess the impact of changing the ordering of the screener on the types of incidents reported. Using an online platform would enable responses to be collected from thousands of victims in a relatively short period of time and would ensure sufficient sample sizes for a robust comparison of the impact of the changes on prevalence rates. Additional details on the testing plan are included in the supplementary document titled ITS testing plan.

References

Gfroerer, J. 2018. War stories from the drug survey: How culture, politics, and statistics shared the National Survey on Drug Use and Health. Cambridge, MA: Cambridge University Press.

Johnson, E.O. and Schultz, L. 2005. Forward telescoping bias in reported age of onset: An example from cigarette smoking. International Journal of Methods in Psychiatric Research, 14(3): 119-129.

Johnson, R.A., Gerstein, D.R., Rasiniski, K.A. 1997. Recall decay and telescoping in self-reports of alcohol and marijuana use: Results from the National Household Survey on Drug Abuse (NHSDA). In *Proceedings of the 1997 Joint Statistical Meetings, 52nd annual conference of the American Association for Public Opinion Research*, Norfolk, VA (pp. 964-969). Alexandria, VA: American Statistical Association.

Loftus, E.F., Klinger, M.R., Smith, K.D., and Fiedler, J. 1990. A tale of two questions: Benefits of asking more than one question. *Public Opinion Quarterly* 54: 330-345.

Prohaska, V., Brown, N.R. and Belli, R.F. 1998. Forward Telescoping: The Question Matters. *Memory* 6(4): 455-465.

Sudman, S., Finn, A., and Lannom, L. 1984. The use of bounded recall procedures in single interviews. The Public Opinion Quarterly 48(2): 520-524.

Cognitive Interviewing for the National Crime Victimization Survey (NCVS) Identity Theft Supplement (ITS)

Prepared by RTI International

June 5, 2020

Sarah Cook, Jeanne Snodgrass, Lynn Langton

INTRODUCTION

This report provides a summary of RTI findings from 27 adult cognitive interviews on the redesigned version of the BJS Identity Theft Supplement (ITS) screener. Interviews took place virtually via Zoom with participants in the Eastern, Central and Pacific time zones in May and early June 2020. Cognitive interviews were conducted virtually due to the COVID-19 pandemic. These preliminary findings may be of use to BJS when incorporating the next round of changes to the NCVS ITS instrument.

RECRUITMENT

All recruitment was done through Amazon's Mechanical Turk (MTurk). MTurk is an online crowdsourcing platform where workers can complete nominal tasks for small payments. For our purposes, we posted a MTurk task (known as a "HIT") for participants to complete an online screener survey to participate in a virtual interview.

Once participants completed the online web screener, our recruiter contacted those who were eligible for the study via email to schedule interviews. Eligibility was based on our need for demographic diversity as well as type of identity theft experienced. An informed consent form was sent via email to the participant for them to review. At the beginning of each virtual interview, the interviewer verified that the respondent had received the informed consent form, asked if they had questions, and received verbal consent to conduct the interview and be recorded.

Table 1 shows the cumulative demographics of participants. Though already a diverse group of participants, some diversity was lost to participants who changed their mind or did not attend their interview. **Table 2** shows this same information distributed by participants and includes the type of identity theft as indicated in the online screener and as reported during the actual interview. The online screener was a condensed version of the revised ITS screener that included four questions about identity theft experiences:

Table 1. Participant Demographics

Time Zone	
EDT	13
CDT	8
MDT	0
PDT	6
Age Range	
18-25	2
26-34	13
35-49	9
50 or older	3
Education	
High school/GED	2
Some college	4
College grad	16
Post-grad degree	8
Gender	
Male	20
Female	7
Race	
White	20
Black/African American	4
Asian	5
American Indian/Alaska Native	2
Native Hawaiian/Pacific Islander	0
Hispanic	
Yes	1

1. During the past 12 months, that is, since [AUTOFILL DATE A YEAR AGO FROM SURVEY DATE], has someone, without your permission used your existing checking account, savings account, or credit card account?
2. During the past 12 months, has someone misused another type of existing account such as your telephone, cable, gas or electric accounts, online payment account like Paypal, insurance policies, entertainment account like ITunes, or something else?
3. During the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today, has someone, without your permission, used your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else?
4. During the past 12 months, has someone used your personal information for some other fraudulent purpose, such as filing a fraudulent tax return, getting medical care, applying for a job or government benefits; giving your information to the police when they were charged with a crime or traffic violation, or something else?

Endorsement of these questions is represented in the table below consecutively as: *Existing (bank), Existing (other), New account, and Personal info*. Three of the recruited 'non-victims' of identity theft ended up as 'victims' once the participants heard the full survey questions and self-reported their experience, and three of our recruited 'victims' ended up as nonvictims during the interview.

Table 2. Participant Demographic, Recruitment, and Final Identity Theft Type Data (n=27)

P#	Time Zone	Age Range	Education	Gender	Race	Recruited IT Type	Final IT Type
1	EDT	35-49	Post-Graduate degree	Female	White	None	None
2	PDT	26-34	College Graduate	Male	Asian	Existing (bank); Existing (other)	Existing (bank)
3	CDT	26-34	Post-Graduate degree	Female	White	Existing (bank)	Existing (bank)
4	CDT	26-34	High School Graduate/GED	Female	Black and AI/AN	Existing (bank); Existing (other); New account	Existing (bank)
5	PDT	35-49	College Graduate	Male	White	Existing (bank); Existing (other); Personal info	New account; Personal info
6	PDT	18-25	College Graduate	Male	Black	None	Existing (bank); Existing (other); Personal info
7	EDT	26-34	College Graduate	Male	Asian	All	None
8	EDT	35-49	Some College	Male	White	Existing (bank); Existing (other)	Existing (other)
10	CDT	35-49	College Graduate	Male	White	Existing (bank)	Existing (bank); New account
11	PDT	26-34	College Graduate	Male	White	Existing (bank); New account	Existing (bank); New account
12	PDT	26-34	College Graduate	Male	Black	All	Existing (bank); Existing (other); New account
13	EDT	35-49	Post-Graduate degree	Male	Asian	Existing (bank); Existing (other); New account	Existing (bank)
15	EDT	26-34	Post-Graduate degree	Male	Asian	None	Existing (other)
16	EDT	50 or older	Post-Graduate degree	Male	White	None	Existing (bank)

Table 2. Participant Demographic, Recruitment, and Final Identity Theft Type Data (n=27)

P#	Time Zone	Age Range	Education	Gender	Race	Recruited IT Type	Final IT Type
17	EDT	26-34	Post-Graduate degree	Female	Asian and AI/AN	Existing (bank); Existing (other)	Existing (bank)
18	EDT	50 or older	Some College	Female	White	Existing (bank)	None
19	CDT	26-34	College Graduate	Male	Asian	Existing (bank); Existing (other)	Existing (bank);
20	PDT	50 or older	College Graduate	Female	White	Existing (bank); Personal info	Existing (bank);
22	CDT	35-49	Post-Graduate degree	Female	White	Existing (bank)	Existing (bank)
23	CDT	26-34	College Graduate	Male	White	Existing (bank); Existing (other)	Existing (bank)
24	EDT	35-49	Some College	Male	White	Existing (other)	Existing (other)
26	EDT	35-49	College Graduate	Male	White	Existing (other)	Existing (bank); Existing (other)
27	CDT	26-34	College Graduate	Male	White	Existing (bank)	Existing (bank); Existing (other)
30	CDT	26-34	College Graduate	Male	White	Existing (bank)	None

31	EDT	26-34	College Graduate	Female	White	Existing (other)	Existing (bank);
							Existing (other);
							Personal Info

32	EDT	35-49	College Graduate	Female	Black	Existing (bank)	Existing (bank)
34	EDT	18-25	College Graduate	Male	White	Existing (other)	Existing (other)

METHODS

Once MTurk respondents completed the online screener, were determined to be eligible to participate in the cognitive interview, and expressed interest in participating in a virtual interview, the RTI recruiter scheduled an interview time with the participant. The recruiter then sent the participant a link to a private Zoom meeting set up for their specific interview. RTI interviewers were trained to stop the interview if anyone else joined the meeting. In many cases, the “waiting room” feature was turned on so no one could join the meeting without being allowed in by the interviewer.

Prior to conducting any interviews, all interviewers completed training on the cognitive interview protocol and project logistics. All interviews were conducted using a cognitive interview protocol that was based on the most recent version of the supplement provided by BJS. The protocol included probes developed to elicit an understanding of how respondents interpreted specific terms or questions. Along with the pre-determined probes, interviewers were encouraged to use spontaneous probing when needed to further understand the participant’s thinking. The interview protocol is included in **Appendix A**.

Prior to the start of the interview, the interviewer obtained verbal participant consent. After the interview, participants were emailed an Amazon.com Gift Card code with a value of $40 to help cover data and technology costs associated with participating in the interview.

FINDINGS AND RECOMMENDATIONS

This section summarizes key findings and recommended changes to specific survey items for which any problems or issues were identified. Overall, the survey performed very well. There are many questions where none of the 27 participants had difficulty understanding and answering them as intended. These items not discussed below did not appear to be problematic and have no recommended changes.

Q2 – Has anyone EVER, without your permission, used your checking or savings account, including any debit or ATM cards, to make a purchase or withdraw money? Please consider only times when money was actually deducted from your account, regardless of whether you were reimbursed later.

1 Yes
2 No (Skip to Q5)

Although all respondents were able to answer this question in relation to bank accounts only, a few mentioned that they also thought about their credit card accounts in this question, not knowing that we were going to ask about credit card accounts separately. Three respondents had credit cards through their bank, which made it more difficult to separate the two. One participant answered "Yes" to this question and, through probing, shared that the theft actually happened in their Google Pay account, which is connected to their bank account. They later said that the incident should be counted in Q9, not Q2, after hearing the response options provided. If they had known there would be an option to report identity theft of an account like Google Pay, they never would have answered "Yes" to Q2.

Recommendation: Suggest changing the last sentence to "**Please consider only times when money was actually deducted from your checking or savings account, regardless of whether you were reimbursed later."** or adding **"Please do not include times when anyone used your credit card or online pay accounts without permission."** Alternatively, to be consistent with Q6**,** start the question with **"Thinking only of checking and savings accounts,".** It may still be helpful to conclude with **"Please do not include times when anyone used your credit card or online pay accounts without permission."**

Q5 – *Now I'd like to ask you about the possible misuse of EXISTING CREDIT CARDS OR CREDIT CARD ACCOUNTS.*

Have you ever had a credit card in your name? Include major credit cards such as a Mastercard or Visa, and store credit cards such as a Macy's card. Please do not include debit cards.

1 Yes
2 No (Skip to Q9)

Most respondents suggested including American Express and Discover as examples of major credit cards, and "big box" retailer cards such as Target, Walmart and Amazon as examples of store cards. However, the current examples still provided enough information for participants to know what they should be thinking about. One person suggested saying "retail" instead of "store" credit cards because you can have credit cards for things that do not have physical stores (such as Amazon).

Recommendation: Consider replacing "Macy's" with "Target or Amazon" and changing "store credit cards" to "retail credit cards" to encompass more possibilities.

Q6 – *Thinking only of credit cards, has anyone EVER used one or more of your credit cards without your permission? Please consider only times when charges actually posted to your account, regardless of whether you were reimbursed later.*

1 Yes
2 No (Skip to Q9)

One respondent mentioned he would answer this question as ‘No’ because he interprets this question to be about the misuse of physical credit cards only. If the question were more specific about including the misuse of credit card numbers as well, he would answer this question as “Yes”.

Recommendation: Consider adding “accounts” after the second mention of ‘credit card’ in the question text.

Q9 – *Now I’d like to ask you about the possible misuse of any of your EXISTIING ACCOUNTS other than credit card or bank accounts.*

Has anyone EVER, without your permission used another of your accounts, such as your telephone, internet or utilities accounts, online payment accounts like Paypal, medical insurance accounts, entertainment accounts, such as for music or games, email or social media accounts, or some other accounts? Please include only times when charges were actually made on the account, regardless of whether you were reimbursed later.

1 Yes
2 No (Skip to Q13)

Respondents overwhelmingly said listing the types of accounts was very helpful in helping them to think about the types of accounts we are asking about, but mentioned that they focused in on specific service provider names and then forgot things said after that. Keeping the proper names at the end of the list might help with that. Another person mentioned that we should add “movies” so they would think of streaming accounts. Some participants mentioned thinking about failed log-in attempts they were alerted to on their accounts, but they all knew not to include those. (INTERVIEWER NOTE: We noticed movies are included below in Q11e.)

We have had several respondents who had their Facebook or Instagram accounts taken over, but because the language at the end of the question focuses on charges made to the account, they were not sure whether to actually include them. Two respondents said they did not include times their accounts were compromised for that very reason. It is possible to misuse entertainment, email, and social media accounts without any financial transaction. In the case of entertainment accounts, the theft is the service they are using and not paying for, not a financial theft. Using another person’s social media accounts is often used for phishing, in which case the infiltration is a means to an end. Email accounts, however, carry more weight because passwords can be sent or reset to an email account. Theft of an email account has many more implications than that of entertainment or social media.

Recommendation: Move ‘online payment accounts’ to the end of the list and include Venmo with the Paypal example. Revise example of entertainment accounts to, “entertainment accounts, such as for music, games, or movies” so participants consider popular streaming services.

Consider the appropriate placement for accessing social media accounts. Does the misuse of email and social media account fit better under the category of ‘misuse of personal information for other fraudulent purposes?’ or should they be in their own either combined or separate categories?

If the intent of the question is to capture account access regardless of financial loss, replace the last sentence with “Please include only times when someone actually got into your account. Do not include failed login attempts”.

Q11 – ***Which of the following types of your EXISTING accounts, other than credit card or bank accounts, did someone run up charges on, take money from, or otherwise misuse? Did they misuse one or more of your….***

11a. Telephone or internet accounts? ***YES NO***

11b. Utilities accounts, such as cable, gas or electric accounts? ***YES NO***

11c. Online payment accounts, such as Paypal? ***YES NO***

11d. Medical insurance accounts? ***YES NO***

11e. Entertainment accounts, such as for movies, music, or games? ***YES NO***

11f. Email or social media accounts? ***YES NO***

11g. Some other type of accounts? ***YES NO***

[If yes] What other type of accounts were misused? __________

(If any 11a-11g = yes, ask Q12a; else skip to Q13)

Recommendation: To remain consistent with Q10, move "Online payment accounts", such as Paypal to the end of the list above "other" and include Venmo as an example.

____

Q13 – ***Next, I have some questions about any NEW ACCOUNTS someone might have opened using your personal information.***

Has anyone EVER, without your permission, used your personal information to successfully open any NEW accounts, such as telephone or internet accounts, credit card or bank accounts, loans or mortgages, insurance accounts, online payment accounts, entertainment accounts, such as for music or games, email or social media accounts, utilities accounts or some other type of account?

1 Yes
2 No (skip to Q17)

A few participants said "No" to this question because they assumed it required a financial loss, even though the question does not specify monetary loss. This is due to priming effects from all of the previous questions referring to losing money.

Recommendation: Consider adding, "Include times even when you did not lose any money." Revise the example of entertainment accounts to, "entertainment accounts, such as for music, games, or movies" so participants consider streaming services and to be consistent with Question 9.

____

Q17 - Next, I have some questions about any other misuses of your personal information.

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; giving your information to the police when they were charged with a crime or traffic violation; applying for government benefits or something else? Please consider only times when your information was actually used, even if the situation was later resolved.

1 Yes
2 No (LOOK AT ANSWER SHEET TO FIND NEXT QUESTION)

Some may find the word 'actually' from the final sentence as confusing. As one participant said "If you use it, you actually use it. How do you not actually use it?"

Recommendation: Only one participant had concerns with this question and since "actually" is an adverb that is often used to emphasize something in fact happening, we recommend leaving the questions as written.

____

Q25 – *Thinking about the most recent time your personal information was misused, in what month and year did you first discover that someone had misused your personal information? This may be the same month and year as the most recent occurrence, or the discovery may have happened before or after the most recent occurrence.*

Enter month: __________ Month (01-12)
Enter year: __________ Year (1955-2021)

Some participants found the last sentence to be confusing, especially remarking on not understanding how discovery 'before' an occurrence happened. One participants was particularly confused and apologized multiple times. When the interviewer read them the question without the second sentence, they said that question was clear and had not realized it was the same question.

Recommendation: Remove the last sentence to avoid unnecessary confusion. Alternatively, it could be left in if it is made clear to only be read if a respondent is having difficulty answering the question. Consider simplifying it to "You could have first discovered the incident before, during, or after the month and year of the most recent occurrence."

____

Q26 - *How long had your personal information been misused before you discovered it?*

1. One day or less (1-24 hours)
2. More than a day, but less than a week (25 hours-6 days)
3. At least a week, but less than one month (7-30 days)
4. One month to less than three months
5. Three months to less than six months
6. Six months to less than one year
7. One year or more
8. Don't know

Most participants reported learning about the identity theft within days or weeks of the first (known) occurrence. A respondent did point out that since this question is in relation to the past 12 months, we might not need response option 7. However, due to the possibility of reoccurring incidents of identity theft, we see this response option as necessary.

Recommendation: Leave question as is.

General Findings

There are questions in this instrument about timelines that could be confusing for some or hard to follow. The two sets of questions we focused on were questions about whether an incident occurred “Ever” or “in the past 12 months, and Q25 and Q26 when we try to identify the date of discovery and length of misuse (compared to the date of the most recent incident). For the questions on whether someone had ever experienced identity theft, respondents were probed on how far back they were thinking when answering those questions. Two respondents mentioned ‘lifetime’ or ’30 years, since I had my account,’ but the majority of respondents reported remembering back to when their most recent incident or incidents occurred, whether that was 3 months ago or 5 years ago. This makes sense though because once they recalled an event, they had their answer and did not need to think further. **Table 3** provides the responses for each type of identity theft and whether it “Ever” happened and whether it happened “in the past 12 months.” Many participants recognized that they had been victimized in the past, but that in many cases their incidents occurred outside of the 12-month time frame.

Table 3. Responses to “Ever” and “12 months” Questions

P#	**Ever -** Existing bank	**12 mos -** Existing bank	**Ever -** Existing credit card	**12 mos -** Existing credit card	**Ever -** Existing other	**12 mos -** Existing other	**Ever -** New account	**12 mos -** New accout	**Ever -** Personal info	**12 mos -** Personal info
1	No		No		No		No		No	
2	Yes	Yes	Yes	No	No		No		No	
3	No		Yes	Yes	No		No		No	
4	No		Yes	Yes	No		No		No	
5	Yes	No	No		No		Yes	Yes	Yes	Yes
6	No		Yes	Yes	Yes	Yes	No		Yes	Yes
7	No		No		No		No		No	
8	Yes	No	No		No		No		No	
10	No		Yes	Yes	No		Yes	Yes	No	
11	No		Yes	No	No		Yes	Yes	No	
12	Yes	Yes	Yes	No	Yes	No	Yes	No	No	
13	Yes	Yes	Yes	Yes	Yes	No	No		No	
15	No		No		Yes	No	No		No	
16	Yes	No	Yes	No	No		No		No	
17	No		Yes	Yes	No		No		No	
18	No		No		No		No		No	
19	Yes	Yes.	Yes	No	No		No		No	

P#	Ever - Existing bank	12 mos - Existing bank	Ever - Existing credit card	12 mos - Existing credit card	Ever - Existing other	12 mos - Existing other	Ever - New account	12 mos - New accout	Ever - Personal info	12 mos - Personal info
20	Yes	Yes	No		No		No		No	
22	Yes	Yes	Yes	Yes	No		No		No	
23	Yes	No	Yes	No	No		No		No	
24	No		No		Yes	Yes	No		No	
26	No		No		Yes	Yes	No		No	
27	No		Yes	Yes	Yes	Yes	No		No	
30	No		No		No		No		No	
31	Yes	No	Yes	No	Yes	Yes	No		Yes	Yes
32	Yes	Yes	No		No		No		No	
34	No		No		Yes	Yes	No		No	

Another concern is whether respondents were able to distinguish among the concepts of when the incident started, was discovered, and most recently occurred an whether they were able to provide dates for each of those reference points. Respondents were asked to describe in their own words what these different reference points meant in light of their own experience and all appeared to understand the concepts. With the exception of one respondent, all of the participants were able to stop the identity theft relatively quickly after they discovered it.

Table 4. Key Dates in Incident Timeline

P#	Most Recent	Discovered (Q25)	Length of use (Q26)
2	February 2020	February 2020	1 day-1 week
3	August 2019	August 2019	<1 day
4	October 2019	October 2019	<1 day
5	July 2019	July 2019	1-3 months
6	February 2020	January 2020	1-3 months
10	September 2019	September 2019	1 day-1 week
11	July 2019	July 2019	<1 day
12	June 2019	June 2019	<1 day
13	November 2019	December 2019	1 day-1 week
17	September 2019	September 2019	1 week–1 month
19	November 2019	November 2019	1 week–1 month
20	March 2020	March 2020	1 day-1 week
22	February 2020	February 2020	<1 day
24	March 2020	March 2020	<1 day
26	October 2019	October 2019	<1 day
27	January 2020	January 2020	<1 day
31	March 2020	March 2020	1 day-1 week
32	August 2019	August 2019	1 week–1 month
34	March 2020	March 2020	<1 day

September 15, 2020

National Victimization Statistical Support Program (NVSSP-2) Cooperative Agreement (COA) 2011-NV-CX-K068

Identity Theft Screener Online Testing

Final Report

Prepared for

Bureau of Justice Statistics
810 7th Street Northwest
Washington, DC 20001

Prepared by

RTI International
3040 E. Cornwallis Road
Research Triangle Park, NC 27709

RTI Project Number 0216100.000.001.015

RTI Project Number
0216100.000.001.015

National Victimization Statistical Support Program (NVSSP-2) Cooperative Agreement (COA) 2011-NV-CX-K068

Identity Theft Screener Online Testing

Final Report

September 2020

Prepared for

Bureau of Justice Statistics
810 7th Street Northwest
Washington, DC 20001

Prepared by

RTI International
3040 E. Cornwallis Road
Research Triangle Park, NC 27709

Contents

Section **Page**

Executive Summary 1

1. Introduction 1

1.1 Background 1

1.2 The Need for Online Testing 3

1.3 Online Testing Approach 4

1.4 Data Collection 5

1.5 Strengths and Limitations of the Use of Online Panels for Testing the ITS Screeners 8

2. Key Findings 10

2.1 Comparison of 12-month Prevalence Estimates Across Versions 1, 2, and 3 10

2.2 Use of the Dual Reference Period and Patterns Across Demographic Groups 13

2.3 Impact of Exclusion of Attempts on Prevalence Estimates 18

2.4 Respondents' Ability to Date Incidents and the Impact of Dating on Telescoping 19

2.5 Comparison to the ITS Estimates 25

3. Recommendations for the 2021 ITS Based on Key Findings 27

4. Methodology 29

4.1 Sampling 29

4.1.1 AmeriSpeak 29

4.1.2 MTurk 29

4.2 Fielding 30

4.2.1 AmeriSpeak 30

4.2.2 MTurk 31

4.2.3 Tables Presenting Sample Sizes by Mode and Platform 32

4.3 Statistical Weighting 34

4.4 Weighting 36

4.4.1 AmeriSpeak Sample 37

4.4.2 TrueNorth Calibration for Nonprobability Sample 37
4.4.3 Design Effect and Sampling Margin of Error Calculations 38
4.5 Assessment of Item Nonresponse, Speeders, and Skippers 38
4.6 Feedback from MTurk Workers.. 42

5. References 44

Appendices

A. Three Versions of ITS Screener Used in Testing A-1
B. Findings from ITS Version 2 Cognitive Testing B-1
C. Standard Error Tables..C-1

Figures

Number **Page**

1. Relationship Between Date of Most Recent Occurrence and Date of Discovery of Identity Theft (Version 2) 22

Tables

Number **Page**

1. Unweighted Sample, by Demographic Characteristics and Mode 6
2. Unweighted Sample, by Demographic Characteristics and Platform 7
3. Weighted Sample, by Demographic Characteristics and Instrument Version............8
4. Prevalence of Identity Theft in Past 12 Months, by Type of Identity Theft and Instrument Version.. 11
5. Persons Aged 18 or Older Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics and Instrument Version 11
6. Most Recent Incident of Identity Theft, by Type of Identity Theft and Instrument Version.. 13
7. Prevalence of Identity Theft, by Type of Identity Theft, Instrument Version, and Reference Period 14
8. Persons Ages 18 or Older Who Experienced One or More Incidents of Identity Theft, by Victim Characteristics, Instrument Version, and Reference Period 15
9. Relationship Between Lifetime Prevalence and 12-month Prevalence, by Type of Identity Theft (Version 2) 16
10. Relationship Between Lifetime Prevalence and 12-month Prevalence of Identity Theft, by Victim Characteristics (Version 2) 17
11. Prevalence of Identity Theft During the Past 12 Months, by Type of Identity Theft and Instrument Version and With Exclusion of Attempts 18
12. Percentage of Victims Providing a Date of Occurrence Prior to or Outside the 12-month Reference Period or Providing a "Don't Know" Response, by Type of Identity Theft (Version 2)... 20
13. Percentage of Victims Providing a Date of Occurrence Prior to or Outside the 12-Month Reference Period or Providing a "Don't Know" Response, by Victim Characteristics and Select Types of Identity Theft (Version 2)............................. 21
14. Relationship Between Date of Most Recent Occurrence and Date of Discovery, by Type of Identity Theft... 22
15. Relationship Between Date of Most Recent Occurrence and Date of Discovery, by Victim Characteristics 23
16. Time From Discovery of Most Recent Incident to Interview, by Questionnaire Version and Type of Identity Theft... 24
17. Relationship Between Time of Most Recent Occurrence and How Long Identity Theft Had Been Happening When It Was Discovered.. 24
18. Prevalence of Identity Theft in Past 12 Months, by Type of Identity Theft, Survey Administrator, and Mode 26
19. Persons Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics, Survey Administrator, and Mode 26

20. Prevalence of Identity Theft in Past 12 Months Accounting for Version 2 Victims Who Failed to Provide Dates of Occurrence or Provided Dates of Occurrence Outside the Reference Period, by Type of Identity Theft and Instrument Version 27

21. Average and Median Number of Minutes Spent on the Survey, by Platform, Survey Mode, and Instrument Version (unweighted) 28

22. Detailed Breakdown of the Survey Recruitment HITs 31

23. Unweighted Prevalence of Identity Theft in the Past 12 Months, by Type of Identity Theft and Mode 32

24. Unweighted Prevalence of Identity Theft in the Past 12 Months, by Type of Identity Theft and Platform 32

25. Unweighted Persons Ages 18 or Older Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics and Mode 33

26. Unweighted Persons Age 18 or Older Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics and Platform 34

27. Census Current Population Survey Feb 2020 was Used for Benchmarking 36

28. Instrument Version 1 Item Nonresponse, by Key Items and Survey Platform 39

29. Instrument Version 2 Item Nonresponse, by Key Items and Survey Platform 39

30. Instrument Version 3 Item Nonresponse, by Key Items and Survey Platform 40

31. Instrument Version 1 Item Nonresponse, by Key Items and Mode 40

32. Instrument Version 2 Item Nonresponse, by Key Items and Mode 41

33. Instrument Version 3 Item Nonresponse, by Key Items and Mode 41

34. Average Number of Missing or “Don't Know” Responses, by Respondent Demographics and Instrument Version (unweighted) 42

Executive Summary

From July 16, 2020, to August 4, 2020, RTI International and NORC successfully administered a randomized test of three versions of the Bureau of Justice Statistics (BJS) Identity Theft Supplement (ITS) screener to more than 31,000 respondents. The respondents were recruited through three online survey platforms: AmeriSpeak, a probability-based panel; and Lucid and Mechanical Turk (MTurk), two nonprobability panels. The goal of the test was to determine which of the three versions of the ITS screener produced the most accurate estimates of the prevalence of identity theft with the highest degree of data quality. The current ITS instrument, which is fielded as part of the National Crime Victimization Survey (NCVS), was Version 1. Version 2 was a revised instrument designed to control for telescoping through the use of a dual reference period, upfront dating of the most recent occurrence, and the exclusion of attempted incidents. Version 3 was similar Version 1; however, it excluded attempted incidents.

