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

Document Title: Assessing the Measurement of Identity Theft through the Identity Theft Supplement to the National Crime Victimization Survey

Authors:
Lynn Langton, PhD, RTI International
Christopher Krebs, PhD, RTI International
Patrick Hsieh, PhD, RTI International
Sarah Cook, RTI International
Philip Lee, RTI International
Jeanne Snodgrass, RTI International
Herschel Sanders, RTI International

BJS Project Managers:
Erika Harrell, PhD, Statistician
Grace Kena, Statistician

Document No.: NCJ 306383

Publication Date: October 2023

Award No.: This project was supported by award number 2017-MU-MU-K048.

Abstract:

This report describes efforts to assess potential sources of measurement error in the Identity Theft Supplement (ITS) to the National Crime Victimization Survey (NCVS). The ITS is the key source of data on the prevalence and nature of identity theft victimization in the United States. The assessment included (1) an analysis of ITS data to examine three central issues in the measurement of identity theft: the definition of identity theft and the scope of incidents included under that label, the unbounded nature of the estimates and the potential for telescoping due to the ITS being administered less frequently than the core NCVS, and the inclusion of attempted incidents; (2) cognitive testing of the recommended changes to the survey instrument based on findings from the data analysis; and (3) an online pilot test of three versions of the ITS instrument to assess which approach produced the most-accurate and most-reliable measures of identity theft victimization.

Disclaimer

The Bureau of Justice Statistics (BJS) funded this third-party report. It is not a BJS report and does not release official government statistics. This report is released to help inform interested parties of the research or analysis contained within and to encourage discussion. BJS has performed a limited review of the report to ensure the general accuracy of information and adherence to confidentiality and disclosure standards. Any statistics included in this report are not official BJS statistics unless they have been previously published in a BJS report. Any analysis, conclusions, or opinions expressed herein are those of the authors and do not necessarily represent the views, opinions, or policies of the BJS or U.S. Department of Justice.

Caveat

This report was completed in 2019 and 2020. Since then, there may have been updates to the ITS data collection described in this report. Please refer to the BJS website for updated information (https://bjs.ojp.gov/data-collection/identity-theft-supplement-its).

This page intentionally left blank.

National Victimization Statistical Support Program (NVSSP)
Cooperative Agreement (COA) 2017-MU-MU-K048
RTI Project Number: 0217713

Assessing the Measurement of Identity Theft through the Identity Theft Supplement to the National Crime Victimization Survey

October 2023

Prepared for
Bureau of Justice Statistics
810 Seventh Street, NW
Washington, DC 20001

Prepared by
Lynn Langton, PhD
Christopher Krebs, PhD
Patrick Hsieh, PhD
Sarah Cook
Philip Lee
Jeanne Snodgrass
Herschel Sanders

RTI International
3040 E. Cornwallis Road
Post Office Box 12194
Research Triangle Park, NC 27709-2194

This page intentionally left blank.

Contents

Section **Page**

Appendices

Figures

Number **Page**

This page intentionally left blank.

Tables

Executive Summary

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. The ITS is used to generate estimates of the prevalence and nature of identity theft victimizations nationwide. The survey collects 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.

In 2019, BJS asked RTI International to conduct a review of state identity theft laws and a secondary data analysis to examine several key issues in the ITS that affect how identity theft is measured and described in reports and the resulting prevalence estimates. The issues examined included (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 consider using a dual reference period in the screener to reduce the likelihood of respondents telescoping incidents into the 12-month reference period; 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; and ask respondents to focus only on successfully completed incidents of identity theft rather than attempted incidents, which introduces considerable error to the estimates.

Using findings from the secondary data analysis, BJS and RTI created two revised versions of the ITS screener, one incorporating all recommended changes (Version 2) and one only addressing the issue of attempted versus completed incidents (Version 3). RTI conducted cognitive interviews with 27 adults in May 2020 using the fully revised version of the instrument. 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.