Comparisons across the three versions revealed that Version 2 resulted in the lowest prevalence of identity theft and appeared to best control for telescoping. Respondents appeared to understand the distinctions in the dating questions and the majority were able to identify the month and year of occurrence. Based on the findings, Version 2 is recommended for the 2021 ITS. However, use of this version would require additional changes to the ITS questionnaire, result in a change to the definition of identity theft, and cause a break-in series for trend analyses.

Across all three versions and all three platforms, there were low levels of item missingness and the response times were within the expected range. The project and findings serve to demonstrate that online testing platforms are an efficient and effective means for collecting data from a large number of respondents, using a consistent approach, in a relatively short period of time. The use of online platforms is a cost-effective and efficient way to quickly obtain a magnitude of responses and is useful for testing how well different versions of survey questions perform in the field.

1. Introduction

1.1 Background

The Bureau of Justice Statistics (BJS) developed the Identity Theft Supplement (ITS) to the National Crime Victimization Survey (NCVS) in 2006 and 2007 in conjunction with the Federal Trade Commission (FTC), National Institute of Justice (NIJ), Bureau of Justice Assistance (BJA), and Office for Victims of Crime (OVC). The survey was designed to fill key data needs for each of the agencies and to respond to a recommendation from the 2007

President's Task Force on Identity Theft[1] that BJS should periodically administer identity theft survey supplements to collect detailed individual-level data on the prevalence and consequences of identity theft.

Since its inception, the survey has been administered five times (in 2008, 2012, 2014, 2016, and 2018) to all NCVS respondents age 16 or older during a 6-month field period following the administration of the core NCVS. It is used to generate estimates of the prevalence and nature of identity theft victimizations nationwide, collecting data on victim experiences with a broad range of identity theft incidents, from the misuse of an existing credit card—which typically results in no or low out-of-pocket losses, takes little time to resolve, and tends to cause low levels of distress—to the misuse of someone's Social Security number, which can result in much greater losses, distress, and time spent resolving related issues. The survey also captures known incidents in which an offender attempts to use a person's identifying information but is unsuccessful at obtaining goods or services. Given the changes in technology and the scope of crimes since the ITS was first introduced (more than a decade ago), BJS was interested in reexamining persistent measurement challenges for the ITS and other NCVS supplements and reevaluating the nature of crimes included in its definition of identity theft. After conducting a series of analyses internally, BJS asked RTI International to conduct a secondary data analysis to examine several key issues in the ITS that impact how identity theft is measured and described in reports and the resulting prevalence estimates, including (1) the unbounded nature of the estimates and the potential for telescoping[2]; (2) the ongoing, episodic nature of many incidents and specific dating of incidents to determine whether they should be included within the survey reference period; and (3) the inclusion of attempted incidents. Findings suggested that BJS should do the following:

- Consider using a dual reference period in the screener to reduce the likelihood of respondents telescoping incidents into the 12-month reference period. With this approach, respondents are first asked about lifetime experiences with identity theft, with a follow-up question asking about their experiences with identity theft in the past 12 months.
- Ask respondents to provide a date of the most recent known occurrence of identity theft to ensure that the incidents reported in the screener occurred within the 12-month survey reference period for the ITS.
- Ask respondents to focus only on successfully completed incidents of identity theft because there are challenges with correctly collecting and identifying attempted incidents, and the grouping of attempted and completed incidents muddles understanding of and appreciation for the severity of completed incidents.

[1] https://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf

[2] Unlike in the core NCVS in which Interviews 2–7 are bounded by the prior interview, the ITS and other NCVS supplements are completely unbounded.

Based on findings from the secondary data analysis, BJS and RTI created two revised versions of the ITS screener (see ***Appendix A***). One revised version (identified as Version 2) incorporates all of the recommended changes, including the use of a dual reference period, dating of the most recent incident following an affirmative screener, and revised language instructing respondents to only include successfully completed incidents of identity theft (i.e., to not include attempted incidents). Version 2 is substantially different from the ITS currently in the field (identified as Version 1) and using it would likely result in estimates that are not comparable to those from prior years. The second revised screener (identified as Version 3) is closer to Version 1 but incorporates language instructing respondents to only include successfully completed incidents of identity theft in their responses to the questions.

Using the Version 2 questionnaire, BJS and RTI conducted cognitive interviews with 27 adults in May of 2020 (see ***Appendix B***). Overall, the respondents found the survey to be straightforward and the questions easy to answer, and their feedback and comments resulted in several recommended revisions and clarifications to the screener items. The biggest change was separating the act of accessing and misusing someone’s social media accounts, which may not result in a direct financial loss, from the misuse of other existing accounts (e.g., utilities accounts) which often result in direct financial loss. In Versions 1 and 3, the misuse of social media accounts continued to be grouped under the category of misuse of other existing accounts rather than be separated as an independent screener question.

1.2 The Need for Online Testing

The cognitive interviews were useful for improving the wording and structure of Version 2. However, the team also wanted to determine whether Version 2 would perform better than Version 1 or Version 3 in terms of reducing telescoping and false positive responses. Several key research questions needed to be addressed to determine which version of the screener should be fielded with the NCVS in 2021, including the following:

- Which version of the screener results in lower prevalence rates suggesting less telescoping of incidents from outside the reference period?
- Are respondents able to date identity theft episodes in terms of when they started, were discovered, and most recently occurred? Do respondents appear to make a distinction between these three episode reference points?
- Does the use of the dual reference period appear to control telescoping in affirmative responses about victimization in the previous 12 months? In other words, are the dates provided for the most recent occurrence more likely to fall within the 12-month reference period?
- Which instrument performs better on data quality measures, such as missing or “don’t know” responses or breakoff rates?

Examining these types of issues required a large sample across which the three versions of the screener could be randomized and administered consistently to quantitatively test for differences in prevalence rates and data quality measures. A power analysis suggested that assuming a base identity theft prevalence of 9% and 70% power, a sample size of 31,500 (divided across the three screener versions) was needed to detect a 1% change in the prevalence of identity theft.

Based on the need to administer the screeners to a large sample in a short period, it was determined that using an online platform—preferably one with a mixed-mode option to collect data from respondents who may not have access to the web—was the best approach for data collection. NORC's AmeriSpeak panel was the only known U.S. panel that would enable the collection of more than 30,000 responses in less than 2 months using both web and telephone survey modes. Thus, RTI entered into a subcontract with NORC to utilize their AmeriSpeak panel and TrueNorth Calibration approach for testing.

1.3 Online Testing Approach

RTI primarily used NORC's AmeriSpeak panel to conduct the online testing. AmeriSpeak is a probability-based panel designed to be representative of the U.S. household population. The panel is composed of nearly 50,000 panel members from more than 40,000 households and provides sample coverage of approximately 97% of the household population.[3] The panelists are pre-registered members, who are selected using area probability and address-based sampling and complete small surveys for minimal compensation. Data are collected through a mixed-mode survey approach via online and telephone interviews. Approximately 15% of completed interviews are conducted via the telephone, ensuring that no groups are left out of the sample (e.g., non-internet users who may be more likely to be elderly, live in rural areas, or earn lower incomes).

Given the time allotted for the ITS screener testing, the AmeriSpeak probability panel was expected to provide a maximum of 10,000 interviews; the balance of the sample (~21,500) was expected to come from nonprobability online panels. NORC's TrueNorth Calibration Approach[4] enables a blending of probability and nonprobability samples using calibration weights to ensure that the final sample of respondents represents the U.S. household population.

Typically, NORC works with one nonprobability panel to supplement the AmeriSpeak sample. However, for the ITS testing, RTI and NORC developed an approach to also utilize sample from Amazon's Mechanical Turk (MTurk) nonprobability panel. RTI has considerable

[3] Additional information about AmeriSpeak panel sample selection is available through NORC's technical overview of the panel, which can be accessed at http://amerispeak.norc.org/Documents/Research/AmeriSpeak%20Technical%20Overview%202019%2002%2018.pdf.

[4] Additional information about the TrueNorth Calibration is available at http://amerispeak.norc.org/our-capabilities/Pages/TrueNorth.aspx.

experience working with MTurk and has previously found that that MTurk workers tend to produce data with better quality compared to other nonprobability panelists when they participate in scientific research (Hsieh et al., 2018). The anticipated distribution of sample across the three panels was as follows: AmeriSpeak—10,000; Lucid (NORC's nonprobability panel)—11,500 to 16,500; and MTurk—5,000 to 10,000. The distributions were estimates given unknowns based on the limited past efforts to collect data from such large samples of respondents.

Potential respondents were screened for being residents of the United States, English speaking, and 18 years of age or older.[5] Respondents were deduplicated across the three panels to the greatest degree possible. Those who agreed to participate were randomly assigned to one of the three versions of the ITS screener. They were informed that the survey was about identity theft, would take between 5 and 15 minutes to complete, and that participation was voluntary and were asked to check a box stating that they understood the terms and consented to participate in the survey. Panelists were offered the cash equivalent of $2 for completing the survey.

1.4 Data Collection

Data collection officially began on July 16, 2020, and ended on August 4, 2020, with a total of 32,177 interviews in the final sample (excluding respondents with major data quality issues who did not meet the threshold for inclusion); 30,901 were completed via the web and 1,276 (12% of the AmeriSpeak sample) via telephone interview. Approximately 34% (10,962) of the sample came from the AmeriSpeak probability-based panel; 35% (11,210) from the Lucid nonprobability panel; and 31% (10,005) from the MTurk nonprobability panel. ***Tables 1*** and ***2*** show the demographic distribution of respondents across the different survey modes and panels.

[5] Although the ITS is administered to persons ages 16 or older, the minimum age was increased to 18 years for online testing due to challenges in recruiting juvenile participants for online surveys.

Table 1. Unweighted Sample, by Demographic Characteristics and Mode

	Total		Web		Phone	
	Number	Percent	Number	Percent	Number	Percent
Total	32,177	100.00 %	30,901	100.00 %	1276	100.00 %
Sex						
Male	15,632	48.58 %	15,180	49.12 %	452	35.42 %
Female	16,545	51.42	15,721	50.88	824	64.58
Race/Hispanic origin*						
White	20,518	63.77 %	19,685	63.70 %	833	65.28 %
Black	3,614	11.23	3,353	10.85	261	20.45
Other	347	1.08	309	1.00	38	2.98
Hispanic	5,457	16.96	5,388	17.44	69	5.41
Two or more races	899	2.79	834	2.70	65	5.09
Asian	1,342	4.17	1,332	4.31	10	0.78
Age						
18–24	2,855	8.87 %	2,850	9.22 %	5	0.39 %
25–34	7,465	23.20	7,450	24.11	15	1.18
35–49	8,354	25.96	8,308	26.89	46	3.61
50–64	7,406	23.02	7,102	22.98	304	23.82
65 or older	6,097	18.95	5,191	16.80	906	71.00
Household income						
$24,999 or less	6,294	19.56 %	5,767	18.66 %	527	41.30 %
$25,000–$49,999	8,487	26.38	8,107	26.24	380	29.78
$50,000–$74,999	6,742	20.95	6,584	21.31	158	12.38
$75,000 or more	10,654	33.11	10,443	33.80	211	16.54

Note: Standard errors provided in Appendix.

*White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 2. Unweighted Sample, by Demographic Characteristics and Platform

	Total		AmeriSpeak		Lucid		MTurk	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Total	32,177	100.00 %	10,962	100.00 %	11,210	100.00 %	10,005	100.00 %
Sex								
Male	15,632	48.58 %	5,221	47.63 %	5,222	46.58 %	5,189	51.86 %
Female	16,545	51.42	5,741	52.37	5,988	53.42	4,816	48.14
Race/Hispanic origin*								
White	20,518	63.77 %	7,446	67.93 %	6,884	61.41 %	6,188	61.85 %
Black	3,614	11.23	1,469	13.40	1,322	11.79	823	8.23
Other	347	1.08	184	1.68	99	0.88	64	0.64
Hispanic	5,457	16.96	1,117	10.19	2,367	21.12	1,973	19.72
Two or more races	899	2.79	396	3.61	204	1.82	299	2.99
Asian	1,342	4.17	350	3.19	334	2.98	658	6.58
Age								
18–24	2,855	8.87 %	465	4.24 %	1,561	13.93 %	829	8.29 %
25–34	7,465	23.20	1,843	16.81	1,748	15.59	3,874	38.72
35–49	8,354	25.96	1,812	16.53	3,089	27.56	3,453	34.51
50–64	7,406	23.02	3,169	28.91	2,784	24.83	1,453	14.52
65 or older	6,097	18.95	3,673	33.51	2,028	18.09	396	3.96
Household income								
$24,999 or less	6,294	19.56 %	2,118	19.32 %	2,816	25.12 %	1,360	13.59 %
$25,000–$49,999	8,487	26.38	2,759	25.17	3,036	27.08	2,692	26.91
$50,000–$74,999	6,742	20.95	2,120	19.34	2,114	18.86	2,508	25.07
$75,000 or more	10,654	33.11	3,965	36.17	3,244	28.94	3,445	34.43

Note: Standard errors provided in Appendix.

*White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

The final sample was weighted using NORC's TrueNorth Calibration approach to benchmark to known population distributions from the U.S. Census Bureau's Current Population Survey (CPS). Three weights were developed to correspond with the three versions of the instrument. In other words, the respondents who completed Versions 1, 2, and 3 were independently calibrated to the benchmarks. ***Table 3*** shows the weighted count and distribution of respondents across each version. The benchmarking distributions are included in the ***Methodology*** section of this report because they do not align perfectly with the demographic categories provided on the file and used in BJS reports. For example, the Census categories used for benchmarking the race/ethnicity of respondents include Non-Hispanic White, Non-Hispanic Black, Hispanic, and Non-Hispanic Other. The demographic categories provided for analysis include Non-Hispanic white, Non-Hispanic black, Hispanic, Non-Hispanic other, Non-Hispanic Asian, and Non-Hispanic persons of two or more races.

Table 3. Weighted Sample, by Demographic Characteristics and Instrument Version

	Version 1		Version 2		Version 3	
	Number	Percent	Number	Percent	Number	Percent
Total	10,609	100.00	10,926	100.00	10,642	100.00
Sex						
Male	5,123	48.29	5,277	48.30	5,140	48.30
Female	5,486	51.71	5,649	51.70	5,502	51.70
Race/Hispanic origin*						
White	6,662	62.79	6,861	62.79	6,683	62.79
Black	1,265	11.93	1,303	11.93	1,269	11.93
Asian	491	4.63	458	4.19	485	4.56
Hispanic	1,768	16.66	1,821	16.66	1,773	16.66
Other	121	1.14	120	1.09	144	1.35
Two or more races	302	2.85	364	3.33	288	2.71
Age						
18–24	1,218	11.48	1,254	11.48	1,222	11.48
25–34	1,854	17.48	1,950	17.85	1,889	17.75
35–49	2,619	24.68	2,656	24.31	2,597	24.41
50–64	2,639	24.87	2,718	24.87	2,647	24.87
65 or older	2,280	21.49	2,348	21.49	2,287	21.49
Household income						
$24,999 or less	2,465	23.23	2,512	22.99	2,488	23.38
$25,000–$49,999	2,763	26.04	2,917	26.70	2,787	26.19
$50,000–$74,999	2,023	19.07	2,117	19.37	2,055	19.31
$75,000 or more	3,358	31.65	3,380	30.93	3,312	31.12

Note: Standard errors provided in Appendix Tables.

*White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

1.5 Strengths and Limitations of the Use of Online Panels for Testing the ITS Screeners

For the purpose of comparing how well different versions of questions perform in the field, online platforms offer considerable advantages. In less than 4 weeks, it was possible to collect more than 30,000 completed surveys. This likely would not be possible with an in-person or telephone survey. Additionally, although the collection relied on three different panels, the survey looked and functioned the same. This ensures that any findings of differences across the questionnaire versions can be attributed to differences in the questions rather than differences in methodology or the samples.

In terms of data quality (see Section 4.5) the online panels performed well. About 7% (2,350) of the initial pool of 34,527 respondents were removed from the final sample because of data quality issues; primarily short completion times or high numbers of skipped questions. Among those in the final sample, levels of item missingness were less than 1% for most items even though most items did not have any soft or hard prompts built in to encourage or force responses. For Versions 1 and 3, the items with the highest percent missing included the question about whether the respondent currently had a credit card in their name, the questions about month and year of discovery for the most recent incident, and the question about how long their personal information was misused before the identity theft was discovered. For Version 2, the questions about month and year of discovery and how long their information had been misused before the identity theft was discovered were also among the more problematic. Even among these items, the level of missingness was generally lower than 5% (see ***Tables 26***, ***27***, and ***28***). Additionally, respondents spent an average of 6 minutes completing the survey, which suggests that they were taking the time to read the questions; however, it is not possible to track the speed at which respondents were completing questions or to know whether they had the browser open to look at something else.

Although the panels provided a significant amount of high-quality data in a short period, there were also some limitations. Despite the calibration weighting, there could still be considerable bias in the samples and the estimates. The weighted cumulative response rate (based on the American Association for Public Opinion Research [AAPOR] Response Rate 3 [RR3] calculation)[6] was less than 6%, increasing the potential or likelihood of systematic nonresponse. Additionally, though it is possible to obtain participation from respondents as young as 13 using AmeriSpeak, the sample of juveniles is considerably more limited than the sample of adults. Although the ITS includes respondents 16 and older, this testing was restricted to those age 18 or older.

As anticipated and discussed further in the context of ***Tables 16*** and ***17***, the prevalence estimates generated through the online testing environment are considerably higher than those generated by the NCVS. This could suggest that the presence of an interviewer has a suppression effect, that respondents become fatigued after completing the core NCVS and do not answer ITS questions accurately, that the interviewer serves to clarify the questions and there are more false positives with online testing,[7] or that topic saliency bias results in an online sample of respondents that is more likely to have experienced identity theft than the general population. If online platforms were used to generate national estimates of identity theft, additional research would be needed to better understand differences in the magnitude of estimates generated through different modes. However, the focus of this testing was not on comparing the findings to the NCVS, but on understanding differences across the three instrument versions, which were all subject to the same factors that result in higher estimates than generated through in-person interviews. The next section of the report describes these findings.

[6] See https://www.aapor.org/AAPOR_Main/media/MainSiteFiles/Standard-Definitions2015_8thEd.pdf for AAPOR response rate definitions.

[7] Although the issue of false positive responses was not examined directly in this study, other studies have found relatively low rates of false positives in online surveys. See, for example, https://rvap.uiowa.edu/assets/Uploads/2898aa5950/Campus-Climate-Survey-2016.pdf (pp 130-136).

2. Key Findings

Across the tables presented in this section, findings are examined by the following categories:

- Instrument version
  - Version 1 – current ITS
  - Version 2 – fully revised ITS
  - Version 3 – ITS with attempts removed
- Survey platform
  - AmeriSpeak
  - Lucid
  - MTurk
- Mode
  - Web
  - Phone

The types of identity theft and demographic characteristics of respondents and victims presented in the tables in the following section are consistent with the categories used and reported by BJS from the ITS.

2.1 Comparison of 12-month Prevalence Estimates Across Versions 1, 2, and 3

- Versions 2 (31.98%) and 3 (30.2%) generated a significantly lower prevalence (90% Confidence Interval [CI]) of identity theft than Version 1 (37.11%). This was anticipated because both Versions 2 and 3 excluded attempted incidents, whereas Version 1 did not (see ***Table 4***).
- Although the prevalence estimate for Version 2 appeared higher than the estimate for Version 3, the difference was not statistically significant for overall identity theft (see Table 4; testing not shown).
- The apparent higher rate of overall identity theft for Version 2 compared to Version 3 may be because social media accounts are asked about separately in Version 2. The reported prevalence of social media account misuse in Version 2 was 12.25%, whereas the prevalence of other existing account misuse (which could include social media) in Version 3 was 10.27% (see Table 4).
- The significantly lower identity theft prevalence rates in Versions 2 and 3 compared to Version 1 were consistent across most demographic groups. However, there were no significant differences in the prevalence rates for the following race categories: black, other, or persons of two or more races (see ***Table 5***).
- In Version 2 compared to Version 1, a significantly higher percentage of respondents experienced banking account misuse (90% CI) and new account misuse (95% CI) as the most recent incident, whereas a significantly lower percentage experienced other

existing account misuse and multiple types in the same incident as their most recent incident (see ***Table 6***).

- In Version 3 compared to Version 1, a significantly higher percentage of respondents experienced credit card and banking account misuse as their most recent incident (90% CI), whereas a significantly lower percentage experienced the misuse of other existing accounts and multiple types as their most recent incident (90% CI; see Table 6).

Table 4. Prevalence of Identity Theft in the Past 12 Months, by Type of Identity Theft and Instrument Version

	Version 1*		Version 2		Version 3	
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a
Total	3,937	37.11 %	3,494	31.98 %++	3,213	30.20 %++
Existing account						
Credit card	1,703	16.05	1,349	12.35 ++	1,484	13.94 ++
Bank	2,148	20.25	1,641	15.02 ++	1,724	16.20 ++
Social media	~	~	1,338	12.25	~	~
Other	1,675	15.79	962	8.81 ++	1,093	10.27 ++
New account	779	7.35	570	5.21 ++	455	4.27 ++
Personal information	507	4.78	333	3.05 ++	400	3.75 ++

Note: Standard errors provided in Appendix Tables.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Based on a representative sample of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 5. Persons Age 18 or Older Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics and Instrument Version

	Version 1		Version 2		Version 3	
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a
Total	3,937	37.11 %	3,494	31.98 %++	3,213	30.20
Sex						
Male*	1,931	37.69	1,638	31.05 ++	1,564	30.43 ++
Female	2,006	36.56	1,855	32.84 ++	1,650	29.98 ++
Race/Hispanic origin/b						
White*	2,329	34.97	1,987	28.96 ++	1,808	27.06 ++
Black	460	36.40	506	38.85	432	34.01
Asian	178	36.21	123	26.79 ++	123	25.42 ++
Hispanic	816	46.14	721	39.61 ++	696	39.27 ++
Other	42	34.49	28	23.55	38	26.21
Two or more races	112	36.95	129	35.31	116	40.38
Age						
18–24	532	43.64	446	35.58 ++	437	35.74 ++
25–34	801	43.22	735	37.69 ++	649	34.35 ++
35–49*	1,051	40.15	969	36.50 ++	831	32.00 ++
50–64	954	36.17	795	29.24 ++	781	29.49 ++
65 or older	598	26.23	548	23.35 +	516	22.57 ++
Household income						
$24,999 or less	867	35.16	758	30.15 ++	740	29.74 ++
$25,000–$49,999	1,000	36.19	910	31.20 ++	830	29.77 ++
$50,000–$74,999	748	36.98	673	31.79 ++	606	29.51 ++
$75,000 or more*	1,322	39.36	1,153	34.12 ++	1,038	31.33 ++
Urbanicity						
Urban	3,430	37.62	3,047	32.36 ++	2,784	30.33 ++
Non-urban	487	33.33	425	28.94 ++	404	28.57 ++
Unknown	20	65.07	22	51.90	26	51.96

Note: Standard errors provided in Appendix Tables. Percentages are based on the number of persons in each category.

*Comparison group.

†Significant difference from comparison group at 95% confidence level.

‡Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 6. Most Recent Incident of Identity Theft, by Type of Identity Theft and Instrument Version

	Version 1*			Version 2			Version 3		
	Number of victims	Percent of all respondents/a	Percent of all victims	Number of victims	Percent of all respondents/a	Percent of all victims	Number of victims	Percent of all respondents/a	Percent of all victims
Total	3,937	37.11 %	100.00 %	3,494	31.98 %++	100.00 %	3,213	30.20 %++	100.00 %
Only one type of existing account									
Credit card	794	7.49	20.18	697	6.38 ++	19.95	814	7.65	25.32 ++
Bank	976	9.20	24.80	965	8.83	27.62 ++	933	8.77	29.03 ++
Social media	~	~	~	782	7.16	22.40	~	~	~
Other	612	5.77	15.54	424	3.88 ++	12.13 ++	356	3.35 ++	11.09 ++
Opened new account only	141	1.33	3.57	162	1.49	4.65 +	95	0.90 ++	2.97
Misused personal information only	90	0.85	2.28	88	0.80	2.51	92	0.86	2.85
Multiple types	1,324	12.48	33.63	375	3.44 ++	10.75 ++	924	8.68 ++	28.74 ++

Note. Standard errors provided in appendix tables.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Based on a representative sample of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

2.2 Use of the Dual Reference Period and Patterns Across Demographic Groups

- A key distinction between Version 2 and Versions 1 and 3 is that Version 2 uses a dual reference period in which respondents were first asked about their experiences with identity theft in their lifetime, followed by a question about their experiences in the past 12 months if they answered the lifetime question affirmatively. As anticipated, for all types of identity theft, the percentage of respondents experiencing identity theft in their lifetime was significant higher (90% CI) than the 12-month prevalence estimates for all three versions. This suggests that respondents were able to clearly see the distinction between the two reference periods and did not have problems thinking about the two different periods (see ***Table 7***).

- Across demographic groups, there were some variations in patterns of identity theft in the previous 12 months across the three versions. In Versions 2 and 3, respondents who are blacks or two or more races were more likely than those who are white to experience identity theft in the prior 12 months than whites, but this was not true of Version 1. In Version 1, persons ages 25 to 34 were more likely than those ages 35 to 49 to experience identity theft, whereas this was not true in Versions 2 and 3. In Versions 1 and 2, persons in the two lowest income categories had lower prevalence rates than persons in the top income categories; these differences did not test in Version 3 (see ***Table 8***).

- Otherwise, the comparisons among demographic groups were consistent across the instruments. For example, across all three versions, there were no differences in the rates of identity theft for male and female respondents or persons who live in urban versus non-urban areas. Additionally, across all three versions, persons age 65 or older had lower rates of identity theft than those ages 35 to 49 (see Table 8).

- Although the patterns of lifetime prevalence rates were fairly similar to those of the 12-month rates, the lifetime prevalence rates revealed additional differences in the likelihood of experiencing identity theft that were not present in the 12-month rates. This is likely a product of the increased sample sizes of lifetime prevalence victims and the ability to better detect differences among groups (see Table 8).

- Focusing solely on Version 2, more than half (53%) of all victims who experienced identity theft in their lifetime had also experienced it during the past 12 months (see ***Table 9***).

- Across most demographic characteristics, the majority of lifetime victims also experienced identity theft during the past 12 months. Blacks, Hispanics, and persons ages 18 to 49 were the exceptions. Among these groups, 40% to 49% of lifetime victims experienced identity theft during the past 12 months (see ***Table 10***).

Table 7. Prevalence of Identity Theft, by Type of Identity Theft, Instrument Version, and Reference Period

	Version 1 - 12-month		Version 2 - 12-month		Version 3 - 12-month		Version 2 - Lifetime*	
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/
Total	3,937	37.11 %++	3,494	31.98 %++	3,213	30.20 %++	7,449	68.18 %
Existing account								
Credit card	1,703	16.05 ++	1,349	12.35 ++	1,484	13.94 ++	3,843	35.18
Bank	2,148	20.25 ++	1,641	15.02 ++	1,724	16.20 ++	4,093	37.46
Social media	~	~	1,338	12.25 ++	~	~	3,009	27.54
Other	1,675	15.79 ++	962	8.81 ++	1,093	10.27 ++	2,055	18.81
New account	779	7.35 ++	570	5.21 ++	455	4.27 ++	1,381	12.64
Personal information	507	4.78 ++	333	3.05 ++	400	3.75 ++	867	7.94

Note: Standard errors provided in Appendix Tables.
*Comparison group.
+Significant difference from comparison group at 95% confidence level.
++Significant difference from comparison group at 90% confidence level.
~Not applicable.
a/Based on a representative sample of US residents age 18 or older.
Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 8. Persons Age 18 or Older Who Experienced One or More Incidents of Identity Theft, by Victim Characteristics, Instrument Version, and Reference Period

	Version 1: 12-month		Version 2: 12-month		Version 3: 12-month		Version 2: Lifetime	
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a
Total	3,937	37.11 %	3,494	31.98 %	3,213	30.20	7,449	68.18 %
Sex								
Male*	1,931	37.69 %	1,638	31.05 %	1,564	30.43	3,510	66.52 %
Female	2,006	36.56	1,855	32.84	1,650	29.98	3,939	69.72 ++
Race/Hispanic origin/b								
White*	2,329	34.97 %	1,987	28.96 %	1,808	27.06	4,652	67.80 %
Black	460	36.40	506	38.85 ++	432	34.01 ++	858	65.81
Asian	178	36.21	123	26.79	123	25.42	282	61.71 ++
Hispanic	816	46.14 ++	721	39.61 ++	696	39.27 ++	1,294	71.06 ++
Other	42	34.49	28	23.55	38	26.21	87	73.00
Two or more races	112	36.95	129	35.31 +	116	40.38 ++	276	75.75 ++
Age								
18–24	532	43.64 %	446	35.58 %	437	35.74	797	63.51 %++
25–34	801	43.22 +	735	37.69	649	34.35	1,409	72.22
35–49*	1,051	40.15	969	36.50	831	32.00	1,898	71.48
50–64	954	36.17 ++	795	29.24 ++	781	29.49	1,863	68.54 +
65 or older	598	26.23 ++	548	23.35 ++	516	22.57 ++	1,482	63.15 ++
Household income								
$24,999 or less	867	35.16 %++	758	30.15 %++	740	29.74	1,523	60.61 %++
$25,000–$49,999	1,000	36.19 ++	910	31.20 ++	830	29.77	1,907	65.37 ++
$50,000–$74,999	748	36.98	673	31.79	606	29.51	1,492	70.49 ++
$75,000 or more*	1,322	39.36	1,153	34.12	1,038	31.33	2,527	74.77
Urbanicity								
Urban	3,430	37.62 %	3,047	32.36 %	2,784	30.33	6,444	68.45 %
Non-urban	487	33.33	425	28.94	404	28.57	973	66.26
Unknown	20	65.07	22	51.90	26	51.96	31	74.03

Note: Percentages are based on the number of persons in each category. Standard errors provided in Appendix Tables.

*Comparison group.

†Significant difference from comparison group at 95% confidence level.

‡Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 9. Relationship Between Lifetime Prevalence and 12-month Prevalence, by Type of Identity Theft (Version 2)

	Lifetime prevalence		12-month prevalence		Percent of lifetime victims
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	No past year ID theft
Total	7,449	68.18 %++	3,494	31.98 %++	53.10 %++
Existing account					
Credit card	3,843	35.18 ++	1,349	12.35 ++	64.61 +
Bank	4,093	37.46 ++	1,641	15.02 ++	59.74
Social media	3,009	27.54 ++	1,338	12.25 ++	54.50 ++
Other	2,055	18.81 ++	962	8.81 ++	52.60 ++
New account	1,381	12.64 ++	570	5.21 ++	58.47
Personal information*	867	7.94	333	3.05	61.26

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 10. Relationship Between Lifetime Prevalence and 12-month Prevalence of Identity Theft, by Victim Characteristics (Version 2)

	Lifetime prevalence (any identity theft)*		12-month prevalence (any identity theft)		Percent of lifetime victims
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	No past year ID theft
Total	7,449	68.18 %	3,494	31.98 %	53.09 %
Sex					
Male	3,510	32.13 %	1,638	14.99 %	53.33 %
Female	3,938	36.04 ++	1,855	16.98	52.89
Race/Hispanic origin/b					
White	4,652	42.58 %	1,987	18.19 %	57.29 %
Black	857	7.84	506	4.63 ++	40.96 ++
Other/b	87	0.80	28	0.26	67.82
Hispanic	1,294	11.84 ++	721	6.60 ++	44.28 ++
Two or more races	276	2.53 ++	129	1.18	53.26
Asian	283	2.59 ++	123	1.13	56.54
Age					
18–24	796	7.29 %+	446	4.08 %	43.97 %+
25–34	1,409	12.90	735	6.73	47.84
35–49	1,898	17.37	969	8.87	48.95
50–64	1,863	17.05	795	7.28 ++	57.33 ++
65 or older	1,482	13.56 ++	548	5.02 ++	63.02 ++
Household income					
$24,999 or less	1,523	13.94 %+	758	6.94 %++	50.23 %++
$25,000–$49,999	1,907	17.45 ++	910	8.33 ++	52.28
$50,000–$74,999	1,492	13.66 ++	673	6.16	54.89
$75,000 or more	2,527	23.13	1,153	10.55	54.37
Urbanicity					
Urban	6,445	58.99 %	425	27.89 %	52.72 %
Non-urban	973	8.91	3,047	3.89 ++	56.32
Unknown	31	0.28	22	0.20 ++	29.89 ++

Note: Standard errors provided in Appendix Tables.

a/Based on a representative sample of US residents age 18 or older.

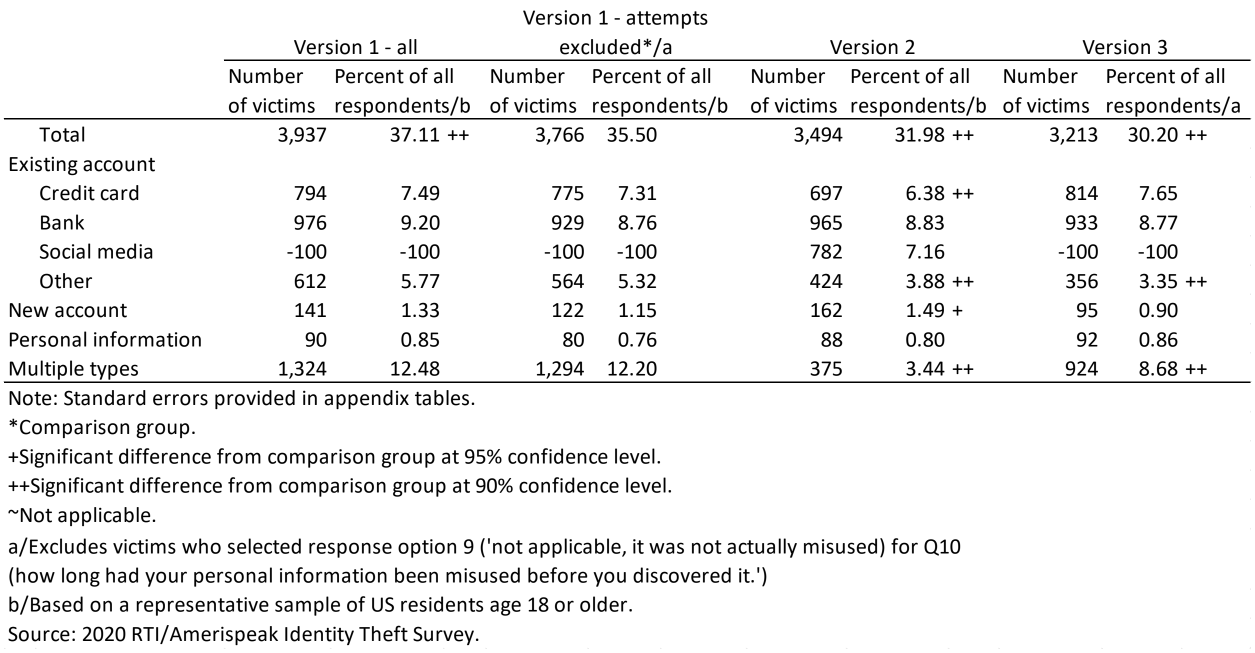
b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

2.3 Impact of Exclusion of Attempts on Prevalence Estimates

- Another distinction between Versions 2 and 3 and Version 1 is that Versions 2 and 3 exclude attempts. Based the questions included in Version 1, it is possible to identify attempted incidents through Question 10, which asks how long the most recent incident of identity theft had been occurring before it was discovered and provides the following response option: "Not applicable, it was not actually misused." Even with the attempts excluded, the prevalence rate for Version 1 was significantly higher than for Version 2 for overall identity theft. The fact that the prevalence rate for Version 2 is lower than the rate for Version 1 after controlling for attempted incidents and with the inclusion of separate questions on social media misuse may suggest that Version 2 is better at controlling for telescoping than Version 1 (see ***Table 11***).
- Although the only difference between Versions 1 and 3 is the exclusion of attempts, the overall prevalence rate for Version 3 was significantly lower (90% CI) than the rate for Version 1 with the attempts excluded. This may be due to an issue that was identified in cognitive testing; the language used to exclude attempts, which focuses on financial losses, may serve to exclude victims who experienced the completed misuse of existing social media accounts but did not experience a financial loss. This issue was addressed in Version 2 by separating the misuse of social media accounts into a separate identity theft category (see Table 11).

Table 11. Prevalence of Identity Theft During the Past 12 Months, by Type of Identity Theft, Instrument Version, and Exclusion of Attempts



	Version 1 - all		Version 1 - attempts excluded*/a		Version 2		Version 3	
	Number of victims	Percent of all respondents/b	Number of victims	Percent of all respondents/b	Number of victims	Percent of all respondents/b	Number of victims	Percent of all respondents/a
Total	3,937	37.11 ++	3,766	35.50	3,494	31.98 ++	3,213	30.20 ++
Existing account								
Credit card	794	7.49	775	7.31	697	6.38 ++	814	7.65
Bank	976	9.20	929	8.76	965	8.83	933	8.77
Social media	-100	-100	-100	-100	782	7.16	-100	-100
Other	612	5.77	564	5.32	424	3.88 ++	356	3.35 ++
New account	141	1.33	122	1.15	162	1.49 +	95	0.90
Personal information	90	0.85	80	0.76	88	0.80	92	0.86
Multiple types	1,324	12.48	1,294	12.20	375	3.44 ++	924	8.68 ++

Note: Standard errors provided in appendix tables.
*Comparison group.
+Significant difference from comparison group at 95% confidence level.
++Significant difference from comparison group at 90% confidence level.
~Not applicable.
a/Excludes victims who selected response option 9 ('not applicable, it was not actually misused) for Q10 (how long had your personal information been misused before you discovered it.')
b/Based on a representative sample of US residents age 18 or older.
Source: 2020 RTI/Amerispeak Identity Theft Survey.

2.4 Respondents' Ability to Date Incidents and the Impact of Dating on Telescoping

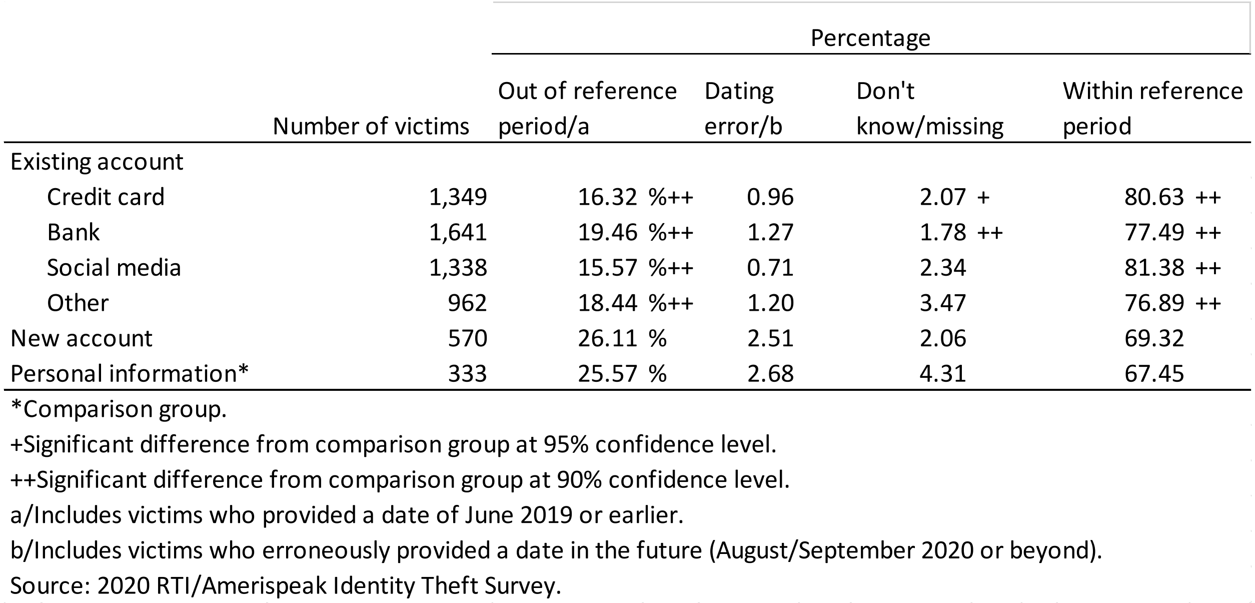
- One of the biggest changes to the Version 2 instrument was that questions about the month and year of most recent occurrence were asked for each type of identity theft that the victim reported experiencing in the past 12 months. Across all type of identity theft, the majority of victims provided a month and year that were within the 12-month reference period. This varied slightly by the type of identity theft with just under 70% of victims of new account and other personal information misuse reporting a date within the reference period, and about 80% of victims of existing account misuse providing a date within the reference period. This finding may suggest that victims of more serious types of identity theft are more likely to telescope incidents into the reference period and that the inclusion of dating questions screens them out (see ***Table 12***).
- Across victim demographic characteristics, the significant differences in the percentage of victims who provided a date of most recent occurrence within the reference period varied by the type of identity theft. However, there were no differences between males and females in the percentage providing a date within the reference period, regardless of the type of identity theft (see ***Table 13***).
- With Version 2, it was possible to examine the relationship between the month and year of the most recent occurrence (among all types of identity theft) and the month and year of discovery of the most recent incident. Of the 2,933 victims (84%) who provided a date within the reference period, about 60% (1,767) provided the same month and year for the most recent occurrence and the discovery of the most recent incident, 31% provided a discovery date prior to the most recent occurrence, and 9% provided a discovery date that was later than the most recent occurrence (see ***Figure 1***).
- For context, the patterns seen in the Version 2 data in the relationship between most recent occurrence and discovery date were generally consistent with those seen in a prior examination of ITS data from 2008.[8]
- A higher percentage of victims of existing account misuse provided the same month and year for the most recent occurrence and discovery compared to victims of new account and other personal information misuse (see ***Table 14***). This finding is consistent with findings in prior BJS reports on identity theft showing that most incidents of existing account misuse are resolved within 1 day.
- About 60% of victims of the misuse of other personal information provided a different month and year for the discovery of the incident and the most recent occurrence, suggesting that victims recognized a distinction between the two reference points in an episode of identity theft. The percentages were lower for other types of identity theft, but as noted, it is not unexpected that the dates would be the same for the majority of victims (see Table 14).
- There were variations across demographic characteristics in the percentage of victims who provided dates of most recent occurrence and discovery that were the same (nearly 60% white vs. about 40% black and Hispanic). Similarly, about 60% of victims age 65 or older provided the same date, compared to less than 45% of victims under age 35. However, these differences may be a product of difference in

[8] Findings from the secondary data analysis of ITS data conducted by RTI in early 2020.

the types of identity theft experienced by different subpopulations (see ***Table 15***). For example, if nonwhite victims are less likely to experience existing account misuse (which tends to be discovered quickly) compared to white victims, this could account for why a higher proportion of white victims gave the same occurrence and discovery month and year.

- There were not significant differences across demographic groups in the percentage of victims with missing, unknown, or out-of-reference period dates (see Table 15).
- All three versions of the questionnaire ask victims to provide the month and year of when they first discovered the most recent incident of identity theft. Across all three versions, the vast majority of incidents (about 95% or more) were discovered within 12 months of the time of the interview. The percentage of incidents discovered more than 12 months from the time of the interview was higher for Version 1 compared to that for Versions 2 and 3. This may suggest that respondents were more likely to telescope incidents into the reference period in Version 1; however, it is difficult to determine this conclusively because it is possible for the discovery to precede the most recent occurrence. In other words, the most recent occurrence could have been within the reference period, although the date of discovery was not (see ***Table 16***).
- There were no major differences among the three versions in terms of how long the identity theft had been occurring at the time of discovery. Across all three versions, less than 3% of victims said it had been happening for 1 year or more. This percentage was highest among those in Version 2 who provided a date of most recent occurrence outside of the 12-month reference period, but the difference was not statistically significant. This may provide some evidence that these victims engaged in telescoping because they were more likely to recall or wanted to discuss a serious episode that lasted for a long time (see ***Table 17***).

Table 12. Percentage of Victims Providing a Date of Occurrence Prior to or Outside the 12-month Reference Period or Providing a "Don't Know" Response, by Type of Identity Theft (Version 2)



		Percentage			
	Number of victims	Out of reference period/a	Dating error/b	Don't know/missing	Within reference period
Existing account					
Credit card	1,349	16.32 %++	0.96	2.07 +	80.63 ++
Bank	1,641	19.46 %++	1.27	1.78 ++	77.49 ++
Social media	1,338	15.57 %++	0.71	2.34	81.38 ++
Other	962	18.44 %++	1.20	3.47	76.89 ++
New account	570	26.11 %	2.51	2.06	69.32
Personal information*	333	25.57 %	2.68	4.31	67.45

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Includes victims who provided a date of June 2019 or earlier.

b/Includes victims who erroneously provided a date in the future (August/September 2020 or beyond).

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 13. Percentage of Victims Providing a Date of Occurrence Prior to or Outside the 12-Month Reference Period or Providing a “Don't Know” Response, by Victim Characteristics and Select Types of Identity Theft (Version 2)

	Credit card misuse					Banking account misuse					New account					Personal information				
	Number of victims	Out of reference period/a	Dating error/b	Don't know/ missing	Within reference period	Number of victims	Out of reference period/a	Dating error/b	Don't know/ missing	Within reference period	Number of victims	Out of reference period/a	Dating error/b	Don't know/ missing	Within reference period	Number of victims	Out of reference period/a	Dating error/b	Don't know/ missing	Within reference period
Total	1,349	16.32 %	0.99 %	2.07 %	80.63 %	1,641	19.46 %	1.27 %	1.78 %	77.49 %	570	26.11 %	2.51 %	2.06 %	69.32 %	333	25.57 %	2.68 %	4.31 %	67.45 %
Sex																				
Male*	697	17.34	1.14	1.50	80.02	791	20.92	1.80	1.66	75.61	299	28.97	3.74	0.67	66.62	184	25.54	3.16	4.58	66.72
Female	652	15.23	0.82	2.67	81.28	850	18.10	0.77	1.88	79.25	271	22.95	1.15	3.61 +	72.30	150	25.60	2.09	3.97	68.34
Race/Hispanic origin/c																				
White*	762	14.32	0.53	2.70	82.45	800	15.44	0.10	2.12	82.33	231	24.49	1.26	0.47	73.78	139	24.47	2.10	2.67	70.76
Black	168	24.21 ++	1.81	1.35	72.63 ++	280	22.01 +	1.64	2.43	73.91 ++	119	24.73	1.90	6.85 +	66.51	54	31.72	0.00 +	9.91	58.37
Asian	59	17.11	0.00 ++	0.00 ++	82.89	46	19.76	4.10	0.00 ++	76.14	15	11.14 +	0.00	0.00	88.86 ++	9	10.19 +	0.00 +	0.00 ++	89.81 ++
Hispanic	313	17.27	1.99	1.48	79.26	443	27.02 ++	3.06 ++	1.12	68.80 ++	189	30.78	4.84	1.34	63.04 +	124	25.67	4.87	4.26	65.20
Other/b	16	6.28 +	0.00 ++	0.00 ++	93.72 ++	15	24.19	0.00 +	0.00 ++	75.81	2	0.00 ++	0.00	0.00	100.00 ++	2	36.99	0.00 +	0.00 ++	63.01
Two or more races	32	16.80	0.00 ++	1.27	81.94	56	2.72 ++	0.00 +	0.72	96.55 ++	14	21.73	0.00	0.00	78.27	5	9.45	0.00 +	0.00 ++	90.55 +
Age																				
18–24	122	28.50	0.00 +	0.50	71.00	221	23.45	2.41	2.01	72.14	66	35.58	3.21	0.52	60.69	37	36.21	0.00	5.68	58.11
25–34	269	22.18	1.00	1.35	75.47	398	21.93	0.53	1.77	75.77	150	21.94 ++	3.27	0.15	74.64 +	97	27.60	4.40 +	2.03	65.97
35–49*	359	18.84	0.93	0.94	79.29	496	21.28	1.88	0.58	76.27	194	32.81	1.77	1.27	64.16	102	24.09	0.37	3.18	72.37
50–64	330	12.58 +	1.74	3.42 +	82.26	352	16.94	1.16	1.51	80.40	114	17.03 ++	3.37	3.21	76.39 +	73	25.56	5.92	5.21	63.31
65 or older	270	6.19 ++	0.58	3.33 +	89.91 ++	174	8.62 ++	0.00 ++	5.48 ++	85.89 ++	45	20.07	0.00	11.25	68.69	25	7.63 ++	0.00	13.11	79.26
Household income																				
$24,999 or less	227	25.22 ++	0.28 +	1.99	72.51 ++	388	24.08 ++	2.69	2.87	70.36 ++	168	27.51	1.57	5.11	65.81 +	96	28.81	0.41	4.59	66.19
$25,000–$49,999	330	12.02	1.54	2.21	84.23	451	16.76	1.45	0.84	80.95	162	23.99	2.46	0.84	72.72	92	20.42	4.17	4.61	70.80
$50,000–$74,999	268	21.73 ++	0.88	2.11	75.28 ++	328	22.82 ++	0.25	2.05	74.88 ++	102	34.98 ++	4.75	0.41	59.86 ++	67	26.44	2.88	4.67	66.02
$75,000 or more*	524	12.41	0.99	1.99	84.61	474	15.91	0.64	1.59	81.86	138	20.36	2.07	1.01	76.56	78	26.86	3.56	3.28	66.29

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

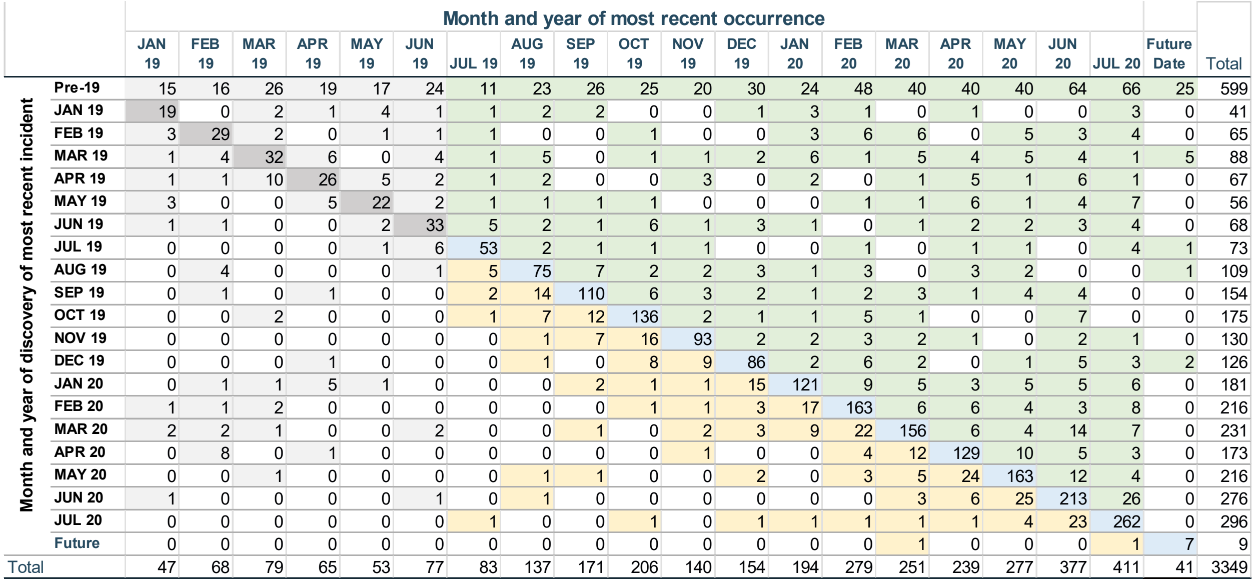
a/Includes victims who provided a date of June 2019 or earlier.

b/Includes victims who provided a date prior to when the interview occurred (August/September 2020 or later).

c/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Figure 1. Relationship Between the Date of Most Recent Occurrence and the Date of Discovery of Identity Theft (Version 2)



Month and year of discovery of most recent incident	Month and year of most recent occurrence																				
	JAN 19	FEB 19	MAR 19	APR 19	MAY 19	JUN 19	JUL 19	AUG 19	SEP 19	OCT 19	NOV 19	DEC 19	JAN 20	FEB 20	MAR 20	APR 20	MAY 20	JUN 20	JUL 20	Future Date	Total
Pre-19	15	16	26	19	17	24	11	23	26	25	20	30	24	48	40	40	40	64	66	25	599
JAN 19	19	0	2	1	4	1	1	2	2	0	0	1	3	1	0	1	0	0	3	0	41
FEB 19	3	29	2	0	1	1	1	0	0	1	0	0	3	6	6	0	5	3	4	0	65
MAR 19	1	4	32	6	0	4	1	5	0	1	1	2	6	1	5	4	5	4	1	5	88
APR 19	1	1	10	26	5	2	1	2	0	0	3	0	2	0	1	5	1	6	1	0	67
MAY 19	3	0	0	5	22	2	1	1	1	1	0	0	0	1	1	6	1	4	7	0	56
JUN 19	1	1	0	0	2	33	5	2	1	6	1	3	1	0	1	2	2	3	4	0	68
JUL 19	0	0	0	0	1	6	53	2	1	1	1	0	0	1	0	1	1	0	4	1	73
AUG 19	0	4	0	0	0	1	5	75	7	2	2	3	1	3	0	3	2	0	0	1	109
SEP 19	0	1	0	1	0	0	2	14	110	6	3	2	1	2	3	1	4	4	0	0	154
OCT 19	0	0	2	0	0	0	1	7	12	136	2	1	1	5	1	0	0	7	0	0	175
NOV 19	0	0	0	0	0	0	0	1	7	16	93	2	2	3	2	1	0	2	1	0	130
DEC 19	0	0	0	1	0	0	0	1	0	8	9	86	2	6	2	0	1	5	3	2	126
JAN 20	0	1	1	5	1	0	0	0	2	1	1	15	121	9	5	3	5	5	6	0	181
FEB 20	1	1	2	0	0	0	0	0	0	1	1	3	17	163	6	6	4	3	8	0	216
MAR 20	2	2	1	0	0	2	0	0	1	0	2	3	9	22	156	6	4	14	7	0	231
APR 20	0	8	0	1	0	0	0	0	0	0	1	0	0	4	12	129	10	5	3	0	173
MAY 20	0	0	1	0	0	0	0	1	1	0	0	2	0	3	5	24	163	12	4	0	216
JUN 20	1	0	0	0	0	1	0	1	0	0	0	0	0	0	3	6	25	213	26	0	276
JUL 20	0	0	0	0	0	0	1	0	0	1	0	1	1	1	1	1	4	23	262	0	296
Future	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	7	9
Total	47	68	79	65	53	77	83	137	171	206	140	154	194	279	251	239	277	377	411	41	3349

Note: Includes victims who provided a month and year of most recent occurrence and discovery.

Within reference period, discovery prior to most recent occurrence (n=908)

Same month/year of most recent occurrence and discovery (in reference period) (n=1,767)

Within reference period, discovery later than most recent occurrence (n=258)

Most recent occurrence outside reference period (n=389)

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 14. Relationship Between the Date of Most Recent Occurrence and Date of Discovery, by Type of Identity Theft

		Percentage of victims		
	Total Number	Same month/ year	Different month/ year	Missing/don't know/out of reference period
Existing account				
Credit card	965	58.68 %++	28.69 %++	12.63 %
Bank	697	49.02 ++	33.25 ++	17.62
Social media	782	54.48 ++	32.02 ++	13.49
Other	424	49.29 ++	36.01 ++	14.69
New account	162	29.63	43.20 ++	27.19 +
Personal information*	88	23.86	60.29	16.04
Multiple types	365	46.46 ++	29.07 ++	24.46 +

Note: Standard errors provided in Appendix Tables.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 15. Relationship Between the Date of Most Recent Occurrence and the Date of Discovery, by Victim Characteristics

		Percentage of victims						
	Total number	Same month/ year			Different month/ year		Missing/don't know/out of reference period	
Total	3,495	50.39	%		33.25		16.37	
Sex								
Male*	1,639	46.98	%		35.81		17.21	
Female	1,856	53.39	%	++	30.98	++	15.63	
Race/Hispanic origin/a								
White*	1,987	57.02	%		29.49		13.49	
Black	506	41.11	%	++	37.15	++	21.74	++
Other/b	29	34.48	%	++	34.48		31.03	
Hispanic	722	38.37	%	++	41.14	++	20.50	++
Two or more races	129	58.14	%		31.78		10.08	
Asian	123	47.15	%	++	33.33		19.51	
Age								
18–24	447	43.85	%		34.68		21.48	
25–34	736	44.57	%		38.86		16.58	
35–49*	970	45.36	%		37.11		17.53	
50–64	794	58.44	%	++	28.84	++	12.72	++
65 or older	548	60.58	%	++	24.09	++	15.33	
Household income								
$24,999 or less	758	40.63	%	++	35.75	++	23.61	++
$25,000–$49,999	910	47.69	%	++	37.36	++	14.95	
$50,000–$74,999	673	52.75	%	+	30.76		16.49	++
$75,000 or more*	1,153	57.50	%		29.84		12.66	
Urbanicity								
Urban*	425	51.53	%		32.47		16.00	
Non-urban	3,046	50.36	%		33.13		16.51	
Unknown	24	31.72	%	+	64.52	++	3.76	++

Note: Standard errors provided in Appendix Tables.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 16. Time From Discovery of the Most Recent Incident to Interview, by Questionnaire Version and Type of Identity Theft

		Percentage of victims					
	Total number of victims	Less than 1 month	1-6 months	7-12 months	13-24 months	25-36 months	More than 36 months
Version 1							
Total	3790	66.39 %	25.66	2.70	2.55	1.11	1.58
Existing account	3619	66.84 % ++	25.37	2.49	2.56	1.08	1.66
New account	746	42.63 %	39.02 ++	4.99	5.72 ++	2.84 +	4.88
Personal information	494	37.45 %	39.44 ++	5.42	6.31 ++	4.03 ++	7.37
Version 2							
Total	3350	68.45 %	25.78	3.32	1.97	0.22	0.26
Existing account	3256	68.86 %	25.50	3.20	1.97	0.20	0.27
New account	326	52.80 %	36.79	5.93	3.02	0.31	1.07
Personal information	570	48.16 %	40.16	6.37	3.04	0.34	1.82
Version 3							
Total	3058	69.20 %	26.58	1.77	1.79	0.39	0.25
Existing account	2922	69.23 % ++	26.57	1.69	1.85	0.40	0.26
New account	433	47.11 % ++	43.53	5.00	3.11	0.84	0.39 +
Personal information	380	47.89 % ++	40.58 ++	4.53	5.67 +	1.09	0.38 ++

Note: Based on unweighted data. Includes victims who provided a month and year of discovery. For version 1 about 2% of victims were missing the date; version 2 about 1.5%; and version 3 about 4%.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 17. Relationship Between the Time of Most Recent Occurrence and How Long the Identity Theft Had Been Happening When It Was Discovered

	Length of time from interview to most recent occurrence - Version 2							
How long ID theft had been happening when discovered	Same month	1 to 6 months	7 to 12 months	Out of reference period	Dating error/a	Total	Version 1*	Version 3
One day or less (1-24 hours)	42.76 %	35.00 %+	35.94 %+	29.73 %++	10.24 %+	35.23 %++	42.30 %	36.90 %++
More than a day, but less than a week (25 hours-6 days)	20.57	25.14 ++	26.59 ++	18.39	8.91 ++	23.96 ++	21.59	23.76 +
At least a week, but less than one month (7-30 days)	10.66	14.45 ++	13.33 +	14.19	9.81	13.61 ++	10.83	13.46 ++
One month to less than three	7.44	9.83 ++	9.67 ++	12.39 ++	21.23 +	9.95 ++	6.49	9.66 ++
Three months to less than six	6.10 +	3.85	3.86	5.45 +	24.02 ++	4.58 ++	2.89	3.37
Six months to less than one year	3.25	2.37	3.10	2.74	15.41	2.89	2.26	1.74
One year or more	1.52	2.30	1.65	4.65 ++	0.70 ++	2.29	1.78	1.63
Not applicable, not actually misued	~	~	~	~	~	~	4.36	~
Unknown	7.71	7.05	5.87	12.46 ++	9.68	7.49	7.49	9.48 ++
Total Count	412	1668	900	404	45	3429	3,920	3,197

Note: Standard errors available in Appendix Tables. Includes victims who provided a month and year of most recent occurrence. The percentage of victims not providing a month or year varied depending on the type of identity theft but was generally less than 1%.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Includes victims who provided a date in the future from when the interview occurred (August/September

Source: 2020 RTI/Amerispeak Identity Theft Survey.

2.5 Comparison to the ITS Estimates

- The identity theft prevalence rates generated through the AmeriSpeak collection were significantly higher across all types of identity theft than the estimates generated through the ITS. Although the rates for respondents interviewed via telephone were lower than the rates for respondents who completed the online survey, both were significantly higher than the 2018 ITS prevalence rates (see ***Table 18***).
- The differences in prevalence estimates between the AmeriSpeak collection and the ITS likely are due to the numerous methodological differences between the two collections. For example, if the presence of an interviewer has a suppression effect, this could account for, at least in part, higher estimates of identity theft in the online panel. The presentation of the surveys also varied between the two collections. The NCVS is presented as a crime survey and questions about identity theft follow questions about other experiences with crime; this could result in respondent fatigue or could condition the respondents to better understand the types of experiences of interest in the survey. In contrast, the AmeriSpeak collection was a standalone survey focused solely on identity theft. Another possible explanation for the differences in the magnitude of prevalence estimates is that the interviewer serves to clarify the questions and reduce the likelihood of false positive responses. Finally, the response rates for the ITS and the AmeriSpeak collection varied dramatically, with the ITS having considerably higher response rates. Lower response rates tend to be correlated with bias, meaning that the AmeriSpeak collection could suffer from topic saliency or other nonresponse bias resulting in an online sample of respondents that is more likely to have experienced identity theft than the general population. Unfortunately, it is not possible to determine which of the methodological differences contribute the greatest degree to the differences in estimates.
- Across all demographic groups, the online AmeriSpeak collection generated higher identity theft prevalence rates than the ITS (see ***Table 19***).
- This was also true across most demographics for AmeriSpeak respondents who participated via telephone interview. Among Hispanics, persons of other races, and person of two or more races, as well as persons younger than age 25, the differences with the ITS were not statistically significant. However, this is largely a product of small sample sizes and large standard errors.

Table 18. Prevalence of Identity Theft in the Past 12 Months, by Type of Identity Theft, Survey Administrator, and Mode

			NORC Version 1					
	2018 Census ITS*		Total		Web		Phone	
	Number of victims	Percent of all persons 16+	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/b	Number of victims	Percent of all respondents/b
Total	23,901,317	9.26 %	3,937	37.11 %+	3,813	37.97 %+	124	21.88 %+
Existing account								
Credit card	12,038,327	4.66	1,703	16.05 +	1,646	16.39 +	57	10.10 +
Bank	10,747,859	4.16	2,148	20.25 +	2,090	20.81 +	58	10.27 +
Other	2,496,609	0.97	1,675	15.79 +	1,635	16.28 +	39	6.97 +
New account	1,744,494	0.68	779	7.35 +	760	7.57 +	19	3.33 +
Personal information	957,039	0.37	507	4.78 +	487	4.85 +	20	3.53 +

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Based on the population of US residents age 16 or older.

b/Based on a representative sample of US residents age 18 or older.

Source: Bureau of Justice Statistics, Identity Theft Supplement, 2018; 2020 RTI/Amerispeak Identity Theft Survey.

Table 19. Persons Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics, Survey Administrator, and Mode

					NORC Version 1					
	2018 Census ITS*				Total		Web		Phone	
	Number of victims (weighted)	Percent of all persons 16+	Number of victims (unweighted)	Percent of all respondents	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a
Total	23,102,762	9.26 %	10,068	9.83 %	3,937	37.11 %+	3,813	37.97 %+	124	21.88 %+
Sex										
Male	11,536,820	9.22 %	4,703	9.81 %	1,931	37.69 %+	1,891	38.56 %+	40	18.13 %+
Female	12,364,497	9.30	5,365	9.85	2,006	36.56 +	1,922	37.40 +	84	24.23 +
Race/Hispanic origin/b										
White	17,077,303	10.44 %	7,773	10.78 %	2,329	34.97 %+	2,254	35.63 %+	75	22.48 %+
Black	2,163,284	7.01	788	7.17	460	36.40 +	434	38.18 +	27	20.71 +
Asian	1,298,128	8.05	428	8.56	178	36.21 +	177	36.36 +	1	20.07 +
Hispanic	2,803,187	6.59	876	6.97	816	46.14 +	804	46.81 +	12	23.41
Other	119,536	8.22	44	8.56	42	34.49 +	37	39.08 +	4	17.37
Two or more races	439,880	12.21	159	12.49	112	36.95 +	107	38.17 +	5	21.61
Age										
16-17	99,312	14.93 %	22	1.21	~	~ %+	~	~ %+	~	~ %
18–24	1,798,299	6.01	530	6.81	532	43.64 +	532	43.64 +	0	0.00
25–34	4,539,644	10.11	1,626	10.39	801	43.22 +	800	43.29 +	1	17.77
35–49	6,997,598	11.35	2,933	11.95	1,051	40.15 +	1,044	40.28 +	7	27.27 +
50–64	6,658,645	10.57	3,037	11.00	954	36.17 +	913	36.48 +	42	30.59 +
65 or older	3,807,820	7.50	1,920	7.68	598	26.23 +	524	27.85 +	74	18.60 +
Household income										
$24,999 or less	2,954,294	6.22 %	1,137	6.19 %	867	35.16 %+	815	37.23 %+	52	18.72 %+
$25,000–$49,999	4,470,915	6.74	1,850	7.11	1,000	36.19 +	956	36.59 +	44	29.28 +
$50,000–$74,999	4,319,302	9.04	1,836	9.68	748	36.98 +	731	37.32 +	17	26.51 +
$75,000 or more	12,156,807	12.60	5,245	13.43	1,322	39.36 +	1,310	39.93 +	11	14.91 +
Urbanicity										
Urban	8,115,717	9.37 %	3,153	10.06	3,430	37.62 %+	3,332	38.40 %+	97	22.11 %+
Non-urban	15,785,600	9.20	6,915	9.73	487	33.33 +	460	34.49 +	26	21.06 +
Unknown	~	~	~	~	20	65.07	20	65.07	0	0.00

Note: Standard errors are provided in appendix tables. Percentages are based on the number of persons in each category.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Based on a representative sample of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: Bureau of Justice Statistics, Identity Theft Supplement, 2018; 2020 RTI/Amerispeak Identity Theft Survey.

3. Recommendations for the 2021 ITS Based on Key Findings

Based on the findings from the AmeriSpeak testing, Version 2 appears to perform better than Versions 1 and 3 in terms of controlling for telescoping and eliminating attempted incidents (key goals of BJS's) while ensuring that victims of the misuse of social media accounts are captured in the estimates. Respondents appeared to understand the distinction between the lifetime and 12-month reference periods, and the dual reference period likely helped to control for some telescoping among victims who wanted to be able to share their experiences. Because Version 2 respondents were allowed to and did provide dates of most recent occurrence that were outside of the 12-month reference period, there is evidence that some telescoping still occurred despite the dual reference period. ***Table 20*** shows the potential impact on Version 2 estimates if respondents who did not provide a date of most recent occurrence or provided a date outside the reference were removed from the original prevalence rates based solely on the question of whether the incident occurred during the past 12 months. With the removal of these cases, which BJS could do during data analysis, Version 2 estimates are significantly lower than both Versions 1 and 3.

Table 20. Prevalence of Identity Theft in the Past 12 Months Accounting for Version 2 Victims Who Failed to Provide Dates of Occurrence or Who Provided Dates of Occurrence Outside the Reference Period, by Type of Identity Theft, victim race/Hispanic origin, and Instrument Version

	Version 1		Version 2 -ORIGINAL		Version 2 - NEW*		Version 3	
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims/b	Percent of all respondents/a	Number of victims	Percent of all respondents/a
Total	3,937	37.11 %++	3,494	31.98 %++	2,755	25.21 %	3,213	30.20 %++
Type of ID theft								
Existing account								
Credit card	1,703	16.05 ++	1,349	12.35 ++	1,088	9.96	1,484	13.94 ++
Bank	2,148	20.25 ++	1,641	15.02 ++	1,272	11.64	1,724	16.20 ++
Social media	~	~	1,338	12.25 ++	1,089	9.97	~	~
Other	1,675	15.79 ++	962	8.81 ++	740	6.77	1,093	10.27 ++
New account	779	7.35 ++	570	5.21 ++	395	3.61	455	4.27 ++
Personal information	507	4.78 ++	333	3.05 ++	225	2.06	400	3.75 ++
Race/Hispanic origin/c								
White	2,329	21.96 ++	1,987	18.19 ++	1,575	14.42	1,808	16.99 ++
Black	460	4.34 ++	506	4.63 ++	392	3.58	432	4.06
Asian	178	1.68 ++	123	1.12 +	95	0.87	123	1.16 +
Hispanic	816	7.69 ++	721	6.60 ++	565	5.17	696	6.54 ++
Other	42	0.39 ++	28	0.26	23	0.21	38	0.35 +
Two or more races	112	1.05	129	1.18	105	0.96	116	1.09

Note: Standard errors provided in Appendix Tables.

~Not applicable.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

b/Includes only victims who provided dates of occurrence within the reference period.

c/White, black, Asian other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Although Version 2 is the recommended version, there are several downsides to moving to Version 2 that should be considered. First, given the difference between the estimates for Versions 1 and 2, it appears that switching to Version 2 would result in a break of series. Because of the many changes to the Version 2 instrument, it would be difficult to quantify the exact magnitude of expected change. Another challenge with Version 2, though considerably less significant, is that the coding on the backend is quite complicated. If BJS switches to Version 2, it would be prudent to ask the Census Bureau to keep programming variables (e.g., Check Items, any variables created to populate the autofills used for determining most recent incident) on the files to simplify the recodes. Finally, Version 2 does cause slightly more burden on respondents. ***Table 21*** shows the mean and median times that respondents spent completing each of the survey versions.

Although Version 3 also appeared to result in lower prevalence rates than Version 1, possibly due to the exclusion of attempted incidents, these findings should be interpreted with caution given findings from the cognitive interviews that suggested that Version 3 may be inadvertently screening out victims who have experienced the completed misuse of an existing social media account. If BJS were to decide to use Version 3 instead of Version 2, it would be important to separate social media accounts from the "other existing account" category.

Table 21. Average and Median Number of Minutes Spent on the Survey, by Platform, Survey Mode, and Instrument Version (unweighted)

	Excluding speeders/skippers			Including speeders/skippers			Victims only		
	N	Mean	Median	N	Mean	Median	N	Mean	Median
Total	32,177	6.16	5.00	34,527	5.90	4.00	12,611	7.67	6.00
Panel									
Amerispeak	10,962	4.72	4.00	12,350	4.34	3.00	3,592	5.83	5.00
Lucid	11,210	6.19	5.00	12,097	6.01	5.00	4,240	7.13	5.00
MTurk	10,005	7.70	6.00	10,080	7.68	6.00	4,779	9.54	7.00
Mode									
Web	30,901	6.12	4.00	33,208	5.86	4.00	12,345	7.63	6.00
Phone	1,276	7.17	6.00	1,319	7.07	6.00	266	9.85	9.00
Version									
1	10,609	5.89	4.00	11,402	5.64	4.00	4,653	7.09	5.00
2	10,926	6.49	5.00	11,685	6.23	5.00	3,831	8.28	6.00
3	10,642	6.10	4.00	11,440	5.83	4.00	4,127	7.76	6.00

Source: 2020 RTI/Amerispeak Identity Theft Survey.

4. Methodology

NORC conducted the 2020 RTI/AmeriSpeak Identity Theft Survey on behalf of RTI and BJS using NORC's AmeriSpeak® Panel, Lucid's nonprobability online opt-in panel, and MTurk for the sample sources. The research was done to evaluate the effectiveness of three different screener options for a larger survey about identity theft conducted by RTI for BJS. This study was offered in English only and conducted via both web and phone.

4.1 Sampling

4.1.1 AmeriSpeak

A general population sample of U.S. adults age 18 and older was selected from NORC's AmeriSpeak Panel for this study. Survey respondents were those who gave consent to take the survey and met the following screening criteria: age 18 or older, English speaking, and living in the United States.

The sample for a specific study is selected from the AmeriSpeak Panel using sampling strata (48 in total) based on age, race/Hispanic ethnicity, education, and gender. The size of each stratum of the selected sample is determined by its population distribution. In addition, sample selection takes into account expected differential survey completion rates by demographic groups so that the set of panel members with completed interviews for a study is a representative sample of the target population. Even if a panel household has more than one active adult panel member, only one adult in the household is eligible for selection (using random within-household sampling). Panelists selected for an AmeriSpeak study earlier in the same business week are not eligible for sample selection until the following business week.

The AmeriSpeak panel sample was supplemented with respondents from the Lucid nonprobability online opt-in panel and from MTurk workers.

4.1.2 MTurk

On the crowdsourcing platform Amazon MTurk, any work—ranging from audio transcription to receipt categorization to survey participation—will be created and published by a "requester" (e.g., social science researcher) in a format called Human Intelligence Task (HIT). When the HIT is published on the platform, interested MTurk workers can accept to complete the task in exchange for the designated incentives once the requester approves the completed task.

The MTurk platform gives requesters a great deal of control over the recruitment of workers for survey participation by allowing researchers to specify the geographic location and the past-performance benchmarks to determine the eligibility threshold for completing the HIT. Specifically, the past-performance benchmarks (e.g., past HIT approval rate, number of past HITs approved) enable researchers to recruit quality participants who tend to put in the effort to produce good quality of data in the context of scientific research (Hsieh et al., 2018; Stambaugh et al., 2018).

Our MTurk recruitment strategy was designed to use a very high threshold of past performance as the eligibility criteria at the beginning of data collection, followed by an iterative adjustment of the eligibility criteria to gradually lower the threshold and allow more workers to participate in the survey. Workers who accepted the survey participation HIT were redirected to participate in our web survey. Those who completed the survey and successfully submitted the completion notice with the MTurk-required verification received $1 for participating.

Additionally, RTI’s past experiences with MTurk were leveraged by soliciting survey participation from all workers who had participated in our past research projects via MTurk recruitment. The MTurk protocol also included mechanisms to verify survey completion and to prevent workers from accessing and recompleting the survey.

4.2 Fielding

4.2.1 AmeriSpeak

A small sample of English-speaking Lucid web-mode panelists were invited on July 10, 2020, for a pretest. In total, NORC collected 168 pretest interviews. The initial data from the pretest was reviewed by NORC and a delivered to RTI.

No change was made before fielding the Main survey to collect the Main interviews. In total, NORC collected 32,177 interviews—30,901 by web mode and 1,276 by phone mode—during the July 16, 2020, through August 4, 2020, field period.

4.2.1.1 Response Rate Reporting for AmeriSpeak Sample

- Weighted AAPOR RR3 recruitment rate: 20.97%
- Weighted household retention rate: 80.37%
- Screener completion rate: 34.72%
- Survey completion rate: 96.90%
- Weighted AAPOR RR3 cumulative response rate: 5.67%

4.2.1.2 Gaining Cooperation of AmeriSpeak Panelists for the Study

To encourage study cooperation, NORC sent email reminders to sampled web-mode panelists on Tuesday, July 21, 2020. To administer the phone survey, NORC dialed the sampled phone-mode panelists throughout the field period. Panelists were offered the cash equivalent of $2 for completing the survey.

4.2.2 MTurk

Data collection for the MTurk recruitment started on July 16, 2020, and concluded on July 30, 2020. It started with a "soft" launch of recruiting 50 workers who had 100% past HIT approval ratings and had not participated in any past RTI research projects. Once data were reviewed to ensure the instrument was working as intended, an invitation was sent out to 3,566 past participants who had provided us with good quality survey response data based on reviews of response patterns for falsification and survey completion times. These participants were sent an invitation email with a direct link to the "RTI past-participant recruitment HIT"; 1,526 completed the survey (see ***Table 22***).

RTI also published the survey recruitment HIT on the MTurk platform to solicit participation from all MTurk workers who had passed our high eligibility threshold of past performance. To ensure the recruitment HIT would be placed at the top of the MTurk worker feed on their dashboards, RTI sequentially published a total of eight recruitment HITs with a fulfillment quota of 500 to 2000. When the pace of completion slowed down significantly, the HIT was closed and then re-published as a new recruitment HIT. RTI also evaluated the eligibility threshold of past performance based on the iterative adjustment strategy. The purpose of establishing the threshold was to ensure that only workers with a proven track record of successfully completed tasks could complete the survey. The lowest eligibility threshold for the final HIT prior to achieving the recruitment goal was a 98% approval rate or better for all work completed on MTurk with a minimum of 50 approved HITs.

Once the HITs were reviewed, workers were approved or, if rejected, were tagged to prevent them from participating in future HITs from the same study. A total of 10,164 workers participated in the survey with a final sample 10,062 workers after validating the survey completion and engaging in data cleaning.

Table 22. Detailed Breakdown of the Survey Recruitment HITs

	Number of Submissions	Number of Approvals	Approval Rate Based on HIT
Invited	1,526	1,515	99.3%
General 0	50	49	98.0%
General 1	500	497	99.4%
General 2	1,000	982	98.2%
General 3	2,000	1,976	98.8%
General 4	1,500	1,484	98.9%
General 5	53	53	100.0%
General 6	102	101	99.0%
General 7	1,897	1,886	99.4%
General 8	1,500	1,483	98.9%

Survey data review	36	36	100.0%
Total	10,164	10,062	99.0%

4.2.3 Tables Presenting Sample Sizes by Mode and Platform

Tables 1 and 2 at the beginning of the report show the unweighted sample characteristics by mode of completion and sample platform. ***Tables 23*** and ***24*** show the unweighted prevalence rates of the different types of identity theft, mode and platform. ***Tables 25*** and ***26*** show the unweighted prevalence rate of identity theft overall, by demographic characteristics of victims and by mode and platform.

Table 23. Unweighted Prevalence of Identity Theft in the Past 12 Months, by Type of Identity Theft and Mode

	Total		Web		Phone	
	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a
Total	12,611	39.19 %	12,345	39.95 %	266	20.85 %
Existing account						
Credit card	6,087	18.92	5,961	19.29	126	9.87
Bank	7,122	22.13	7,003	22.66	119	9.33
Social media	1,613	5.01	1,587	5.14	26	2.04
Other	5,344	16.61	5,286	17.11	58	4.55
New account	3,759	11.68	3,724	12.05	35	2.74
Personal information	3,293	10.23	3,263	10.56	30	2.35

Note: Standard errors provided in Appendix Tables.

a/Based on a representative sample of the population of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 24. Unweighted Prevalence of Identity Theft in the Past 12 Months, by Type of Identity Theft and Platform

	Total		AmeriSpeak		Lucid		MTurk	
	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a
Total	12,611	39.19 %	3,592	32.77 %	4,240	37.82 %	4,779	47.77 %
Existing account								
Credit card	6,087	18.92	1,608	14.67	1,971	17.58	2,508	25.07
Bank	7,122	22.13	1,549	14.13	2,653	23.67	2,920	29.19
Social media	1,613	5.01	419	3.82	526	4.69	668	6.68
Other	5,344	16.61	1,050	9.58	1,845	16.46	2,449	24.48
New account	3,759	11.68	489	4.46	1,415	12.62	1,855	18.54
Personal information	3,293	10.23	337	3.07	1,273	11.36	1,683	16.82

a/Based on a representative sample of the population of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 25. Unweighted Persons Age 18 or Older Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics and Mode

	Total		Web		Phone	
	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a
Total	12,611	39.19 %	12,345	39.95 %	266	20.85 %
Sex						
Male	6,367	40.73 %	6,274	41.33 %	93	20.58 %
Female	6,244	37.74	6,071	38.62	173	21.00
Race/Hispanic origin*						
White	7,062	34.42 %	6,904	35.07 %	158	18.97 %
Black	1,560	43.17	1,504	44.86	56	21.46
Other	489	36.44	485	36.41	4	40.00
Hispanic	3,024	55.42	3,006	55.79	18	26.09
Two or more races	121	34.87	111	35.92	10	26.32
Asian	355	39.49	335	40.17	20	30.77
Age						
18–24	1,248	43.71 %	1,248	43.79 %	0	0.00 %
25–34	3,607	48.32	3,604	48.38	3	20.00
35–49	3,728	44.63	3,716	44.73	12	26.09
50–64	2,467	33.31	2,382	33.54	85	27.96
65 or older	1,561	25.60	1,395	26.87	166	18.32
Household income						
$24,999 or less	2,326	36.96 %	2,221	38.51 %	105	19.92 %
$25,000–$49,999	3,288	38.74	3,207	39.56	81	21.32
$50,000–$74,999	2,703	40.09	2,669	40.54	34	21.52
$75,000 or more	4,294	40.30	4,248	40.68	46	21.80

a/Based on a representative sample of the population of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 26. Unweighted Persons Age 18 or Older Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics and Platform

	Total		AmeriSpeak		Lucid		MTurk	
	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a	Number of victims	Percent of respondents/a
Total	12,611	39.19 %	3,592	32.77 %	4,240	37.82 %	4,779	47.77 %
Sex								
Male	6,367	40.73 %	1,669	31.97 %	2,155	41.27 %	2,543	49.01 %
Female	6,244	37.74	1,923	33.50	2,085	34.82	2,236	46.43
Race/Hispanic origin*								
White	7,062	34.42 %	2,206	29.63 %	2,326	33.79 %	2,530	40.89 %
Black	1,560	43.17	569	38.73	567	42.89	424	51.52
Other	489	36.44	148	42.29	132	39.52	209	31.76
Hispanic	3,024	55.42	447	40.02	1,107	46.77	1,470	74.51
Two or more races	121	34.87	66	35.87	30	30.30	25	39.06
Asian	355	39.49	156	39.39	78	38.24	121	40.47
Age								
18–24	1,248	43.71 %	190	40.86 %	710	45.48 %	348	41.98 %
25–34	3,607	48.32	700	37.98	870	49.77	2,037	52.58
35–49	3,728	44.63	669	36.92	1,406	45.52	1,653	47.87
50–64	2,467	33.31	1,081	34.11	779	27.98	607	41.78
65 or older	1,561	25.60	952	25.92	475	23.42	134	33.84
Household income								
$24,999 or less	2,326	36.96 %	714	33.71 %	973	34.55 %	639	46.99 %
$25,000–$49,999	3,288	38.74	909	32.95	1,049	34.55	1,330	49.41
$50,000–$74,999	2,703	40.09	653	30.80	760	35.95	1,290	51.44
$75,000 or more	4,294	40.30	1,316	33.19	1,458	44.94	1,520	44.12

a/Based on a representative sample of the population of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

4.3 Statistical Weighting

Statistical weights for the study eligible respondents were initially calculated using panel base sampling weights.

Panel base sampling weights for all sampled housing units are computed as the inverse of probability of selection from the NORC National Frame (i.e., the sampling frame used to sample housing units for AmeriSpeak) or an address-based sample. The sample design and recruitment protocol for the AmeriSpeak Panel involves subsampling initial nonrespondent housing units, which are selected for in-person follow-up interviews. The subsample of housing units that are selected for the nonresponse follow-up (NRFU) have their panel base sampling weights inflated by the inverse of the subsampling rate. The base sampling weights are further adjusted to account for unknown eligibility and nonresponse among eligible housing units. The household-level nonresponse-adjusted weights are then post-stratified to external counts for number of households obtained from the CPS. Then, these household-level post-stratified weights are assigned to each eligible adult in every recruited household. A person-level nonresponse adjustment accounts for all nonresponding adults within a recruited household.

Finally, panel weights are raked to external population totals associated with age, sex, education, race/Hispanic ethnicity, housing tenure, telephone status, and Census Division. The external population totals are obtained from the CPS. The weights adjusted to the external population totals are the *final panel weights*.

The following variables and categories were used for panel weighting:

- Age: 18–24, 25–29, 20–39, 40–49, 50–59, 60–64, and 65+
- Gender: Male and Female
- Census Division: New England, Middle Atlantic, East North Central, West North Central, South Atlantic, East South Central, West South Central, Mountain, and Pacific
- Race/Ethnicity: Non-Hispanic White, Non-Hispanic Black, Hispanic, and Non-Hispanic Other
- Education: Less Than High School, High School/GED, Some College, and BA and Above
- Housing Tenure: Home Owner and Other
- Household Phone Status: Cell Phone Only, Dual User, and Landline Only/Phoneless

Study-specific base sampling weights are derived using a combination of the final panel weight and the probability of selection associated with the sampled panel member. Because not all sampled panel members respond to the survey interview, an adjustment is needed to account and adjust for survey nonrespondents. This adjustment decreases potential nonresponse bias associated with sampled panel members who did not complete the survey interview for the study. Thus, the nonresponse-adjusted survey weights for the study are adjusted via a raking ratio method to general population totals associated with the following topline sociodemographic characteristics: age, sex, education, race/Hispanic ethnicity, and Census Division; and the following sociodemographic interactions: age x gender, age x race/ethnicity, and race/ethnicity x gender.

The study-specific post-stratification weighting variables and the variable categories are as follows:

- Age: 18–24, 25–29, 20–39, 40–49, 50–59, 60–64, and 65+
- Gender: Male and Female
- Census Division: New England, Middle Atlantic, East North Central, West North Central, South Atlantic, East South Central, West South Central, Mountain, and Pacific
- Race/Ethnicity: Non-Hispanic White, Non-Hispanic Black, Hispanic, and Non-Hispanic Other

- Education: Less Than High School, High School/GED, Some College, and BA and Above
- Age x Gender: 18–34 Male, 18–34 Female, 35–49 Male, 35–49 Female, 50–64 Male, 50–64 Female, 65+ Male, and 65+ Female
- Age x Race/Ethnicity: 18–34 Non-Hispanic White, 18–34 All Other, 35–49 Non-Hispanic White, 35–49 All Other, 50–64 All Other, 50–64 All Other, 65+ Non-Hispanic White, and 65+ All Other
- Race/Ethnicity x Gender: Non-Hispanic White Male, Non-Hispanic White Female, All Other Male, and All Other Female

The weights adjusted to the external population totals are the *final study weights*. Raking and re-raking is done during the weighting process such that the weighted demographic distribution of the survey completes resemble the demographic distribution in the target population. The assumption is that the key survey items are related to the demographics. Therefore, by aligning the survey respondent demographics with the target population, the key survey items should also be in closer alignment with the target population.

Table 27. Census Current Population Survey (Feb 2020) Used for Benchmarking

Age	
18–24	11.48%
25–29	9.05%
30–39	17.31%
40–49	15.80%
50–59	16.61%
60–64	8.27%
65+	21.49%
Gender	
Male	48.30%
Female	51.70%
Census Division	
New England	4.69%
Middle Atlantic	12.75%
East North Central	14.30%
West North Central	6.44%
South Atlantic	20.29%
East South Central	5.80%
West South Central	11.92%
Mountain	7.51%
Pacific	16.32%

Education	
No High School	9.77%
Diploma	28.25%
High School	27.73%
Diploma	34.26%
Some College	
College Degree	
Race/Ethnicity	
Non-Hispanic White	62.79%
Non-Hispanic Black	11.93%
Hispanic	16.66%
Non-Hispanic Others	8.62%

4.4 Weighting

NORC calculated panel weights for the completed AmeriSpeak Panel and nonprobability online interviews. In this section, we first describe the calculation of the weights for the AmeriSpeak sample and then the statistical corrections made to the nonprobability sample via NORC's TrueNorth calibration weighting service.

4.4.1 AmeriSpeak Sample

Calculating the weights for the AmeriSpeak Panel interviews generally involves the following sequential steps: (1) incorporating the appropriate probability of selection and (2) incorporating nonresponse and raking ratio adjustments (to population benchmarks).

For the AmeriSpeak Panel interviews, study-specific base weights are derived from the final panel weight and the probability of selection from the panel under the study sample design. Because not all sampled panel members responded to the interview request, an adjustment is needed to compensate for survey nonrespondents. This adjustment decreases potential nonresponse bias associated with sampled panel members who did not respond to the interview for the study. A weighting class approach is used to adjust the weights for survey respondents to represent nonrespondents.

At this stage of weighting, any extreme weights were trimmed using a power transformation to minimize the mean squared error. Weights were then re-raked to the same population totals.

4.4.2 TrueNorth Calibration for Nonprobability Sample

To incorporate the nonprobability sample, NORC used TrueNorth calibration, which is an innovative, hybrid calibration approach developed at NORC based on small-area estimation methods to explicitly account for potential bias associated with the nonprobability sample. The purpose of TrueNorth calibration is to adjust the weights for the nonprobability sample to bring weighted distributions of the nonprobability sample in line with the population distribution for characteristics correlated with the survey variables. Such calibration adjustments help to reduce potential bias, yielding more accurate population estimates.

The weighted AmeriSpeak sample and the calibrated nonprobability sample were used to develop a small-area model to support domain-level estimates, where the domains were defined by race/ethnicity, age, and gender. The dependent variables for the models were key survey variables. The model included covariates, domain-level random effects, and sampling errors. The covariates were external data available from other national surveys such as health insurance, internet access, voting behavior, and housing type from the U.S. Census Bureau’s ACS or CPS.

Finally, the combined AmeriSpeak and nonprobability sample weights were derived so that the weighted estimate reproduced the small domain estimates (derived using the small area model) for key survey variables for the combined sample.

4.4.3 Design Effect and Sampling Margin of Error Calculations

Study design effect:

- Screener Version 1: 1.44808
- Screener Version 2: 1.50797
- Screener Version 3: 1.53612

Study margin of error:

- Screener Version 1: +/- 1.23%
- Screener Version 2: +/- 1.24%
- Screener Version 3: +/- 1.27%

Under TrueNorth, the margins of error were estimated from the root mean-squared error associated with the small area model and other statistical adjustments. A TrueNorth estimate of margin of error is a measure of uncertainty that accounts for the variability associated with the probability sample as well as the potential bias associated with the nonprobability sample.

The final weighted sample for each instrument version is presented in Table 3 in the introduction of the report.

4.5 Assessment of Item Nonresponse, Speeders, and Skippers

Tables 28 through ***33*** show the levels of item missingness for key variables for each of the three instrument versions, by mode of completion and platform. Levels of missingness are shown both including and excluding speeders and skippers. Respondents were not included in the final weighted sample if their survey completion time was below the minimum established threshold or their number of items skipped was above the maximum threshold. Overall, for the majority of items across all three versions, levels of item missingness were low.

Table 34 shows the average number of missing or "don't know" responses, by respondent demographics and instrument version.

Table 28. Instrument Version 1 Item Nonresponse, by Key Items and Survey Platform

	Total			AmeriSpeak			Lucid			MTurk			Total (excluding speeders and skippers)*		
	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent
Q1	38	10,738	0.35 %	15	3,658	0.41 %	8	3,764	0.21 %	15	3,316	0.45 %	31	10,609	0.29 %
Q1a	85	10,095	0.84	26	3,460	0.75	37	3,411	1.08	22	3,224	0.68	84	9,989	0.84
Q2	236	10,738	2.20	57	3,658	1.56	138	3,764	3.67	41	3,316	1.24	224	10,609	2.11
Q2a	15	8,775	0.17	3	3,124	0.10	11	936	1.18	1	493	0.20	14	1,933	0.72
Q3	51	10,738	0.47	14	3,123	0.45	19	2,794	0.68	15	2,865	0.52	45	8,688	0.52
Q4	49	10,738	0.46	26	3,658	0.71	14	3,764	0.37	11	3,316	0.33	38	10,609	0.36
Q5	59	10,738	0.55	23	3,658	0.63	12	3,764	0.32	14	3,316	0.42	35	10,609	0.33
Q7	59	10,738	0.55	40	3,658	1.09	10	3,764	0.27	9	3,316	0.27	44	10,609	0.41
Q9a	109	4,667	2.34	79	1,350	5.85	23	1,589	1.45	7	1,728	0.41	103	4,635	2.22
Q9b	84	4,667	1.80	48	1,350	3.56	28	1,589	1.76	8	1,728	0.46	79	4,635	1.70
Q10	313	4,667	6.71	116	1,350	8.59	118	1,589	7.43	79	1,728	4.57	311	4,635	6.71

Note: Number missing includes 'don't know' responses. Based on unweighted data.

*Excludes respondents who did not meet the data quality thresholds for inclusion in the final sample.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 29. Instrument Version 2 Item Nonresponse, by Key Items and Survey Platform

	Total			AmeriSpeak			Lucid			MTurk			Total (excluding speeders and skippers)*		
	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent
Q1	26	11037	0.24 %	12	3813	0.31 %	6	3775	0.16 %	8	3449	0.23 %	16	10926	0.15 %
Q2	29	10670	0.27	9	3728	0.24	14	3552	0.39	6	3390	0.18	27	10576	0.26
Q3	12	4312	0.28	4	1350	0.30	4	1327	0.30	4	1635	0.24	10	4265	0.23
Q4a	14	1916	0.73	9	394	2.28	5	701	0.71	0	821	0.00	13	1897	0.69
Q4b	19	1916	0.99	6	394	1.52	9	701	1.28	4	821	0.49	18	1897	0.95
Q5	30	11037	0.27	12	3813	0.31	9	3775	0.24	9	3449	0.26	18	10926	0.16
Q6	36	9528	0.38	8	3447	0.23	19	3054	0.62	9	3449	0.26	35	9455	0.37
Q7	18	4279	0.42	7	1564	0.45	4	1196	0.33	7	1519	0.46	16	4243	0.38
Q8a	17	1680	1.01	14	444	3.15	3	517	0.58	0	716	0.00	15	1664	0.90
Q8b	19	1680	1.13	8	444	1.80	7	517	1.35	4	716	0.56	18	1664	1.08
Q9	38	11037	0.34	24	3813	0.63	13	3775	0.34	1	3449	0.03	25	10926	0.23
Q10	33	3368	0.98	9	1028	0.88	9	1042	0.86	15	1298	1.16	32	3346	0.96
Q10a	18	1626	1.11	12	425	2.82	3	529	0.57	3	672	0.45	16	1613	0.99
Q10b	19	1626	1.17	7	425	1.65	7	529	1.32	5	672	0.74	18	1613	1.12
Q11	51	11037	0.46	24	3813	0.63	11	3775	0.29	16	3449	0.46	34	10926	0.31
Q12	18	2432	0.74	5	640	0.78	8	730	1.10	5	1062	0.47	17	2402	0.71
Q14a	13	1286	1.01	6	249	2.41	4	396	1.01	3	641	0.47	13	1277	1.02
Q14b	19	1286	1.48	7	249	2.81	5	396	1.26	7	641	1.09	19	1277	1.49
Q15	58	11037	0.53	26	3813	0.68	12	3775	0.32	20	3449	0.58	43	10926	0.39
Q16	12	1778	0.67	2	411	0.49	1	579	0.17	9	788	1.14	12	1759	0.68
Q18a	6	861	0.70	4	105	3.81	0	289	0.00	2	467	0.43	6	854	0.70
Q18b	6	861	0.70	2	105	1.90	2	289	0.69	2	467	0.43	6	854	0.70
Q19	68	11037	0.62	30	3813	0.79	20	3775	0.53	18	3449	0.52	49	10926	0.45
Q20	6	1527	0.39	0	320	0.00	2	492	0.41	4	715	0.56	6	1509	0.40
Q22a	6	732	0.82	2	58	3.45	2	250	0.80	2	424	0.47	6	730	0.82
Q22b	19	732	2.60	4	58	6.90	8	250	3.20	7	424	1.65	19	730	2.60
Q25a	58	3805	1.52	31	1112	2.79	20	1227	1.63	7	1466	0.48	55	3776	1.46
Q25b	61	3805	1.60	31	1112	2.79	22	1227	1.79	8	1466	0.55	58	3776	1.54
Q26	244	3805	6.41	94	1112	8.45	91	2548	3.57	59	1466	4.02	237	3776	6.28

Note: Number missing includes 'don't know' responses. Based on unweighted data.

*Excludes respondents who did not meet the data quality thresholds for inclusion in the final sample.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 30. Instrument Version 3 Item Nonresponse, by Key Items and Survey Platform

	Total			AmeriSpeak			Lucid			MTurk			Total (excluding speeders and skippers)*		
	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent
Q1	34	10758	0.32 %	12	3706	0.32 %	13	3737	0.35 %	9	3315	0.27 %	27	10642	0.25 %
Q1a	39	10174	0.38	10	3531	0.28	16	3425	0.47	13	3218	0.40	37	10080	0.37
Q2	197	10758	1.83	39	3706	1.05	121	3737	3.24	37	3315	1.12	180	10642	1.69
Q2a	28	8837	0.32	5	3218	0.16	9	2741	0.33	14	2878	0.49	27	8758	0.31
Q3	76	10758	0.71	29	3706	0.78	26	3737	0.70	21	3315	0.63	61	10642	0.57
Q4	40	10758	0.37	19	3706	0.51	14	3737	0.37	7	3315	0.21	25	10642	0.23
Q5	61	10758	0.57	23	3706	0.62	21	3737	0.56	17	3315	0.51	45	10642	0.42
Q9a	155	4128	3.75	88	1120	7.86	47	1415	3.32	20	1593	1.26	147	4111	3.58
q9b	145	4128	3.51	71	1120	6.34	54	1415	3.82	20	1593	1.26	138	4111	3.36
Q10	34	4128	0.82	90	1120	8.04	138	1415	9.75	75	1593	4.71	297	4111	7.22

Note: Number missing includes 'don't know' responses. Based on unweighted data.

*Excludes respondents who did not meet the data quality thresholds for inclusion in the final sample.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 31. Instrument Version 1 Item Nonresponse, by Key Items and Mode

	Total			Web			Phone			Total (excluding speeders and skippers)*		
	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent
Q1	38	10738	0.35 %	36	10302	0.35 %	2	436	0.46 %	31	10609	0.29 %
Q1a	85	10095	0.84	81	9726	0.83	4	369	1.08	84	9989	0.84
Q2	236	10738	2.20	235	10302	2.28	1	436	0.23	224	10609	2.11
Q2a	15	8775	0.17	15	1854	0.81	0	109	0.00	14	1933	0.72
Q3	51	10738	0.47	47	8448	0.56	1	334	0.30	45	8688	0.52
Q4	49	10738	0.46	47	10302	0.46	4	436	0.92	38	10609	0.36
Q5	59	10738	0.55	45	10302	0.44	4	436	0.92	35	10609	0.33
Q7	59	10738	0.55	53	10302	0.51	6	436	1.38	44	10609	0.41
Q9a	109	4667	2.34	85	4560	1.86	24	107	22.43	103	4635	2.22
Q9b	84	4667	1.80	80	4560	1.75	4	107	3.74	79	4635	1.70
Q10	313	4667	6.71	302	4560	6.62	11	107	10.28	311	4635	6.71

Note: Number missing includes 'don't know' responses. Based on unweighted data.

*Excludes respondents who did not meet the data quality thresholds for inclusion in the final sample.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 32. Instrument Version 2 Item Nonresponse, by Key Items and Mode

	Total			Web			Phone			Total (excluding speeders and skippers)*		
	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent
Q1	26	11037	0.24 %	26	10621	0.24 %	0	416	0.00 %	16	10926	0.15 %
Q2	29	10670	0.27	28	10286	0.27	1	384	0.26	27	10576	0.26
Q3	12	4312	0.28	11	4204	0.26	1	108	0.93	10	4265	0.23
Q4a	14	1916	0.73	10	1881	0.53	4	35	11.43	13	1897	0.69
Q4b	19	1916	0.99	19	1881	1.01	0	35	0.00	18	1897	0.95
Q5	30	11037	0.27	30	10621	0.28	0	416	0.00	18	10926	0.16
Q6	36	9528	0.38	36	9183	0.39	0	345	0.00	35	9455	0.37
Q7	18	4279	0.42	16	4170	0.38	2	109	1.83	16	4243	0.38
Q8a	17	1680	1.01	13	1643	0.79	4	37	10.81	15	1664	0.90
Q8b	19	1680	1.13	18	1643	1.10	1	37	2.70	18	1664	1.08
Q9	38	11037	0.34	29	10621	0.27	9	416	2.16	25	10926	0.23
Q10	33	3368	0.98	31	3322	0.93	2	46	4.35	32	3346	0.96
Q10a	18	1626	1.11	12	1600	0.75	6	26	23.08	16	1613	0.99
Q10b	19	1626	1.17	18	1600	1.13	1	26	3.85	18	1613	1.12
Q11	51	11037	0.46	48	10621	0.45	3	416	0.72	34	10926	0.31
Q12	18	2432	0.74	17	2397	0.71	1	416	0.24	17	2402	0.71
Q14a	13	1286	1.01	11	1276	0.86	2	10	20.00	13	1277	1.02
Q14b	19	1286	1.48	19	1276	1.49	0	10	0.00	19	1277	1.49
Q15	58	11037	0.53	55	10621	0.52	3	416	0.72	43	10926	0.39
Q16	12	1778	0.67	11	1743	0.63	1	35	2.86	12	1759	0.68
Q18a	6	861	0.70	3	852	0.35	3	9	33.33	6	854	0.70
Q18b	6	861	0.70	5	852	0.59	1	9	11.11	6	854	0.70
Q19	68	11037	0.62	66	10621	0.62	2	416	0.48	49	10926	0.45
Q20	6	1527	0.39	6	1503	0.40	0	24	0.00	6	1509	0.40
Q22a	6	732	0.82	6	727	0.83	0	5	0.00	6	730	0.82
Q22b	19	732	2.60	19	727	2.61	0	5	0.00	19	730	2.60
Q25a	58	3805	1.52	56	3736	1.50	2	69	2.90	55	3776	1.46
Q25b	61	3805	1.60	61	3736	1.63	0	69	0.00	58	3776	1.54
Q26	244	3805	6.41	240	3736	6.42	4	69	5.80	237	3776	6.28

Note: Number missing includes 'don't know' responses. Based on unweighted data.

*Excludes respondents who did not meet the data quality thresholds for inclusion in the final sample.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 33. Instrument Version 3 Item Nonresponse, by Key Items and Mode

	Total			Web			Phone			Total (excluding speeders and skippers)*		
	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent	Number missing	Number eligible	Percent
Q1	34	10758	0.32 %	33	10320	0.32 %	1	438	0.23 %	27	10642	0.25 %
Q1a	39	10174	0.38	38	9799	0.39	1	375	0.27	37	10080	0.37
Q2	197	10758	1.83	196	10320	1.90	1	438	0.23	180	10642	1.69
Q2a	28	8837	0.32	28	8492	0.33	0	345	0.00	27	8758	0.31
Q3	76	10758	0.71	74	10320	0.72	2	438	0.46	61	10642	0.57
Q4	40	10758	0.37	39	10320	0.38	1	438	0.23	25	10642	0.23
Q5	61	10758	0.57	61	10320	0.59	0	438	0.00	45	10642	0.42
Q9a	155	4128	3.75	140	4049	3.46	15	79	18.99	147	4111	3.58
Q9b	145	4128	3.51	141	4049	3.48	4	79	5.06	138	4111	3.36
Q10	34	4128	0.82	296	4049	7.31	7	79	8.86	297	4111	7.22

Note: Number missing includes 'don't know' responses. Based on unweighted data.

*Excludes respondents who did not meet the data quality thresholds for inclusion in the final sample.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table 34. Average Number of Missing or "Don't Know" Responses, by Respondent Demographics and Instrument Version (unweighted)

	Total			AmeriSpeak			Lucid			MTurk		
	Version 1	Version 2	Version 3	Version 1	Version 2	Version 3	Version 1	Version 2	Version 3	Version 1	Version 2	Version 3
Total	0.10	0.07	0.09	0.11	0.08	0.09	0.11	0.06	0.11	0.07	0.06	0.07
Sex												
Male	0.10	0.07	0.09	0.11	0.07	0.08	0.12	0.06	0.12	0.07	0.07	0.08
Female	0.10	0.07	0.09	0.12	0.09	0.09	0.10	0.06	0.11	0.07	0.04	0.06
Race/Hispanic origin*												
White	0.08	0.05	0.06	0.09	0.05	0.06	0.09	0.05	0.09	0.05	0.04	0.05
Black	0.15	0.12	0.13	0.18	0.15	0.13	0.15	0.11	0.16	0.12	0.08	0.09
Other	0.19	0.09	0.11	0.24	0.09	0.16	0.17	0.16	0.05	0.09	0.00	0.08
Hispanic	0.12	0.10	0.15	0.11	0.14	0.19	0.13	0.08	0.16	0.12	0.11	0.13
Two or more races	0.11	0.08	0.09	0.17	0.11	0.08	0.10	0.08	0.12	0.04	0.03	0.07
Asian	0.09	0.06	0.10	0.13	0.13	0.23	0.14	0.06	0.12	0.04	0.03	0.03
Age												
18–24	0.15	0.09	0.15	0.24	0.07	0.30	0.17	0.12	0.17	0.03	0.05	0.03
25–34	0.10	0.08	0.11	0.13	0.10	0.13	0.13	0.08	0.14	0.07	0.07	0.08
35–49	0.10	0.07	0.09	0.13	0.09	0.08	0.11	0.06	0.12	0.07	0.05	0.07
50–64	0.09	0.06	0.07	0.10	0.08	0.07	0.08	0.04	0.08	0.07	0.05	0.06
65 or older	0.08	0.05	0.06	0.09	0.06	0.06	0.06	0.04	0.07	0.02	0.06	0.02
Household income												
$24,999 or less	0.14	0.10	0.13	0.17	0.14	0.13	0.14	0.08	0.14	0.10	0.07	0.10
$25,000–$49,999	0.10	0.06	0.10	0.12	0.07	0.11	0.09	0.05	0.12	0.09	0.07	0.07
$50,000–$74,999	0.08	0.06	0.08	0.08	0.06	0.07	0.10	0.06	0.10	0.06	0.06	0.07
$75,000 or more	0.08	0.06	0.07	0.09	0.07	0.06	0.10	0.06	0.09	0.04	0.05	0.05

Note: Out of 12 questions included for version 1; 22 items for version 2; and 12 items for version 3. Includes speeders and skippers. Based on unweighted data.
*White, black, Asian other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.
Source: 2020 RTI/Amerispeak Identity Theft Survey.

4.6 Feedback from MTurk Workers

One of the features of MTurk was the ability for workers to communicate with survey requesters. A few workers have taken advantage of this feature to let us know that they submitted the wrong code, give us feedback about the survey, and give more detail of their story in relation to the survey.

Feedback about the survey through email:

> "Good survey and well done. Keep up the good work and have a great day."
>
> "Thank you for the opportunity to participate in this survey. I really appreciate it."
>
> "Dear Requester I like your work thank you for approval my job I want to earn more then rewards survey next time work in improve the request."
>
> "Excellent pay and it didn't take long to do."
>
> "Thanks for the survey, have a nice day."

More detail about their experience with identity theft:

> "Just wanted to clarify something. I remembered something after I answered. There actually was this one time that I had to dispute a few small items on my checking account. But this was about 15 years ago so I don't remember. There was also a time back in 2010 or 2011 that I wasn't able to open a

checking account because my name was on...was it Chexsystems?? I don't know, but I remember it had something to do with someone trying to use my e-trade account or something. It was a big hassle getting my name off of it, but I don't remember the details.”

“I completed this survey but I'd say that for most of the questions my honest answer was "not that I know of" because it is certainly possible that people have used my identity for things that would not immediately, or perhaps even ever come to my attention as long as there was no problem with the fraudulent use, such as opening up a utility in my name.”

“Thank you for the email invitation to this hit. I wanted to provide you with a little additional data related to this topic in case it is of any use to your research. My Partner and I both pay Zander for identity theft protection and in addition to BitDefender for protection against computer viruses, I also have Zemana which includes a program to prevent someone using a keystroke logger on my computer. Those are just some of the steps we take to protect ourselves against identity theft.”

“I’m not sure if my original message went through or not but I was delighted to assist in giving information for this HIT. But I am asking if your team has any additional information outside of the norm of the FED trade, make another HIT. I'm sure there are other TURkers who might help with the HIT. Also, if you do know of any information now, please divulge, it would be greatly appreciated.”

“Thanks so much for allowing me to work on this HIT.”

“Hi there.. I just finished your identity theft survey and honestly, the yes and no only answers are a bit off-putting considering most people have no idea if their information is being misused or not. Every single question asked, the honest answer would have to be "Not to my knowledge". Yes or No doesn't apply to me and I'm betting on most people here.”

“On TurkerView, a site where MTurk workers write reviews of the project they completed for the benefit of other workers, a majority thought our pay is fair or generous. One reviewer liked that no one gets screened out as long as they qualify for the survey. A reviewer mentioned that the demographics page was annoying but thought it was a simple HIT and asked us to keep up the good work.”

5. References

American Association for Public Opinion Research. (2015). *Standard definitions: Final dispositions of case codes and outcome rates for surveys*. Available at: https://www.aapor.org/AAPOR_Main/media/MainSiteFiles/Standard-Definitions2015_8thEd.pdf

Hsieh, Y. P., Sanders, H., Eckman, S., & Smith, A. (2018). *Motivated misreporting in crowdsourcing tasks of content coding, image classification, and survey.* Paper presented at the 73th Annual Conference of the American Association for Public Opinion Research, Denver, CO. May 16–19, 2018.

Krebs, C., Lindquist, C., Berzofsky, M., Shook-Sa, B., & Peterson, K. (2016). *Campus climate validation study: Final technical report*. Bureau of Justice Statistics Research and Development Series. NCJ 249545. Available at: https://rvap.uiowa.edu/assets/Uploads/2898aa5950/Campus-Climate-Survey-2016.pdf

Appendix A.
Three Versions of ITS Screener Used in Testing

A.1 Identity Theft Supplement Questionnaire–Version 1

SECTION A. SCREENER QUESTIONS

INTRO 1: This survey asks questions about possible experiences with 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. We estimate these questions will take between 5 to 15 minutes depending on your circumstances.

The first set of questions are about the possible misuse of EXISTING ACCOUNTS.

1. During the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today, have you had at least one active checking or savings account through a bank or financial institution?

   YES
   NO (skip to Q2)

1a. [During the past 12 months,] Has someone, without your permission, used or attempted to use your existing checking or savings account, including any debit or ATM cards?

   YES
   NO

2. Do you currently have at least one credit card in your name? Include major credit cards such as a MasterCard or Visa, and store credit cards such as a Macy's card. Please do not include debit cards.

   YES
   NO (ask follow up)

   Have you had one in the past 12 months, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR]?

   YES
   NO (skip to Q3)

   2a. During the past 12 months, has someone used or attempted to use one or more of your existing credit cards without your permission? Please do not include debit cards.

      YES
      NO

3.

[During the past 12 months,] Has someone misused or attempted to misuse another type of existing account such as your telephone, cable, gas or electric accounts, online payment account like Paypal, insurance policies, entertainment account like ITunes, or something else?

YES
NO (skip to Intro to Q4)

Which of the following types of your EXISTING accounts, other than credit card or banking accounts did the person run up charges on, take money from, or otherwise misuse? Did they use or attempt to use one or more of your…

3a. Medical insurance accounts?

YES
NO

3b. Telephone accounts?

YES
NO

3c. Utilities accounts, such as cable, gas or electric accounts?

YES
NO

3d. Online payment accounts such as Paypal?

YES
NO

3e. Did they use or attempt to use one or more of your…

Entertainment accounts such as for movies, music, or games?

YES
NO

EX_ENTERTAINMENT

3f. Email accounts?

YES
NO

3g. Some other type of accounts?

YES
NO

[If yes] What other type of accounts were misused? ___________________________

HARD EDIT CHECK - If Q3 is marked “yes” and ALL of Q3a through Q3g are marked “no”

You reported one or more of your existing accounts were misused but didn't identify any of these existing accounts in Q3a, Q3b, Q3c, Q3d, Q3e, Q3f, or Q3g. Would you like to change one of your responses?

YES
NO

Intro: The next questions are about any NEW ACCOUNTS someone might have opened.

4. During the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today, has someone, without your permission, used or attempted to use your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else?

YES
NO (skip to Intro to Q5)

Which of the following types of NEW accounts did someone open or attempt to open? Did someone open or attempt to open…

4a. New telephone accounts?

YES
NO

4b. New credit card accounts?

YES
NO

4c. New checking or savings accounts?

YES
NO

4d. New loans or mortgages?

YES
NO

4e. New insurance policies?

YES
NO

4f. Did someone open or attempt to open…

New online payment accounts such as Paypal?

YES
NO

4g. New utilities accounts, such as cable, gas, or electric?

YES
NO

4h. Some other type of new account?

YES
NO

[If yes] What other type of new account was opened or attempted to be opened?

____

HARD EDIT CHECK - If Q4 is marked “yes” and ALL of Q4a through Q4h are marked “no”

Responses to questions Q4a, Q4b, Q4c, Q4d, Q4e, Q4f, Q4g, and Q4h are inconsistent with answer to Q4 = Yes. Would you like to change one of your responses?

YES
NO

Intro: The next questions about any other misuses of your personal information.

5. [During the past 12 months,] Has someone used or attempted to use your personal information for some other fraudulent purpose, such as filing a fraudulent tax return, getting medical care, applying for a job or government benefits; giving your information to the police when they were charged with a crime or traffic violation, or something else?

YES
NO (skip to Check Item A)

As far as you know, did the person use or attempt to use your personal information in any of the following ways? Did they use or attempt to use your personal information…

5a. To file a fraudulent tax return?

YES
NO

5b. To get medical treatment?

YES
NO

5c. To apply for a job?

YES
NO

5d. To provide false information to the police?

YES
NO

5e. To apply for government benefits?

YES
NO

5f. In some other way we haven't already mentioned?

YES
NO

[If yes] How was your personal information misused in some other way that we haven't already mentioned? ____

HARD EDIT CHECK - If Q5 is marked "yes" and ALL of Q5a through Q5f are marked "no"

Response to Q5 is inconsistent with responses to Q5a, Q5b, Q5c, Q5d, Q5e, Q5f. Would you like to change one of your responses?

YES
NO

CHECK ITEM A

Is "no" marked for Q1a, Q2a, Q3, Q4, and Q5

YES - Skip to Section G
NO - Check Item B

CHECK ITEM B

Is only one response marked "yes" from questions Q1a, Q2a, Q3, Q4, and Q5?

YES – (Skip to Q6a)
NO – (Skip to Q6b)

6a. Now we would like to know how many times you were a victim of identity theft in the past 12 months. An incident of identity theft occurs when your identity is stolen. A stolen credit card or debit card may be used multiple times but this should be considered a single incident.

You said that someone, in the past 12 months, that is since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], <autofill "yes" response from 1a, 2a, 3, 4, or 5>. Did this happen to you once or more than once?

1. More than once (skip to Section B)

2. Once (skip to Section B)

If you don't know, please select the best response.

6b. Now we would like to know how many times you were a victim of identity theft in the past 12 months. An incident of identity theft occurs when your identity is stolen. A stolen credit card or debit card may be used multiple times but this should be considered a single incident. Also, if multiple credit card numbers and a Social Security number were obtained at the same time, this should be considered a single incident.

You said that someone <autofill "yes" responses from 1a, 2a, 3, 4, or 5> in the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR]. Were all these thefts the result of one related incident, or was your personal information stolen multiple times in separate unrelated incidents?

1. Multiple Incidents (ask Q7)
2. One related incident (skip to Section B)

If you don't know, please select the best response.

7. You said that there were: <autofill "yes" responses from 1a, 2a, 3, 4, or 5> in the past 12 months. Which of these happened during the most recent incident in which someone misused or attempted to misuse your personal information?

(Only show response items that match autofill in this question)

Mark all that apply.

1. Misuse or attempted misuse of an existing credit card account
2. Misuse or attempted misuse of an existing banking account (debit, checking, ATM, savings)
3. Misuse or attempted misuse of other types of existing accounts
4. Misuse or attempted misuse of personal information to open a NEW account
5. Misuse or attempted misuse of personal information for other fraudulent purpose.

SECTION B. HOW/WHEN IDENTITY THEFT DISCOVERED

INTRO: For those with more than one incident: The next questions ask you to consider only the most recent incident during the past 12 months in which you discovered that someone misused or attempted to misuse your personal information.

For everyone: Thinking about <the/the most recent> incident, the next couple of questions are about when you discovered the misuse of your personal information.

9. In what month and year did you first discover that someone had misused or attempted to misuse your personal information?

Enter month: __________ Month (01-12)
Enter year: __________ Year (1955-2018)

10. How long had your personal information been misused before you discovered it?

1. One day or less (1-24 hours)
2. More than a day, but less than a week (25 hours-6 days)
3. At least a week, but less than one month (7-30 days)
4. One month to less than three months
5. Three months to less than six months
6. Six months to less than one year
7. One year or more
8. Don't know
9. Not applicable, it was not actually misused

SECTION C. DEMOGRAPHICS

The last set of questions ask about your personal characteristics.

11. What is the highest level of education you have completed?

    1 High School Graduate
    2 Some College
    3 College Graduate
    4 Post-Graduate degree

12. What is your gender?

    1 Male
    2 Female
    3 Transgender
    4 None of these

13. Are you Spanish, Hispanic, or Latino?

    1 Yes
    2 No

14. Please choose one or more races that you consider yourself to be.

    1 White
    2 Black or African American
    3 American Indian or Alaskan Native
    4 Asian
    5 Native Hawaiian or Other Pacific Islander
    6 Other (specify ____________________)

15. Which of the following age groups includes your age?

    1 Under 18
    2 18-25
    3 26-34
    4 35-49
    5 50 or Older

A.2 Identity Theft Supplement Questionnaire—Version 2

SECTION A. SCREENER QUESTIONS

INTRO 1: This survey asks questions about possible experiences with 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. We estimate these questions will take between 5 to 15 minutes depending on your circumstances.

The first set of questions are about the possible misuse of EXISTING ACCOUNTS, which includes existing checking, savings, credit card, social media, and other types of accounts.

1. First, have you ever had an active checking or savings account through a bank or financial institution?

   YES
   NO (skip to Q5)

2. Has anyone EVER, without your permission, used your checking or savings account, including any debit or ATM cards, to make a purchase or withdraw money? Please consider only times when money was actually deducted from your checking or savings account, regardless of whether you were reimbursed later. Please do not include times when anyone used your credit card or online pay accounts.

   YES
   NO (skip to Q5)

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

   YES
   NO (skip to Q5)

4a. In what year did this most recently happen? ________________________

4b. And in what month? ____________________________

If you don't know, please provide your best estimate.

5. The next questions are about the possible misuse of EXISTING CREDIT CARD ACCOUNTS.

Have you ever had a credit card account in your name? Include major credit cards such as a MasterCard or Visa, and retail credit cards such as a Macy's, Walmart, or Amazon card. Please do not include debit cards.

   YES
   NO (skip to Q9)

6. Thinking only of credit card accounts, has anyone EVER used one or more of your credit card accounts without your permission? Please consider only times when charges actually posted to your account, regardless of whether you were reimbursed later.

   YES
   NO (skip to Q9)

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

   YES
   NO (skip to Q9)

8a. In what year did this most recently happen? ________________________

8b. And in what month? ____________________________

If you don't know, please provide your best estimate.

9. These next questions focus on the misuse of your email or social media accounts.

Has anyone EVER, without your permission used your email or social media account to pretend to be you?

   Yes
   No (skip to Q11)

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

   YES
   NO (skip to Q11)

   10a. In what year did this most recently happen? ________________________

   10b. And in what month? ____________________________

11. *These next questions ask about the possible misuse of any of your EXISTIING ACCOUNTS other than banking, credit card, email or social media accounts.*

Has anyone EVER, without your permission used another of your accounts, such as your telephone, internet or utilities accounts; medical insurance accounts; entertainment accounts, such as for music, movies, or games; online payment accounts like Paypal or Venmo; or some other accounts? Please include only times when someone successfully got into and used your account.

   YES
   NO (skip to Q15)

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

   YES
   NO (skip to Q15)

13. Which of the following types of your EXISTING accounts, other than credit card or bank accounts, did someone run up charges on, take money from, or otherwise misuse? Did they misuse one or more of your….

13a. Telephone or internet accounts?

YES
NO

13b. Utilities accounts, such as cable, gas or electric accounts?

YES
NO

13c. Medical insurance accounts?

YES
NO

13d. Entertainment accounts, such as for movies, music, or games?

YES
NO

13e. Online payment accounts, such as Paypal or Venmo?

YES
NO

13f. Some other type of accounts?

YES
NO

[If yes] What other type of accounts were misused? __________

(If any 13a-13f = yes, ask Q14a; else skip to Q15)

14a. Please think about the most recent time someone misused [this/one of these] existing accounts. In what year did this most recently occur? ______________________________

14b. In what month [was this existing account/were these existing accounts] most recently misused? __________________________

If you don't know, please provide your best estimate.

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

Has anyone EVER, without your permission, used your personal information to successfully open any NEW accounts, such as telephone or internet accounts; credit card or bank accounts; loans or mortgages; insurance accounts; entertainment accounts, such as for music, movies or games; email or social media accounts; utilities accounts; online payment accounts, such as Paypal or Venmo; or some other type of account? Please include times when someone successfully opened a new account, even if you did not lose any money or were reimbursed later.

YES
NO (skip to Q19)

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

YES
NO (skip to Q19)

17. Which of the following types of NEW accounts did someone successfully open during the past 12 months? Did someone open…

17a. New telephone or internet accounts?

YES
NO

17b. New credit card accounts?

YES
NO

17c. New checking or savings accounts?

YES
NO

17d. New loans or mortgages?

YES
NO

17e. New insurance policies?

YES
NO

17f. New entertainment accounts, such as for music, movies, or games?

YES
NO

17g. New email or social media accounts?

YES
NO

17h. New utilities accounts, such as cable, gas, or electric?

YES
NO

17i. New online payment accounts, such as Paypal or Venmo?

YES
NO

17j. Some other type of new account?

YES
NO

[If yes] What other type of new account was opened? __________

(If any 17a-17j = yes, ask Q18a; else skip to Q19)

18a. Please think about the most recent time someone successfully opened [this/one of these] new accounts. In what year was this?______________________________

18b. And in what month? Think about the most recent month when the new account was opened in your name regardless if it remained opened for multiple months or years. ___________________________

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

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; giving your information to the police when they were charged with a crime or traffic violation; 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
NO (skip to Check Item A)

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

YES
NO (skip to Check Item A)

21. In which of the following ways has someone used your personal information during the past 12 months? Was your personal information used….

21a. To file a fraudulent tax return?

YES
NO

21b. To get medical treatment?

YES
NO

21c. To apply for a job?

YES
NO

21d. To provide false information to the police?

YES
NO

21e. To apply for government benefits?

YES
NO

21f. In some other way we haven't already mentioned?

YES
NO

[If yes] How else was your personal information misused? __________

(If any 21a-21f = yes, ask Q22a; else skip to Check Item A)

22a. Please think about the most recent time your personal information was misused in [this way/one of these ways]. In what year did this most recently happen? _________________________

22b. And in what month? *If your information was misused for multiple months or years, think about the month it was most recently misused.* ___________________________

If you don't know, please provide your best estimate.

CHECK ITEM A
Is "no" or 'out of universe' marked for Q2, Q6, Q9, Q11, Q15, and Q19
YES – Survey is completed (*no identity theft in respondent's lifetime*)
NO - Read Check Item B

CHECK ITEM B
Is "no" or 'out of universe' marked for Q3, Q7, Q10, Q12, Q16, AND Q20
Yes – Skip to Long Term Consequences
NO – Read Check Item C

CHECK ITEM C
Is only one response marked "yes" from questions Q3, Q7, Q10, Q12, Q16, AND Q20
YES – Skip to Section B (intro 2)
NO – Read Check Item D

CHECK ITEM D
Is the most recent Month/Year provided more than once in Q4a/b, Q8a/b, Q10a/b, Q14a/b, Q18a/b, and Q22a/b (e.g. if respondent answered 2021, May in both Q4a/b and Q8a/b, select 'yes.')?
NO – Skip to Section B (intro 1)
YES – Ask Q23

23. You said that in <autofill most recent month/year provided in Q4a/b, Q8a/b, Q10a/b, Q14a/b, Q18a/b AND Q22a/b> someone <autofill applicable "yes" responses from Q3, Q7, Q10, Q12, Q16, AND Q20>. Were these the result of one related incident, or was your personal information misused multiple times in separate unrelated incidents?

1. Multiple Incidents (ask Q24)
2. One related incident (skip to Section B, intro 1)

If respondent states "I don't know," instruct him/her to select what he/she believes to be the best response.

24. Which of these happened most recently?

(Mark all that apply, and only read response items that match autofill from Q3, Q7, Q10, Q12, Q16, and Q20)

1. Misuse of an existing credit card account
2. Misuse of an existing banking account (debit, checking, ATM, savings)
3. Misuse of other types of existing accounts
4. Misuse of personal information to open a NEW account
5. Misuse of personal information for other fraudulent purpose.

(Skip to Intro 1)

SECTION B. HOW/WHEN IDENTITY THEFT WAS DISCOVERED

INTRO 1: *For those with more than one incident:* The next questions will ask you to consider only the most recent incident of identity theft that you experienced during the prior 12 months. (read intro 2)

INTRO 2: For the next series of questions, please think about the [autofill most recent type of ID theft from (Q3, Q7, Q10, Q12, Q16, Q20) OR Q24, if applicable] you experienced in [autofill most recent month/year from Q4a/b, Q8a/b, Q10a/b, Q14a/b, Q18a/b, or Q22a/b].

25. Thinking about [the/the most recent time] your personal information was misused, in what month and year did you first *discover* that someone had misused your personal information?

Enter month: __________ Month (01-12)

Enter year: __________ Year (1955-2021)

26. How long had your personal information been misused *before* you discovered it?

1. One day or less (1-24 hours)
2. More than a day, but less than a week (25 hours-6 days)
3. At least a week, but less than one month (7-30 days)
4. One month to less than three months
5. Three months to less than six months
6. Six months to less than one year
7. One year or more
8. Don't know

SECTION C. DEMOGRAPHICS

The last set of questions ask about your personal characteristics.

27. What is the highest level of education you have completed?

1 High School Graduate
2 Some College
3 College Graduate
4 Post-Graduate degree

28. What is your gender?

1 Male
2 Female
3 Transgender
4 None of these

29. Are you Spanish, Hispanic, or Latino?

1 Yes
2 No

30. Please choose one or more races that you consider yourself to be.

1 White
2 Black or African American
3 American Indian or Alaskan Native
4 Asian
5 Native Hawaiian or Other Pacific Islander
6 Other (specify ____________________)

31. Which of the following age groups includes your age?

1 Under 18
2 18-25
3 26-34
4 35-49
5 50 or Older

A.3 Identity Theft Supplement Questionnaire—Version 3

SECTION A. SCREENER QUESTIONS

INTRO 1. This survey asks questions about possible experiences with 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. We estimate these questions will take between 5 to 15 minutes depending on your circumstances.

The first set of questions are about the possible misuse of EXISTING ACCOUNTS.

1. During the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today, have you had at least one active checking or savings account through a bank or financial institution?

   YES
   NO (skip to Q2)

   1a. [During the past 12 months,] Has someone, without your permission, used your existing checking or savings account, including any debit or ATM cards? Please consider only times when money was actually deducted from your checking or savings account, regardless of whether you were reimbursed later. Please do not include times when anyone used your credit card or online pay accounts.

   YES
   NO

2. Do you currently have at least one credit card in your name? Include major credit cards such as a MasterCard or Visa, and store credit cards such as a Macy's card. Please do not include debit cards.

   YES
   NO (ask follow up)

   Have you had one in the past 12 months, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR]?

   YES
   NO (skip to Q3)

   2a. During the past 12 months, has someone used one or more of your existing credit cards without your permission? Please do not include debit cards. Please consider only times when charges actually posted to your account, regardless of whether you were reimbursed later.

   YES
   NO

3. [During the past 12 months,] has someone misused another type of existing account such as your telephone, cable, gas or electric accounts, online payment account like Paypal, insurance policies, entertainment account like ITunes, or something else? Please include only times when someone successfully got into and used your account.

   YES
   NO (skip to Intro to Q4)

Which of the following types of your EXISTING accounts, other than credit card or banking accounts did the person run up charges on, take money from, or otherwise misuse? Did they use one or more of your…

3a. Medical insurance accounts?

YES
NO

3b. Telephone accounts?

YES
NO

3c. Utilities accounts, such as cable, gas or electric accounts?

YES
NO

3d. Online payment accounts such as Paypal?

YES
NO

3e. Did they use or attempt to use one or more of your…

Entertainment accounts such as for movies, music, or games?

YES
NO

3f. Email accounts?

YES
NO

3g. Some other type of accounts?

YES
NO

[If yes] What other type of accounts were misused? __________

HARD EDIT CHECK - If Q3 is marked "yes" and ALL of Q3a through Q3g are marked "no"

You reported one or more of your existing accounts were misused, but didn't identify any of these existing accounts in 3a, 3b, 3c, 3d, 3e, 3f, or 3g.

Intro: The next set of questions are about any NEW ACCOUNTS someone might have opened.

4. During the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today, has someone, without your permission, used your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else? Please include times when someone successfully opened a new account, even if you did not lose any money or were reimbursed later.

   YES
   NO (skip to Intro to Q5)

Which of the following types of NEW accounts did someone open? Did someone open …

4a. New telephone accounts?

YES
NO

4b. New credit card accounts?

YES
NO

4c. New checking or savings accounts?

YES
NO

4d. New loans or mortgages?

YES
NO

4e. New insurance policies?

4f. Did someone open …

New online payment accounts such as Paypal?

YES
NO

4g. New utilities accounts, such as cable, gas, or electric?

YES
NO

4h. Some other type of new account?

YES
NO

[If yes] What other type of new account was opened? __________

HARD EDIT CHECK - If Q4 is marked “yes” and ALL of Q4a through Q4h are marked “no”

Responses to questions 4a, 4b, 4c, 4d, 4e, 4f, 4g, 4h are inconsistent with answer to Q4 = Yes.

Intro: The next questions about any other misuses of your personal information.

5. [During the past 12 months,] Has someone used your personal information for some other fraudulent purpose, such as filing a fraudulent tax return, getting medical care, applying for a job or government benefits; giving your information to the police when they were charged with a crime or traffic violation, or something else? Please consider only times when your information was actually used, even if the situation was later resolved.

   YES
   NO (skip to Check Item A)

As far as you know, did the person use your personal information in any of the following ways? Did they use your personal information…

5a. To file a fraudulent tax return?

YES
NO

5b. To get medical treatment?

YES
NO

5c. To apply for a job?

YES
NO

5d. To provide false information to the police?

YES
NO

5e. To apply for government benefits?

YES
NO

5f. In some other way we haven’t already mentioned?

YES
NO

How was your personal information misused in some other way that we haven’t already mentioned? __________

HARD EDIT CHECK - If Q5 is marked “yes” and ALL of Q5a through Q5f are marked “no”

Response to Q5 is inconsistent with responses to Q5a, Q5b, Q5c, Q5d, Q5e, Q5f.

CHECK ITEM A
Is “no” marked for Q1a, Q2a, Q3, Q4, and Q5
YES - Skip to Section G
NO –Check Item B

CHECK ITEM B
Is only one response marked "yes" from questions Q1a, Q2a, Q3, Q4, and Q5?
YES - Ask Q6a
NO - Ask Q6b

6a. Now we would like to know how many times you were a victim of identity theft in the past 12 months. An incident of identity theft occurs when your identity is stolen. A stolen credit card or debit card may be used multiple times, but this should be considered a single incident.

You said that someone, in the past 12 months, that is since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], <autofill "yes" response from 1a, 2a, 3, 4, or 5>. Did this happen to you once or more than once?

1. More than once (skip to Section B)
2. Once (skip to Section B)

If you don't know, please provide your best estimate.

6b. Now we would like to know how many times you were a victim of identity theft in the past 12 months. An incident of identity theft occurs when your identity is stolen. A stolen credit card or debit card may be used multiple times, but this should be considered a single incident. Also, if multiple credit card numbers and a Social Security number were obtained at the same time, this should be considered a single incident.

You said that someone <autofill "yes" responses from 1a, 2a, 3, 4, or 5> in the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR]. Were all these thefts the result of one related incident, or was your personal information stolen multiple times in separate unrelated incidents?

1. Multiple Incidents (ask Q7)
2. One related incident (skip to Section B)

If you don't know, please provide your best estimate.

7. You said that there were: <autofill "yes" responses from 1a, 2a, 3, 4, or 5> in the past 12 months. Which of these happened during the most recent incident in which someone misused your personal information?

(only show response items that match autofill in this question)

Mark all that apply.

1. Misuse of an existing credit card account
2. Misuse of an existing banking account (debit, checking, ATM, savings)
3. Misuse of other types of existing accounts
4. Misuse of personal information to open a NEW account
5. Misuse of personal information for other fraudulent purpose.

SECTION B. HOW/WHEN IDENTITY THEFT WAS DISCOVERED

INTRO: For those with more than one incident: The next set of questions ask you to consider only the most recent incident during the past 12 months in which you discovered that someone misused your personal information.

For everyone: Thinking about <the/the most recent> incident, the next couple of questions are about when the misuse of your personal information most recently occurred and how and when you discovered the misuse of your personal information.

8. Thinking about [the/the most recent] time your personal information was misused, in what month and year did the misuse most recently occur?

   Enter month: __________ Month (01-12)

   Enter year: __________ Year (1955-2021)

If you don't know, please provide your best estimate.

9. In what month and year did you first discover that someone had misused your personal information? This may be the same month and year as the most recent occurrence, or the discovery may have happened before or after the most recent occurrence.

   Enter month: __________ Month (01-12)

   Enter year: __________ Year (1955-2021)

If you don't know, please provide your best estimate.

10. How long had your personal information been misused before you discovered it?

    1. One day or less (1-24 hours)
    2. More than a day, but less than a week (25 hours-6 days)
    3. At least a week, but less than one month (7-30 days)
    4. One month to less than three months
    5. Three months to less than six months
    6. Six months to less than one year
    7. One year or more
    8. Don't know

SECTION C. DEMOGRAPHICS

The last set of questions ask about your personal characteristics.

11. What is the highest level of education you have completed?

    1 High School Graduate
    2 Some College
    3 College Graduate
    4 Post-Graduate degree

12. What is your gender?

    1 Male
    2 Female
    3 Transgender

4 None of these

13. Are you Spanish, Hispanic, or Latino?

1 Yes
2 No

14. Please choose one or more races that you consider yourself to be.

1 White
2 Black or African American
3 American Indian or Alaskan Native
4 Asian
5 Native Hawaiian or Other Pacific Islander
6 Other (specify ____________________)

15. Which of the following age groups includes your age?

1 Under 18
2 18-25
3 26-34
4 35-49
5 50 or Older

Appendix B.
Findings From ITS Version 2 Cognitive Testing

Cognitive Interviewing for the National Crime Victimization Survey (NCVS) Identity Theft Supplement (ITS)

Prepared by RTI International

June 5, 2020

Sarah Cook, Jeanne Snodgrass, Lynn Langton

INTRODUCTION

This report provides a summary of RTI findings from 27 adult cognitive interviews on the redesigned version of the BJS Identity Theft Supplement (ITS) screener. Interviews took place virtually via Zoom with participants in the Eastern, Central and Pacific time zones in May and early June 2020. Cognitive interviews were conducted virtually due to the COVID-19 pandemic. These preliminary findings may be of use to BJS when incorporating the next round of changes to the NCVS ITS instrument.

Table 1. Participant Demographics

Time Zone		
	EDT	13
	CDT	8
	MDT	0
	PDT	6
Age Range		
	18-25	2
	26-34	13
	35-49	9
	50 or older	3
Education		
	High school/GED	2
	Some college	4
	College grad	16
	Post-grad degree	8
Gender		
	Male	20
	Female	7
Race		
	White	20
	Black/African American	4
	Asian	5
	American Indian/Alaska Native	2
	Native Hawaiian/Pacific Islander	0
Hispanic		
	Yes	1

RECRUITMENT

All recruitment was done through Amazon's Mechanical Turk (MTurk). MTurk is an online crowdsourcing platform where workers can complete nominal tasks for small payments. For our purposes, we posted a MTurk task (known as a "HIT") for participants to complete an online screener survey to participate in a virtual interview.

Once participants completed the online web screener, our recruiter contacted those who were eligible for the study via email to schedule interviews. Eligibility was based on our need for demographic diversity as well as type of identity theft experienced. An informed consent form was sent via email to the participant for them to review. At the beginning of each virtual interview, the interviewer verified that the respondent had received the informed consent form, asked if they had questions, and received verbal consent to conduct the interview and be recorded.

Table 1 shows the cumulative demographics of participants. Though already a diverse group of participants, some diversity was lost to participants who changed their mind or did not attend their interview. **Table 2** shows this same information distributed by participants and includes the type of identity theft as indicated in the online screener and as reported during the actual interview. The online screener was a condensed version of the revised ITS screener that included four questions about identity theft experiences:

1. During the past 12 months, that is, since [AUTOFILL DATE A YEAR AGO FROM SURVEY DATE], has someone, without your permission used your existing checking account, savings account, or credit card account?
2. During the past 12 months, has someone misused another type of existing account such as your telephone, cable, gas or electric accounts, online payment account like Paypal, insurance policies, entertainment account like ITunes, or something else?
3. During the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today, has someone, without your permission, used your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else?
4. During the past 12 months, has someone used your personal information for some other fraudulent purpose, such as filing a fraudulent tax return, getting medical care, applying for a job or government benefits; giving your information to the police when they were charged with a crime or traffic violation, or something else?

Endorsement of these questions is represented in the table below consecutively as: *Existing (bank), Existing (other), New account, and Personal info*. Three of the recruited 'non-victims' of identity theft ended up as 'victims' once the participants heard the full survey questions and self-reported their experience, and three of our recruited 'victims' ended up as nonvictims during the interview.

Table 2. Participant Demographic, Recruitment, and Final Identity Theft Type Data (n=27)

P#	Time Zone	Age Range	Education	Gender	Race	Recruited IT Type	Final IT Type
1	EDT	35-49	Post-Graduate degree	Female	White	None	None
2	PDT	26-34	College Graduate	Male	Asian	Existing (bank); Existing (other)	Existing (bank)
3	CDT	26-34	Post-Graduate degree	Female	White	Existing (bank)	Existing (bank)
4	CDT	26-34	High School Graduate/GED	Female	Black and AI/AN	Existing (bank); Existing (other); New account	Existing (bank)
5	PDT	35-49	College Graduate	Male	White	Existing (bank); Existing (other); Personal info	New account; Personal info
6	PDT	18-25	College Graduate	Male	Black	None	Existing (bank); Existing (other); Personal info

Table 2. Participant Demographic, Recruitment, and Final Identity Theft Type Data (n=27)

P#	Time Zone	Age Range	Education	Gender	Race	Recruited IT Type	Final IT Type
7	EDT	26-34	College Graduate	Male	Asian	All	None
8	EDT	35-49	Some College	Male	White	Existing (bank); Existing (other)	Existing (other)
10	CDT	35-49	College Graduate	Male	White	Existing (bank)	Existing (bank); New account
11	PDT	26-34	College Graduate	Male	White	Existing (bank); New account	Existing (bank); New account
12	PDT	26-34	College Graduate	Male	Black	All	Existing (bank); Existing (other); New account
13	EDT	35-49	Post-Graduate degree	Male	Asian	Existing (bank); Existing (other); New account	Existing (bank)
15	EDT	26-34	Post-Graduate degree	Male	Asian	None	Existing (other)
16	EDT	50 or older	Post-Graduate degree	Male	White	None	Existing (bank)
17	EDT	26-34	Post-Graduate degree	Female	Asian and AI/AN	Existing (bank); Existing (other)	Existing (bank)
18	EDT	50 or older	Some College	Female	White	Existing (bank)	None
19	CDT	26-34	College Graduate	Male	Asian	Existing (bank); Existing (other)	Existing (bank);
20	PDT	50 or older	College Graduate	Female	White	Existing (bank); Personal info	Existing (bank);
22	CDT	35-49	Post-Graduate degree	Female	White	Existing (bank)	Existing (bank)
23	CDT	26-34	College Graduate	Male	White	Existing (bank); Existing (other)	Existing (bank)
24	EDT	35-49	Some College	Male	White	Existing (other)	Existing (other)
26	EDT	35-49	College Graduate	Male	White	Existing (other)	Existing (bank); Existing (other)
27	CDT	26-34	College Graduate	Male	White	Existing (bank)	Existing (bank); Existing (other)
30	CDT	26-34	College Graduate	Male	White	Existing (bank)	None
31	EDT	26-34	College Graduate	Female	White	Existing (other)	Existing (bank); Existing (other); Personal Info
32	EDT	35-49	College Graduate	Female	Black	Existing (bank)	Existing (bank)

Table 2. Participant Demographic, Recruitment, and Final Identity Theft Type Data (n=27)

P#	Time Zone	Age Range	Education	Gender	Race	Recruited IT Type	Final IT Type
34	EDT	18-25	College Graduate	Male	White	Existing (other)	Existing (other)

METHODS

Once MTurk respondents completed the online screener, were determined to be eligible to participate in the cognitive interview, and expressed interest in participating in a virtual interview, the RTI recruiter scheduled an interview time with the participant. The recruiter then sent the participant a link to a private Zoom meeting set up for their specific interview. RTI interviewers were trained to stop the interview if anyone else joined the meeting. In many cases, the “waiting room” feature was turned on so no one could join the meeting without being allowed in by the interviewer.

Prior to conducting any interviews, all interviewers completed training on the cognitive interview protocol and project logistics. All interviews were conducted using a cognitive interview protocol that was based on the most recent version of the supplement provided by BJS. The protocol included probes developed to elicit an understanding of how respondents interpreted specific terms or questions. Along with the pre-determined probes, interviewers were encouraged to use spontaneous probing when needed to further understand the participant’s thinking. The interview protocol is included in **Appendix A**.

Prior to the start of the interview, the interviewer obtained verbal participant consent. After the interview, participants were emailed an Amazon.com Gift Card code with a value of $40 to help cover data and technology costs associated with participating in the interview.

FINDINGS AND RECOMMENDATIONS

This section summarizes key findings and recommended changes to specific survey items for which any problems or issues were identified. Overall, the survey performed very well. There are many questions where none of the 27 participants had difficulty understanding and answering them as intended. These items not discussed below did not appear to be problematic and have no recommended changes.

Q2 – Has anyone EVER, without your permission, used your checking or savings account, including any debit or ATM cards, to make a purchase or withdraw money? Please consider only times when money was actually deducted from your account, regardless of whether you were reimbursed later.

1. ***Yes***
2. ***No (Skip to Q5)***

Although all respondents were able to answer this question in relation to bank accounts only, a few mentioned that they also thought about their credit card accounts in this question, not knowing that we were going to ask about credit card accounts separately. Three respondents had credit cards through their bank, which made it more difficult to separate the two. One participant answered “Yes” to this question and, through probing, shared that the theft actually happened in their Google Pay account, which is connected to their bank account. They later said that the incident should be counted in Q9, not Q2, after hearing the response options provided. If they had known there would be an option to report identity theft of an account like Google Pay, they never would have answered “Yes” to Q2.

Recommendation: Suggest changing the last sentence to **“Please consider only times when money was actually deducted from your checking or savings account, regardless of whether you were reimbursed**

later." or adding "Please do not include times when anyone used your credit card or online pay accounts without permission." Alternatively, to be consistent with Q6, start the question with **"Thinking only of checking and savings accounts,"**. It may still be helpful to conclude with **"Please do not include times when anyone used your credit card or online pay accounts without permission.**"

Q5 – Now I'd like to ask you about the possible misuse of EXISTING CREDIT CARDS OR CREDIT CARD ACCOUNTS.

Have you ever had a credit card in your name? Include major credit cards such as a Mastercard or Visa, and store credit cards such as a Macy's card. Please do not include debit cards.

1 Yes
2 No (Skip to Q9)

Most respondents suggested including American Express and Discover as examples of major credit cards, and "big box" retailer cards such as Target, Walmart and Amazon as examples of store cards. However, the current examples still provided enough information for participants to know what they should be thinking about. One person suggested saying "retail" instead of "store" credit cards because you can have credit cards for things that do not have physical stores (such as Amazon).

Recommendation: Consider replacing "Macy's" with "Target or Amazon" and changing "store credit cards" to "retail credit cards" to encompass more possibilities.

Q6 – Thinking only of credit cards, has anyone EVER used one or more of your credit cards without your permission? Please consider only times when charges actually posted to your account, regardless of whether you were reimbursed later.

1 Yes
2 No (Skip to Q9)

One respondent mentioned he would answer this question as 'No' because he interprets this question to be about the misuse of physical credit cards only. If the question were more specific about including the misuse of credit card numbers as well, he would answer this question as "Yes".

Recommendation: Consider adding "accounts" after the second mention of 'credit card' in the question text.

Q9 – Now I'd like to ask you about the possible misuse of any of your EXISTIING ACCOUNTS other than credit card or bank accounts.

Has anyone EVER, without your permission used another of your accounts, such as your telephone, internet or utilities accounts, online payment accounts like Paypal, medical insurance accounts, entertainment accounts, such as for music or games, email or social media accounts, or some other accounts? Please include only times when charges were actually made on the account, regardless of whether you were reimbursed later.

Yes
No (Skip to Q13)

Respondents overwhelmingly said listing the types of accounts was very helpful in helping them to think about the types of accounts we are asking about, but mentioned that they focused in on specific service provider names and then forgot things said after that. Keeping the proper names at the end of the list might help with that. Another person mentioned that we should add “movies” so they would think of streaming accounts. Some participants mentioned thinking about failed log-in attempts they were alerted to on their accounts, but they all knew not to include those. (INTERVIEWER NOTE: We noticed movies are included below in Q11e.)

We have had several respondents who had their Facebook or Instagram accounts taken over, but because the language at the end of the question focuses on charges made to the account, they were not sure whether to actually include them. Two respondents said they did not include times their accounts were compromised for that very reason. It is possible to misuse entertainment, email, and social media accounts without any financial transaction. In the case of entertainment accounts, the theft is the service they are using and not paying for, not a financial theft. Using another person’s social media accounts is often used for phishing, in which case the infiltration is a means to an end. Email accounts, however, carry more weight because passwords can be sent or reset to an email account. Theft of an email account has many more implications than that of entertainment or social media.

Recommendation: Move ‘online payment accounts’ to the end of the list and include Venmo with the Paypal example. Revise example of entertainment accounts to, “entertainment accounts, such as for music, games, or movies” so participants consider popular streaming services.

Consider the appropriate placement for accessing social media accounts. Does the misuse of email and social media account fit better under the category of ‘misuse of personal information for other fraudulent purposes?’ or should they be in their own either combined or separate categories?

If the intent of the question is to capture account access regardless of financial loss, replace the last sentence with “Please include only times when someone actually got into your account. Do not include failed login attempts”.

Q11 – Which of the following types of your EXISTING accounts, other than credit card or bank accounts, did someone run up charges on, take money from, or otherwise misuse? Did they misuse one or more of your….

11a. Telephone or internet accounts? YES NO
11b. Utilities accounts, such as cable, gas or electric accounts? YES NO
11c. Online payment accounts, such as Paypal? YES NO
11d. Medical insurance accounts? YES NO
11e. Entertainment accounts, such as for movies, music, or games? YES NO
11f. Email or social media accounts? YES NO
11g. Some other type of accounts? YES NO
[If yes] What other type of accounts were misused? ____________
(If any 11a-11g = yes, ask Q12a; else skip to Q13)

Recommendation: To remain consistent with Q10, move “Online payment accounts”, such as Paypal to the end of the list above “other” and include Venmo as an example.

Q13 – Next, I have some questions about any NEW ACCOUNTS someone might have opened using your personal information.

Has anyone EVER, without your permission, used your personal information to successfully open any NEW accounts, such as telephone or internet accounts, credit card or bank accounts, loans or mortgages, insurance accounts, online payment accounts, entertainment accounts, such as for music or games, email or social media accounts, utilities accounts or some other type of account?

1 Yes
2 No (skip to Q17)

A few participants said "No" to this question because they assumed it required a financial loss, even though the question does not specify monetary loss. This is due to priming effects from all of the previous questions referring to losing money.

Recommendation: Consider adding, "Include times even when you did not lose any money." Revise the example of entertainment accounts to, "entertainment accounts, such as for music, games, or movies" so participants consider streaming services and to be consistent with Question 9.

Q17 - Next, I have some questions about any other misuses of your personal information.

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; giving your information to the police when they were charged with a crime or traffic violation; applying for government benefits or something else? Please consider only times when your information was actually used, even if the situation was later resolved.

1 Yes
2 No (LOOK AT ANSWER SHEET TO FIND NEXT QUESTION)

Some may find the word 'actually' from the final sentence as confusing. As one participant said "If you use it, you actually use it. How do you not actually use it?"

Recommendation: Only one participant had concerns with this question and since "actually" is an adverb that is often used to emphasize something in fact happening, we recommend leaving the questions as written.

Q25 – Thinking about the most recent time your personal information was misused, in what month and year did you first discover that someone had misused your personal information? This may be the same month and year as the most recent occurrence, or the discovery may have happened before or after the most recent occurrence.

Enter month: __________ Month (01-12)

Enter year: __________ Year (1955-2021)

Some participants found the last sentence to be confusing, especially remarking on not understanding how discovery 'before' an occurrence happened. One participants was particularly confused and apologized multiple times. When the interviewer read them the question without the second sentence, they said that question was clear and had not realized it was the same question.

Recommendation: Remove the last sentence to avoid unnecessary confusion. Alternatively, it could be left in if it is made clear to only be read if a respondent is having difficulty answering the question. Consider simplifying it to "You could have first discovered the incident before, during, or after the month and year of the most recent occurrence."

Q26 - How long had your personal information been misused before you discovered it?

1. ***One day or less (1-24 hours)***
2. ***More than a day, but less than a week (25 hours-6 days)***
3. ***At least a week, but less than one month (7-30 days)***
4. ***One month to less than three months***
5. ***Three months to less than six months***
6. ***Six months to less than one year***
7. ***One year or more***
8. ***Don't know***

Most participants reported learning about the identity theft within days or weeks of the first (known) occurrence. A respondent did point out that since this question is in relation to the past 12 months, we might not need response option 7. However, due to the possibility of reoccurring incidents of identity theft, we see this response option as necessary.

Recommendation: Leave question as is.

General Findings

There are questions in this instrument about timelines that could be confusing for some or hard to follow. The two sets of questions we focused on were questions about whether an incident occurred "Ever" or "in the past 12 months, and Q25 and Q26 when we try to identify the date of discovery and length of misuse (compared to the date of the most recent incident). For the questions on whether someone had ever experienced identity theft, respondents were probed on how far back they were thinking when answering those questions. Two respondents mentioned 'lifetime' or '30 years, since I had my account,' but the majority of respondents reported remembering back to when their most recent incident or incidents occurred, whether that was 3 months ago or 5 years ago. This makes sense though because once they recalled an event, they had their answer and did not need to think further. **Table 3** provides the responses for each type of identity theft and whether it "Ever" happened and whether it happened "in the past 12 months." Many participants recognized that they had been victimized in the past, but that in many cases their incidents occurred outside of the 12-month time frame.

Table 3. Responses to "Ever" and "12 months" Questions

P#	Ever - Existing bank	12 mos - Existing bank	Ever - Existing credit card	12 mos - Existing credit card	Ever - Existing other	12 mos - Existing other	Ever - New account	12 mos - New account	Ever - Personal info	12 mos - Personal info
1	No		No		No		No		No	
2	Yes	Yes	Yes	No	No		No		No	
3	No		Yes	Yes	No		No		No	
4	No		Yes	Yes	No		No		No	
5	Yes	No	No		No		Yes	Yes	Yes	Yes
6	No		Yes	Yes	Yes	Yes	No		Yes	Yes
7	No		No		No		No		No	
8	Yes	No	No		No		No		No	
10	No		Yes	Yes	No		Yes	Yes	No	
11	No		Yes	No	No		Yes	Yes	No	
12	Yes	Yes	Yes	No	Yes	No	Yes	No	No	
13	Yes	Yes	Yes	Yes	Yes	No	No		No	
15	No		No		Yes	No	No		No	
16	Yes	No	Yes	No	No		No		No	
17	No		Yes	Yes	No		No		No	
18	No		No		No		No		No	
19	Yes	Yes.	Yes	No	No		No		No	
20	Yes	Yes	No		No		No		No	
22	Yes	Yes	Yes	Yes	No		No		No	
23	Yes	No	Yes	No	No		No		No	
24	No		No		Yes	Yes	No		No	
26	No		No		Yes	Yes	No		No	
27	No		Yes	Yes	Yes	Yes	No		No	
30	No		No		No		No		No	
31	Yes	No	Yes	No	Yes	Yes	No		Yes	Yes
32	Yes	Yes	No		No		No		No	
34	No		No		Yes	Yes	No		No	

Another concern is whether respondents were able to distinguish among the concepts of when the incident started, was discovered, and most recently occurred an whether they were able to provide dates for each of those reference points. Respondents were asked to describe in their own words what these different reference points meant in light of their own experience and all appeared to understand the concepts. With the exception of one respondent, all of the participants were able to stop the identity theft relatively quickly after they discovered it. **Table 4** needs to be introduced.

Table 4. Key Dates in Incident Timeline

P#	Most Recent	Discovered (Q25)	Length of use (Q26)
2	February 2020	February 2020	1 day-1 week
3	August 2019	August 2019	<1 day
4	October 2019	October 2019	<1 day
5	July 2019	July 2019	1-3 months
6	February 2020	January 2020	1-3 months
10	September 2019	September 2019	1 day-1 week
11	July 2019	July 2019	<1 day
12	June 2019	June 2019	<1 day
13	November 2019	December 2019	1 day-1 week
17	September 2019	September 2019	1 week–1 month
19	November 2019	November 2019	1 week–1 month
20	March 2020	March 2020	1 day-1 week
22	February 2020	February 2020	<1 day
24	March 2020	March 2020	<1 day
26	October 2019	October 2019	<1 day
27	January 2020	January 2020	<1 day
31	March 2020	March 2020	1 day-1 week
32	August 2019	August 2019	1 week–1 month
34	March 2020	March 2020	<1 day

Appendix C.
Standard Error Tables

Appendix Table 1. Standard errors for Table 1. Unweighted sample, by demographic characteristics and mode

	Total		Web		Phone	
	Number	Percent	Number	Percent	Number	Percent
Total	87.57	~ %	87.23	~ %	16.24	~ %
Sex						
Male	71.47	0.45 %	71.07	0.45 %	9.63	2.92 %
Female	70.94	0.45	70.18	0.45	13.12	2.92
Race/Hispanic origin*						
White	74.24	0.44 %	73.64	0.45 %	12.54	3.01 %
Black	38.53	0.29	37.86	0.29	7.48	2.50
Asian/c	21.95	0.17	21.86	0.17	2.00	0.75
Hispanic	52.34	0.38	52.20	0.39	4.24	1.54
Other	10.98	0.09	10.52	0.08	3.16	1.17
Two or more races	18.74	0.15	18.21	0.15	4.47	1.62
Age						
18–24	34.64	0.27 %	34.64	0.27 %	0.00	0.00 %
25–34	56.59	0.40	56.57	0.41	1.73	0.65
35–49	57.41	0.41	57.33	0.41	3.46	1.27
50–64	47.73	0.35	46.97	0.36	9.21	2.86
65 or older	38.54	0.29	36.53	0.28	12.85	2.97
Household income						
$24,999 or less	46.45	0.35 %	45.47	0.35 %	10.23	3.00 %
$25,000–$49,999	54.33	0.39	53.74	0.39	8.99	2.82
$50,000–$74,999	49.76	0.37	49.47	0.37	5.83	2.05
$75,000 or more	61.00	0.42	60.72	0.43	6.78	2.32

*White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 2. Standard errors for Table 2. Unweighted sample, by demographic characteristics and platform

	Total		AmeriSpeak		Lucid		MTurk	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Total	87.57	~ %	56.49	~ %	60.67	~ %	63.79	~ %
Sex								
Male	71.47	0.45 %	39.78	0.83 %	44.84	0.77 %	48.40	0.72 %
Female	70.94	0.45	42.52	0.83	44.16	0.77	45.61	0.72
Race/Hispanic origin*								
White	74.24	0.44 %	45.33	0.81 %	46.45	0.76 %	48.28	0.72 %
Black	38.53	0.29	23.64	0.61	23.60	0.52	20.46	0.41
Asian/c	21.95	0.17	12.14	0.33	11.47	0.27	14.41	0.30
Hispanic	52.34	0.38	21.00	0.55	32.69	0.67	37.46	0.67
Other	10.98	0.09	8.12	0.22	5.47	0.13	5.00	0.10
Two or more races	18.74	0.15	12.46	0.34	8.82	0.21	10.98	0.23
Age								
18–24	34.64	0.27 %	13.74	0.37 %	26.35	0.57 %	18.55	0.38 %
25–34	56.59	0.40	26.17	0.66	29.09	0.62	43.68	0.72
35–49	57.41	0.41	25.60	0.65	36.67	0.72	39.60	0.69
50–64	47.73	0.35	32.32	0.77	27.57	0.59	24.40	0.48
65 or older	38.54	0.29	30.40	0.74	21.63	0.48	11.55	0.24
Household income								
$24,999 or less	46.45	0.35 %	26.42	0.67 %	30.72	0.65 %	25.03	0.49 %
$25,000–$49,999	54.33	0.39	29.72	0.73	31.86	0.66	35.71	0.65
$50,000–$74,999	49.76	0.37	25.29	0.64	27.24	0.59	35.19	0.64
$75,000 or more	61.00	0.42	35.53	0.80	37.31	0.73	38.06	0.67

*White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 3. Standard errors for Table 3. Weighted sample, by demographic characteristics

	Version 1		Version 2		Version 3	
	Number	Percent	Number	Percent	Number	Percent
Total	111.71	~ %	112.90	~ %	115.70	~ %
Sex						
Male	85.48	0.60 %	85.08	0.59 %	87.18	0.61 %
Female	83.18	0.60	85.80	0.59	86.85	0.61
Race/Hispanic origin*						
White	88.50	0.59 %	88.70	0.59 %	90.94	0.61 %
Black	46.22	0.41	46.70	0.40	47.49	0.42
Asian	26.86	0.25	25.58	0.23	26.42	0.24
Hispanic	56.11	0.48	57.97	0.48	58.95	0.50
Other	13.97	0.13	14.25	0.13	14.97	0.14
Two or more races	20.16	0.19	23.68	0.21	20.88	0.19
Age						
18–24	50.11	0.44 %	47.80	0.41 %	51.46	0.45 %
25–34	45.33	0.41	44.75	0.40	46.64	0.42
35–49	57.51	0.49	58.48	0.49	60.33	0.51
50–64	61.19	0.51	64.65	0.52	64.36	0.53
65 or older	60.13	0.51	61.51	0.50	59.61	0.51
Household income						
$24,999 or less	66.19	0.54 %	67.09	0.53 %	68.14	0.56 %
$25,000–$49,999	62.42	0.52	64.69	0.52	64.03	0.53
$50,000–$74,999	50.81	0.45	52.16	0.45	52.94	0.46
$75,000 or more	64.92	0.54	64.00	0.52	66.74	0.55

*White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 4. Standard errors for Table 4: Prevalence of identity theft in the past 12 months, by type of identity theft and instrument version

	Version 1*		Version 2		Version 3	
	Number of victims	Percent of all resondents/a	Number of victims	Percent of all resondents/a	Number of victims	Percent of all resondents/a
Total	71.10	0.57	69.41	0.55 ++	67.40	0.55 ++
Existing account						
Credit card	46.88	0.42	44.03	0.38 ++	45.62	0.41 ++
Bank	53.49	0.47	49.23	0.42 ++	50.65	0.44 ++
Social media	~	~	44.19	0.38	~	~
Other	48.58	0.43	37.40	0.33 ++	38.43	0.35 ++
New account	31.63	0.29	29.08	0.26 ++	22.35	0.21 ++
Personal information	22.14	0.21	19.59	0.18 ++	19.55	0.18 ++

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Based on a representative sample of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 5. Standard errors for Table 5: Persons age 18 or older who experienced one or more incidents of identity theft during the past 12 months, by victim characteristics and instrument version

	Version 1*		Version 2		Version 3	
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a
Total	71.10	0.57	69.41	0.55 ++	67.40	0.55 ++
Sex						
Male	52.72	0.84	48.81	0.78 ++	49.53	0.82 ++
Female	50.17	0.76	51.24	0.76 ++	47.43	0.75 ++
Race/Hispanic origin/b						
White	53.86	0.68	50.68	0.64 ++	47.51	0.63 ++
Black	24.81	1.69	28.57	1.75	27.43	1.78
Asian	14.95	2.56	11.92	2.33 ++	12.20	2.25 ++
Hispanic	37.72	1.60	35.44	1.56 ++	36.87	1.64 ++
Other	6.88	5.11	5.91	4.56	6.93	4.31
Two or more races	11.37	3.13	15.25	3.24	13.21	3.56
Age						
18–24	33.56	2.06	28.02	1.82 ++	29.94	2.01 ++
25–34	29.04	1.23	27.84	1.14 ++	27.11	1.19 ++
35–49	36.08	1.10	36.39	1.10 ++	33.86	1.10 ++
50–64	36.65	1.14	36.64	1.13 ++	35.41	1.13 ++
65 or older	28.65	1.12	29.82	1.12 +	27.64	1.08 ++
Household income						
$24,999 or less	38.71	1.29	36.44	1.23 ++	36.61	1.26 ++
$25,000–$49,999	36.34	1.09	37.59	1.07 ++	34.00	1.05 ++
$50,000–$74,999	30.50	1.23	29.15	1.16 ++	30.16	1.22 ++
$75,000 or more	40.77	0.98	38.83	0.94 ++	37.07	0.95 ++
Urbanicity						
Urban	66.80	0.62	65.16	0.59 ++	62.41	0.59 ++
Non-urban	26.05	1.48	25.00	1.45 ++	25.79	1.55 ++
Unknown	4.81	9.39	5.72	9.01	7.58	9.51

Note: Percentages are based on the number of persons in each category.

*Comparison group.

†Significant difference from comparison group at 95% confidence level.

‡Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 6. Standard errors for Table 6. Most recent incident of identity theft, by type of identity theft and instrument version

	Version 1*			Version 2			Version 3		
	Number of victims	Percent of all resondents/a	Percent of all victims	Number of victims	Percent of all resondents/a	Percent of all victims	Number of victims	Percent of all resondents/	Percent of all victims
Total	71.10	0.57	~	69.41	0.55 ++	~	67.40	0.55 ++	~
Only one type of existing account									
Credit card	32.01	0.29	0.74	31.85	0.28 ++	0.82	35.81	0.33	0.96 ++
Bank	36.70	0.33	0.82	38.34	0.34	0.94 ++	39.28	0.35	1.02 ++
Social media	~	~ ~	~ ~	33.93	0.30	0.86	~	~ ~	~
Other	30.20	0.28	0.70	24.01	0.22 ++	0.65 ++	21.83	0.20 ++	0.65 ++
Opened new account only	14.54	0.14	0.36	15.68	0.14	0.44 +	12.13	0.11 ++	0.37
Misused personal information only	10.18	0.10	0.26	9.34	0.09	0.27	10.32	0.10	0.32
Multiple types	42.70	0.38	0.89	24.05	0.22 ++	0.65 ++	35.06	0.32 ++	0.95 ++

*Comparison group.

†Significant difference from comparison group at 95% confidence level.

‡Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Based on a representative sample of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 7. Standard errors for Table 7. Prevalence of identity theft, by type of identity theft, instrument version, and reference period

	Version 1 - 12-month		Version 2 - 12-month		Version 3 - 12-month		Version 2 - Lifetime*	
	Number of victims	Percent of all resondents/a	Number of victims	Percent of all resondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all resondents/
Total	71.10	0.57 %++	69.41	0.55 %++	67.40	0.55 ++	96.63	0.55 %
Existing account								
Credit card	46.88	0.42 ++	44.03	0.38 ++	45.62	0.41 ++	71.07	0.55
Bank	53.49	0.47 ++	49.23	0.42 ++	50.65	0.44 ++	75.86	0.57
Social media	~	~	44.19	0.38 ++	~	~	64.93	0.52
Other	48.58	0.43 ++	37.40	0.33 ++	38.43	0.35 ++	55.29	0.46
New account	31.63	0.29 ++	29.08	0.26 ++	22.35	0.21 ++	44.51	0.39
Personal information	22.14	0.21 ++	19.59	0.18 ++	19.55	0.18 ++	31.63	0.28

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Based on a representative sample of US residents age 18 or older.

Appendix Table 8. Standard errors for Table 8. Persons age 18 or older who experienced one or more incidents of identity theft, by victim characteristics, instrument version, and reference period

	Version 1 - 12-month		Version 2 - 12-month		Version 3 - 12-month		Version 2 - Lifetime	
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a
Total	71.10	0.57 %	69.41	0.55 %	67.40	0.55 %	96.63	0.55 %
Sex								
Male*	52.72	0.84 %	48.81	0.78 %	49.53	0.82	69.48	0.82 %
Female	50.17	0.76	51.24	0.76	47.43	0.75	73.28	0.74 ++
Race/Hispanic origin/b								
White*	53.86	0.68 %	50.68	0.64 %	47.51	0.63 %	74.61	0.66 %
Black	24.81	1.69	28.57	1.75 ++	27.43	1.78 ++	37.47	1.74
Asian	14.95	2.56	11.92	2.33	12.20	2.25	19.71	2.76 ++
Hispanic	37.72	1.60 ++	35.44	1.56 ++	36.87	1.64 ++	48.72	1.48 ++
Other	6.88	5.11	5.91	4.56	6.93	4.31	11.98	5.45
Two or more races	11.37	3.13	15.25	3.24 +	13.21	3.56 ++	20.81	2.74 ++
Age								
18–24	33.56	2.06 %	28.02	1.82 %	29.94	2.01 %	38.37	1.85 %++
25–34	29.04	1.23 +	27.84	1.14	27.11	1.19	38.19	1.06
35–49*	36.08	1.10	36.39	1.10	33.86	1.10	49.43	1.04
50–64	36.65	1.14 ++	36.64	1.13 ++	35.41	1.13	54.15	1.13 +
65 or older	28.65	1.12 ++	29.82	1.12 ++	27.64	1.08 ++	48.85	1.30 ++
Household income								
$24,999 or less	38.71	1.29 %++	36.44	1.23 %++	36.61	1.26 %	52.51	1.34 %++
$25,000–$49,999	36.34	1.09 ++	37.59	1.07 ++	34.00	1.05	52.80	1.09 ++
$50,000–$74,999	30.50	1.23	29.15	1.16	30.16	1.22	44.05	1.15 ++
$75,000 or more*	40.77	0.98	38.83	0.94	37.07	0.95	55.88	0.86
Urbanicity								
Urban	66.80	0.62 %	65.16	0.59 %	62.41	0.59 %	90.60	0.59 %
Non-urban	26.05	1.48	25.00	1.45	25.79	1.55	38.55	1.50
Unknown	4.81	9.39	5.72	9.01	7.58	9.51	6.91	7.21

Note: Percentages are based on the number of persons in each category.

*Comparison group.

†Significant difference from comparison group at 95% confidence level.

‡Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 9. Standard errors for Table 9. Relationship between lifetime prevalence and 12-month prevalence, by type of identity theft (Version 2)

	Lifetime prevalence		12-month prevalence		Percent of lifetime victims
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	No past year id theft
Total	96.63	0.55 %	69.41	0.55 %	0.70 %
Existing account					
Credit card	71.07	0.55	44.03	0.38	0.93
Bank	75.86	0.57	49.23	0.42	0.95
Social media	64.93	0.52	44.19	0.38	1.11
Other	55.29	0.46	37.40	0.33	1.37
New account	44.51	0.39	29.08	0.26	1.61
Personal information	31.63	0.28	29.08	0.18	1.79

a/Based on a representative sample of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 10. Standard errors for Table 10. Relationship between lifetime prevalence and 12-month prevalence of identity theft, by victim characteristics

	Lifetime prevalence (any identity theft)*		12-month prevalence (any identity theft)		Percent of lifetime victims
	Number of victims	Percent of all respondents/a	Number of victims	Percent of all reespondents/a	No past year id theft
Total	96.63	0.55	69.41	0.55	0.70
Sex					
Male*	69.48	0.55	48.81	0.42	1.03
Female	73.28	0.56 ++	51.24	0.44	0.97
Race/Hispanic origin/b					
White*	74.61	0.57	50.68	0.43	0.84
Black	37.47	0.33	28.57	0.26 ++	2.18 ++
Asian	19.71	0.18 ++	11.92	0.11	3.40
Hispanic	48.72	0.42 ++	35.44	0.31 ++	1.91 ++
Other/b	11.98	0.11	5.91	0.05	5.99 +
Two or more races	20.81	0.19 ++	15.25	0.14 +	3.81
Age					
18–24	38.37	0.34 ++	28.02	0.25	2.42 +
25–34	38.19	0.34	27.84	0.25	1.38
35–49*	49.43	0.43	36.39	0.32	1.33
50–64	54.15	0.46 +	36.64	0.32 ++	1.47 ++
65 or older	48.85	0.42 ++	29.82	0.27 ++	1.61 ++
Household income					
$24,999 or less	52.51	0.44 ++	36.44	0.32 ++	1.75 ++
$25,000–$49,999	52.80	0.45 ++	37.59	0.33 ++	1.41
$50,000–$74,999	44.05	0.38 ++	29.15	0.26	1.49
$75,000 or more*	55.88	0.47	38.83	0.34	1.14
Urbanicity					
Urban*	90.60	0.58	65.16	0.52	0.76
Non-urban	38.55	0.34	25.00	0.23 ++	1.97 +
Unknown	6.91	0.06	5.72	0.05 ++	10.19 ++

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 11. Standard errors for Table 11. Prevalence of identity theft during the past 12 months, by type of identity theft, instrument version, and exclusion of attempts

	Version 1 - all		Version 1 - attempts excluded*/a		Version 2		Version 3	
	Number of victims	Percent of all respondents/b	Number of victims	Percent of all respondents/b	Number of victims	Percent of all respondents/b	Number of victims	Percent of all resondents/a
Total	71.10	0.57 ++	69.50	0.56	69.41	0.55 ++	67.40	0.55 ++
Existing account								
Credit card	32.01	0.29	31.70	0.29	31.85	0.28 ++	35.81	0.33
Bank	36.70	0.33	35.54	0.32	38.34	0.34	39.28	0.35
Social media	~	~	~	~	33.93	0.30	~	~
Other	30.20	0.28	29.27	0.27	24.01	0.22 ++	21.83	0.20 ++
New account	14.54	0.14	13.00	0.12	15.68	0.14 +	12.13	0.11
Personal information	10.18	0.10	9.25	0.09	9.34	0.09	10.32	0.10
Multiple types	42.70	0.38	42.22	0.38	24.05	0.22 ++	35.06	0.32 ++

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Excludes victims who selected response option 9 ('not applicable, it was not actually misused) for Q10 (how long had your personal information been misused before you discovered it.')

b/Based on a representative sample of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 12. Standard errors for Table 12. Percentage of victims providing a date of occurrence prior to or outside the 12-month reference period or providing a “don't know” response, by type of identity theft (Version 2)

	Number of victims	Out of reference period/a	Dating error/b	Don't know/missing	Within reference period
Existing account					
Credit card	44.03	1.17 %++	0.35	0.50 +	1.27 ++
Bank	49.23	1.19 %++	0.42	0.44 ++	1.28 ++
Social media	44.19	1.19 %++	0.35	0.60	1.32 ++
Other	37.40	1.55 %++	0.48	0.94	1.74 ++
New account	29.08	2.24 %	1.01	0.80	2.40
Personal information*	19.59	2.65 %	1.32	1.13	2.86

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Includes victims who provided a date of June 2019 or earlier.

b/Includes victims who erroneously provided a date in the future (August/September 2020 or beyond).

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 13. Standard errors for Table 13. Percentage of victims providing a date of occurrence prior to or outside the 12-month reference period or providing a “don't know” response, by characteristics of victims and select types of identity theft (Version 2)

	Credit card misuse					Banking account misuse					New account					Personal information				
	Number of victims	Out of reference period/a	Dating error/b	Don't know/ missing	Within reference period	Number of victims	Out of reference period/a	Dating error/b	Don't know/ missing	Within reference period	Number of victims	Out of reference period/a	Dating error/b	Don't know/ missing	Within reference period	Number of victims	Out of reference period/a	Dating error/b	Don't know/ missing	Within reference period
Total	44.03	1.17	0.35	0.50	1.27	49.23	1.19	0.42	0.44	1.28	29.08	2.24	1.01	0.80	2.40	19.59	2.65	1.32	1.13	2.86
Sex																				
Male*	32.04	1.68	0.59	0.57	1.81	35.54	1.77	0.78	0.66	1.93	21.49	3.30	1.77	0.45	3.48	14.76	3.69	2.18	1.48	4.00
Female	30.66	1.61	0.37	0.83	1.78	34.67	1.61	0.36	0.58	1.70	19.71	2.93	0.81	1.60 +	3.22	12.95	3.79	1.20	1.73	4.04
Race/Hispanic origin/c																				
White*	31.15	1.38	0.21	0.80	1.55	32.41	1.40	0.06	0.68	1.52	16.90	3.26	0.93	0.29	3.32	10.62	3.46	1.26	1.28	3.65
Black	17.02	4.54 ++	1.30	1.07	4.67 ++	21.66	3.19 +	1.15	1.39	3.45 ++	14.77	5.04	1.77	3.42 +	5.75	7.83	6.75	0.00 +	4.60	7.16
Asian	7.96	4.73	0.00 ++	0.00 ++	4.73	7.55	5.95	2.89	0.00 ++	6.43	3.98	6.05 +	0.00	0.00	6.05 ++	2.91	7.45 +	0.00 +	0.00 ++	7.45 ++
Hispanic	24.25	2.46	1.25	0.66	2.75	27.55	2.78 ++	1.32 ++	0.56	2.93 ++	17.76	4.26	2.58	0.92	4.56 +	14.00	5.10	3.22	1.68	5.55
Other/b	4.48	4.59 +	0.00 ++	0.00 ++	4.59 ++	4.57	13.99	0.00 +	0.00 ++	13.99	1.21	0.00 ++	0.00	0.00	0.00 ++	1.11	21.72	0.00 +	0.00 ++	21.72
Two or more races	6.44	9.10	0.00 ++	1.28	9.10	11.04	2.70 ++	0.00 +	0.73	2.80 ++	4.00	13.15	0.00	0.00	13.15	2.49	9.66	0.00 +	0.00 ++	9.66 +
Age																				
18–24	15.22	5.92	0.00 +	0.50	5.93	20.67	4.13	1.71	1.57	4.41	9.71	7.24	3.14	0.53	7.35	6.91	8.88	0.00	5.45	9.22
25–34	16.29	2.44	0.42	1.24	2.63	21.71	2.28	0.26	0.98	2.40	12.91	3.38 ++	2.11	0.15	3.74 +	9.48	4.53	2.29 +	1.05	4.76
35–49*	22.08	2.25	0.55	0.51	2.33	26.05	2.08	0.84	0.30	2.19	16.59	4.24	1.12	0.84	4.28	9.69	3.97	0.28	1.46	4.13
50–64	23.71	2.31 +	1.20	1.33 +	2.77	24.49	2.59	1.08	0.73	2.80	15.44	3.89 ++	3.28	2.37	5.22 +	10.95	7.27	5.07	2.61	7.79
65 or older	20.86	1.49 ++	0.47	1.20 +	1.95 ++	17.64	2.64 ++	0.00 ++	2.24 ++	3.36 ++	8.85	8.10	0.00	6.83	9.44	5.92	4.62 ++	0.00	6.92	8.20
Household income																				
$24,999 or less	19.82	3.89 ++	0.20 +	1.11	3.96 ++	26.48	3.00 ++	1.24	1.26	3.22 ++	18.10	4.88	1.29	2.47	5.17 +	11.66	5.83	0.41	2.60	5.98
$25,000–$49,999	23.33	2.01	1.20	1.14	2.48	27.62	2.15	1.03	0.75	2.39	16.07	4.14	2.32	0.79	4.49	11.46	4.82	4.03	1.95	5.83
$50,000–$74,999	18.38	2.82 ++	0.69	0.96	2.96 ++	20.14	2.58 ++	0.14	0.88	2.66 ++	10.75	4.89 ++	3.07	0.35	5.17 ++	7.73	5.41	2.18	2.46	5.71
$75,000 or more*	26.53	1.45	0.34	0.80	1.65	24.82	1.85	0.31	0.59	1.94	12.31	3.59	1.52	0.86	3.83	7.70	4.49	2.21	1.75	4.80

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Includes victims who provided a date of June 2019 or earlier.

b/Includes victims who provided a date prior to when the interview occurred (August/September 2020 or later).

a/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 14. Standard errors for Table 14. Relationship between the date of most recent occurrence and the date of discovery, by type of identity theft

		Percentage of victims		
	Total Number	Same month/ year	Different month/ year	Missing/don't know/out of reference period
Existing account				
Credit card	31.85	2.28 %++	2.10 %++	1.59 %
Bank	38.34	2.01 ++	1.86 ++	1.59
Social media	33.93	2.17 ++	1.99 ++	1.55
Other	24.01017	2.85 ++	2.68 ++	1.99
New account	15.68353	4.53	4.71 ++	4.49 +
Personal information*	9.339869	5.30	5.46	3.74
Multiple types	24.05309	3.19 ++	2.99 ++	2.82 +

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 15. Standard errors for Table 15. Relationship between the date of most recent occurrence and the date of discovery, by victim characteristics

		Percentage of victims		
	Total number	Same month/ year	Different month/ year	Missing/don't know/out of reference period
Total	69.41	1.03	0.96	0.79
Sex				
Male*	48.81	1.51	1.43	1.19
Female	51.24	1.41 ++	1.29 ++	1.06
Race/Hispanic origin/a				
White*	50.68	1.29	1.18	0.90
Black	28.57	2.79 ++	2.67 ++	2.49 ++
Asian	11.92	4.87 ++	4.42	4.06
Hispanic	35.44	2.45 ++	2.39 ++	2.05 ++
Other/b	5.91	9.38 ++	9.46	11.03
Two or more races	15.25	5.75	5.34	3.29
Age				
18–24	28.02	3.14	2.88	2.76
25–34	27.84	1.88	1.89	1.49
35–49*	36.39	1.89	1.79	1.55
50–64	36.64	2.29 ++	2.12 ++	1.49 ++
65 or older	29.82	2.68 ++	2.34 ++	1.98
Household income				
$24,999 or less	36.44	2.36 ++	2.29 ++	2.18 ++
$25,000–$49,999	37.59	2.08 ++	2.00 ++	1.54
$50,000–$74,999	29.15	2.18 +	1.97	1.67 ++
$75,000 or more*	38.83	1.66	1.50	1.07
Urbanicity				
Urban*	65.16	1.10	1.02	0.85
Non-urban	25.00	2.96	2.77	2.21
Unknown	5.72	10.83 +	11.30 ++	3.48 ++

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 16. Standard errors for Table 16. Time from discovery of the most recent incident to the interview, by questionnaire version and type of identity theft

		Percentage of victims					
	Total number of victims	Less than 1 month	1-6 months	7-12 months	13-24 months	25-36 months	More than 36 months
Version 1							
Total	69.55	0.92	0.86	0.32	0.30	0.22	0.26
Existing account	68.26	0.94 ++	0.88	0.30	0.31	0.22	0.27
New account	30.60	2.02	2.05 ++	0.93	0.91 ++	0.65 +	1.00
Personal information	21.79	2.12	2.18 ++	0.91	0.93 ++	0.71 ++	1.55
Version 2							
Total	67.67	0.97	0.89	0.39	0.34	0.07	0.14
Existing account	66.94	0.98	0.91	0.38	0.35	0.07	0.14
New account	28.58	2.61	2.49	1.48	1.02	0.16	0.73
Personal information	19.36	2.97	2.90	1.75	1.17	0.17	1.22
Version 3							
Total	65.67	1.04	0.98	0.31	0.41	0.12	0.13
Existing account	64.42	1.07 ++	1.00	0.30	0.43	0.13	0.13
New account	21.96	2.55 ++	2.55	1.12	0.78	0.35	0.12 +
Personal information	19.21	2.53 ++	2.43 ++	0.93	2.01 +	0.52	0.12 ++

Note: Based on unweighted data. Includes victims who provided a month and year of discovery. For version 1 about 2% of victims were missing the date; version 2 about 1.5%; and version 3 about 4%.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 17. Standard errors for Table 17. Relationship between the time of most recent occurrence and how long the identity theft had been happened when it was discovered

	Lenth of time from interview to most recent occurrence - Version 2							
How long ID theft had been happening when discovered	Same month	1 to 6 months	7 to 12 months	Out of reference period	Dating error/a	Total	Version 1*	Version 3
One day or less (1-24 hours)	3.18	1.40 ++	1.94 ++	2.82 ++	5.03 ++	0.99 ++	0.93	1.05 ++
More than a day, but less than a week (25 hours-6 days)	2.66	1.27 ++	1.77 ++	2.10	4.00 ++	0.88 ++	0.78	0.91 +
At least a week, but less than one month (7-30 days)	2.09	1.04 ++	1.30 +	2.09	3.91	0.71 ++	0.54	0.72 ++
One month to less than three	1.52	0.86 ++	1.12 ++	2.31 ++	8.03 +	0.62 ++	0.51	0.67 ++
Three months to less than six	1.88 +	0.59	0.77	1.32 +	9.49 ++	0.47 ++	0.31	0.36
Six months to less than one year	1.06	0.44	0.72	0.76	8.61	0.35	0.30	0.21
One year or more	0.60	0.40	0.41	1.21 ++	0.45 ++	0.27	0.23	0.25
Not applicable, not actually misued	~	~	~	~	~	~	0.41	~
Unknown	1.89	0.76	1.01	2.15 ++	5.32	0.57	0.52	0.73 ++
Total Count	26.65	48.00	35.49	24.50	9.06	68.65	70.96	67.21

Note: Includes victims who provided a month and year of most recent occurrence. The percentage of victims not providing a month or year varied depending on the type of identity theft but was generally less than 1%.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Includes victims who provided a date prior to when the interview occurred (August/September 2020

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 18. Standard errors for Table 18. Prevalence of identity theft in the past 12 months, by type of identity theft, survey administrator, and mode

			NORC Version 1					
	2018 Census ITS*		Total		Web		Phone	
	Number of victims	Percent of all adults/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/
Total	404,533	0.13 %	71.10	0.57 %+	69.94	0.58 %+	13.92	2.26 %
Existing account								
Credit card	249,521	0.09	46.88	0.42 +	46.04	0.43 +	9.19	1.57
Bank	247,852	0.09	53.49	0.47 +	52.64	0.48 +	9.89	1.67
Other	105,612	0.04	48.58	0.43 +	47.95	0.45 +	8.07	1.39
New account	83,565	0.03	31.63	0.29 +	31.13	0.30 +	5.65	0.98
Personal information	57,890	0.02	22.14	0.21 +	21.51	0.21 +	5.27	0.92

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

~Not applicable.

a/Based on the population of US residents age 16 or older.

b/Based on a representative sample of US residents age 18 or older.

Source: Bureau of Justice Statistics, Identity Theft Supplement, 2018; 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 19. Standard errors for Table 19. Persons ages 18 or older who experienced one or more incidents of identity theft during the past 12 months, by victim characteristics, survey administrator, and mode

			NORC Version 1					
	2018 Census ITS*		Total		Web		Phone	
	Number of victims	Percent of all persons 16+	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a	Number of victims	Percent of all respondents/a
Total	404,533	0.13	71.10	0.57 %+	69.94	0.58 %+	13.92	2.26 %+
Sex								
Male	218,952	0.15	52.72	0.84 %+	52.17	0.86 %+	7.89	3.44 %+
Female	266,345	8.96	50.17	0.76 +	48.94	0.79 +	11.48	2.94 +
Race/Hispanic origin/b								
White	340,618	0.16	53.86	0.68 %+	52.90	0.70 %+	10.63	2.82 %+
Black	115,445	0.36	24.81	1.69 +	24.01	1.79 +	6.32	4.67 +
Asian	72,413	0.43	14.95	2.56 +	14.94	2.57 +	0.63	16.01 +
Hispanic	111,287	0.26	37.72	1.60 +	37.34	1.60 +	5.40	10.41
Other	21,422	1.29	6.88	5.11 +	6.50	5.81 +	2.26	8.77
Two or more races	44,813	1.18	11.37	3.13 +	11.08	3.28 +	2.55	10.11
Age								
16-17	23,084	0.29		%+		%+		%
18–24	109,226	0.31	33.56	2.06 +	33.56	2.06 +	0.00	
25–34	152,687	0.29	29.04	1.23 +	29.02	1.23 +	0.94	18.67
35–49	174,922	0.23	36.08	1.10 +	35.91	1.10 +	3.51	12.14 +
50–64	177,378	0.25	36.65	1.14 +	35.64	1.16 +	8.67	5.44 +
65 or older	124,257	0.21	28.65	1.12 +	26.79	1.25 +	10.28	2.43 +
Household income								
$24,999 or less	116,448	0.23	38.71	1.29 %+	37.44	1.38 %+	9.95	3.32 %+
$25,000–$49,999	173,663	0.24	36.34	1.09 +	35.52	1.12 +	7.83	4.66 +
$50,000–$74,999	152,880	0.27	30.50	1.23 +	30.12	1.25 +	4.88	6.86 +
$75,000 or more	265,643	0.21	40.77	0.98 +	40.66	0.99 +	3.14	4.02 +
Urbanicity								
Urban	260,802	0.21	66.80	0.62 %+	65.78	0.63 %+	12.47	2.59 %+
Non-urban	355,987	0.16	26.05	1.48 +	25.32	1.55 +	6.20	4.58 +
Unknown	~	~	4.81	9.39	4.81	9.39	0.00	

Note: Percentages are based on the number of persons in each category.

*Comparison group.

†Significant difference from comparison group at 95% confidence level.

‡Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: Bureau of Justice Statistics, Identity Theft Supplement, 2018; 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 20. Standard errors for Table 20. Prevalence of identity theft in the past 12 months accounting for Version 2 victims who failed to provide dates of occurrence or who provided dates of occurrence outside the reference period, by type of identity theft, victim race/Hispanic origin, and instrument version

	Version 1		Version 2 -ORIGINAL		Version 2 - NEW*		Version 3	
	Number of victims	Percent of all resondents/a	Number of	Percent of all resondents/a	Number of victims/b	Percent of all resondents/a	Number of victims	Percent of all resondents/a
Total	71.10	0.57 ++	69.41	0.55 ++	62.09	0.51	67.40	0.55 ++
Type of ID theft								
Existing account								
Credit card	46.88	0.42 ++	44.03	0.38 ++	39.99	0.35	45.62	0.41 ++
Bank	53.49	0.47 ++	49.23	0.42 ++	43.39	0.38	50.65	0.44 ++
Social media	~	~	44.19	0.38 ++	39.82	0.35	~	~
Other	48.58	0.43 ++	37.40	0.33 ++	32.08	0.29	38.43	0.35 ++
New account	31.63	0.29 ++	29.08	0.26 ++	24.03	0.22	22.35	0.21 ++
Personal information	22.14	0.21 ++	19.59	0.18 ++	15.58	0.14	19.55	0.18 ++
Race/Hispanic origin/c								
White	53.86	0.47 ++	50.68	0.43 ++	45.02	0.39	47.51	0.42 ++
Black	24.81	0.23 ++	28.57	0.26 ++	24.88	0.22	27.43	0.25
Asian	14.95	0.14 ++	11.92	0.11 +	10.72	0.10	12.20	0.11 +
Hispanic	37.72	0.34 ++	35.44	0.31 ++	31.80	0.28	36.87	0.33 ++
Other	6.88	0.06 ++	5.91	0.05	5.23	0.05	6.93	0.07 +
Two or more races	11.37	0.11	15.25	0.14	14.10	0.13	13.21	0.12

Note: Standard errors provided in appendix tables.

~Not applicable.

*Comparison group.

+Significant difference from comparison group at 95% confidence level.

++Significant difference from comparison group at 90% confidence level.

a/Based on a representative sample of US residents age 18 or older.

b/Includes only victims who provided dates of occurrence within the reference period.

c/White, black, Asian other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 21. Standard errors for table 22. Unweighted prevalence of identity theft in past 12 months, by type of identity theft and mode

	Total		Web		Phone	
	Number of victims	Percent of surveyed adults/a	Number of victims	Percent of surveyed adults/a	Number of victims	Percent of surveyed adults/a
Total	87.57	0.27	87.23	0.28	16.24	1.14
Existing account						
Credit card	70.25	0.22	69.69	0.22	11.20	0.84
Bank	74.47	0.23	74.02	0.24	10.89	0.81
Social media	39.14	0.12	38.84	0.13	5.10	0.40
Other	66.76	0.21	66.47	0.21	7.61	0.58
New account	57.62	0.18	57.39	0.19	5.91	0.46
Personal information	54.37	0.17	54.15	0.17	5.47	0.42

a/Based on a representative sample of the population of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 22. Standard errors for Table 23. Unweighted prevalence of identity theft in the past 12 months, by type of identity theft and platform

	Total		AmeriSpeak		Lucid		MTurk	
	Number of victims	Percent of surveyed adults/a	Number of victims	Percent of surveyed adults/a	Number of victims	Percent of surveyed adults/a	Number of victims	Percent of surveyed adults/a
Total	87.57	0.27	56.49	0.45	60.67	0.46	63.79	0.50
Existing account								
Credit card	70.25	0.22	39.09	0.34	43.02	0.36	48.09	0.43
Bank	74.47	0.23	38.40	0.33	49.34	0.40	51.53	0.45
Social media	39.14	0.12	20.34	0.18	22.75	0.20	25.58	0.25
Other	66.76	0.21	31.87	0.28	41.70	0.35	47.57	0.43
New account	57.62	0.18	21.95	0.20	36.78	0.31	41.81	0.39
Personal information	54.37	0.17	18.26	0.16	34.97	0.30	39.94	0.37

a/Based on a representative sample of the population of US residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 23. Standard errors for Table 24. Unweighted persons age 18 or older who experienced one or more incidents of identity theft during the past 12 months, by victim characteristics and mode

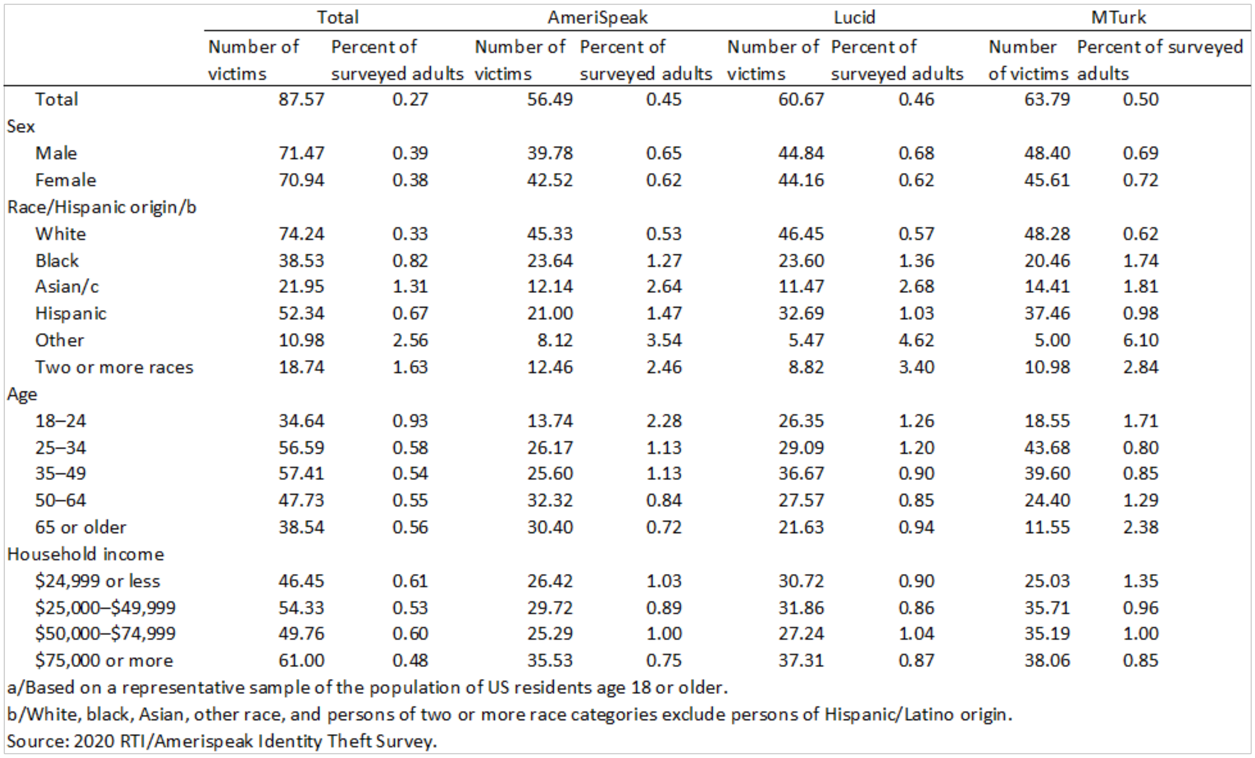
	Total		Web		Phone	
	Number of victims	Percent of surveyed adults	Number of victims	Percent of surveyed adults	Number of victims	Percent of surveyed adults
Total	87.57	0.27	87.23	0.28	16.24	1.14
Sex						
Male	71.47	0.39	71.07	0.40	9.63	1.90
Female	70.94	0.38	70.18	0.39	13.12	1.42
Race/Hispanic origin/b						
White	74.24	0.33	73.64	0.34	12.54	1.36
Black	38.53	0.82	37.86	0.86	7.48	2.54
Asian/c	21.95	1.31	21.86	1.32	2.00	15.49
Hispanic	52.34	0.67	52.20	0.68	4.24	5.29
Other	10.98	2.56	10.52	2.73	3.16	7.14
Two or more races	18.74	1.63	18.21	1.70	4.47	5.72
Age						
18–24	34.64	0.93	34.64	0.93	0.00	0.00
25–34	56.59	0.58	56.57	0.58	1.73	10.33
35–49	57.41	0.54	57.33	0.55	3.46	6.47
50–64	47.73	0.55	46.97	0.56	9.21	2.57
65 or older	38.54	0.56	36.53	0.62	12.85	1.29
Household income						
$24,999 or less	46.45	0.61	45.47	0.64	10.23	1.74
$25,000–$49,999	54.33	0.53	53.74	0.54	8.99	2.10
$50,000–$74,999	49.76	0.60	49.47	0.61	5.83	3.27
$75,000 or more	61.00	0.48	60.72	0.48	6.78	2.84

a/Based on a representative sample of the population of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Appendix Table 24. Standard errors for Table 25. Unweighted persons age 18 or older who experienced one or more incidents of identity theft during the past 12 months, by victim characteristics and platform



	Total		AmeriSpeak		Lucid		MTurk	
	Number of victims	Percent of surveyed adults	Number of victims	Percent of surveyed adults	Number of victims	Percent of surveyed adults	Number of victims	Percent of surveyed adults
Total	87.57	0.27	56.49	0.45	60.67	0.46	63.79	0.50
Sex								
Male	71.47	0.39	39.78	0.65	44.84	0.68	48.40	0.69
Female	70.94	0.38	42.52	0.62	44.16	0.62	45.61	0.72
Race/Hispanic origin/b								
White	74.24	0.33	45.33	0.53	46.45	0.57	48.28	0.62
Black	38.53	0.82	23.64	1.27	23.60	1.36	20.46	1.74
Asian/c	21.95	1.31	12.14	2.64	11.47	2.68	14.41	1.81
Hispanic	52.34	0.67	21.00	1.47	32.69	1.03	37.46	0.98
Other	10.98	2.56	8.12	3.54	5.47	4.62	5.00	6.10
Two or more races	18.74	1.63	12.46	2.46	8.82	3.40	10.98	2.84
Age								
18–24	34.64	0.93	13.74	2.28	26.35	1.26	18.55	1.71
25–34	56.59	0.58	26.17	1.13	29.09	1.20	43.68	0.80
35–49	57.41	0.54	25.60	1.13	36.67	0.90	39.60	0.85
50–64	47.73	0.55	32.32	0.84	27.57	0.85	24.40	1.29
65 or older	38.54	0.56	30.40	0.72	21.63	0.94	11.55	2.38
Household income								
$24,999 or less	46.45	0.61	26.42	1.03	30.72	0.90	25.03	1.35
$25,000–$49,999	54.33	0.53	29.72	0.89	31.86	0.86	35.71	0.96
$50,000–$74,999	49.76	0.60	25.29	1.00	27.24	1.04	35.19	1.00
$75,000 or more	61.00	0.48	35.53	0.75	37.31	0.87	38.06	0.85

a/Based on a representative sample of the population of US residents age 18 or older.

b/White, black, Asian, other race, and persons of two or more race categories exclude persons of Hispanic/Latino origin.

Source: 2020 RTI/Amerispeak Identity Theft Survey.