From July 16, 2020, to August 4, 2020, RTI International and NORC at the University of Chicago successfully administered a randomized test of three versions of the ITS screener to more than 31,000 respondents, recruited through three online survey platforms: AmeriSpeak®, a probability-based panel, and Lucid and Mechanical Turk (MTurk), two nonprobability panels. The current ITS instrument, which is fielded as part of the NCVS, was Version 1. Version 2 was a revised instrument designed to control for telescoping through the use of a dual reference period, up-front dating of the most recent occurrence,

[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 through 7 are bounded by the prior interview, the ITS and other NCVS supplements are completely unbounded.

and the exclusion of attempted incidents. Version 3 was similar to Version 1; however, it excluded attempted incidents.

The goal of the test was to determine which of the three versions of the screener produced the most-accurate estimates of the prevalence of identity theft with the highest degree of data quality. 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 most were able to identify the month and year of the occurrence. Based on these findings, we recommended Version 2 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, item missingness was low, 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. Online platforms are a cost-effective and efficient way to quickly obtain a magnitude of responses and are useful for testing how well different versions of survey questions perform in the field.

Assessing the Measurement of Identity Theft

1 Introduction

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 President's Identity Theft Task Force Report (2008) that BJS should periodically administer identity theft survey supplements to collect detailed individual-level data on the prevalence and consequences of identity theft. Prevalence refers to the number of unique persons that experienced one or more identity thefts in a given time period.

The first iteration of the ITS was administered in 2008 to all NCVS respondents age 16 or older during a 6-month period. After a redesign to address identified problems with the initial survey instrument and measurement approach,[3] the ITS was then administered in 2012, 2014, 2016, and 2018 using an instrument that remained largely unchanged from one administration to the next to enable analysis of trends over time.

For the ITS, identity theft is defined as "the unauthorized use or attempted use of existing accounts, or the unauthorized use or attempted use of personal information, to open a new account or for other fraudulent purposes" (Langton & Planty, 2010). BJS uses the survey 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. It also captures known incidents in which an offender attempts to use a person's identifying information but is unsuccessful at obtaining goods or services. However, BJS has not historically distinguished between attempted and successful incidents in reports on identity theft.

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, including a review of state identity theft laws to better understand the scope of incidents covered by state statutes (see Appendix A), BJS asked RTI International to conduct a secondary data analysis to examine several key issues in the ITS that affect how identity theft is measured and described in reports and the resulting prevalence estimates. The issues examined included (1) the unbounded nature of the estimates and the potential for telescoping;[4] (2) the ongoing, episodic nature of many incidents and specific dating of incidents to determine whether

[3] The changes and rationale for the changes were documented with the materials submitted in the 2012 Office of Management and Budget Paperwork Reduction Act Information Collection Review package, available at https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201112-1121-004.

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

they should be included within the survey reference period; and (3) the inclusion of attempted incidents in the definition of identity theft. 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; correctly collecting and identifying attempted incidents poses challenges, and the grouping of attempted and completed incidents muddles understanding of and appreciation for the severity of completed incidents.

Drawing on findings from the secondary data analysis, BJS and RTI created two revised versions of the ITS screener (see Appendix C). RTI conducted cognitive interviews with 27 adults in May 2020 to test whether respondents understood the wording of the revised questions and were able to place incidents in the time periods asked about in the survey. 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. From July 16, 2020, to August 4, 2020, RTI and NORC successfully administered a randomized test of the three versions of the 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.

This report describes (1) the secondary data analysis and the findings that led to the subsequent revisions to the ITS survey instrument, (2) the process of conducting cognitive interviews of the revised survey and findings from that effort, and (3) the process of and findings from the large pilot test of three versions of the instrument.

2 Analysis of ITS Data

This section presents findings and recommendations from the secondary analysis of ITS data. Using existing ITS data, RTI examined several key measurement issues that affect 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 chapter presents these three measurement issues, findings from the data, and resulting recommendations. Key recommendations for changes to the ITS are as follows:

- Continue to use the most recent occurrence[5] 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 the most recent known occurrence to ensure that incidents are within the 12-month survey reference period.
- Consider using a dual 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 theft 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 the 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 affecting trends in overall prevalence rates.

2.1 Reference Points

Measurement challenges: Most crimes are discrete events that occur on a particular date. 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. Several key points in an identity theft incident could be used for dating and determining whether the incident is within the reference period, including

- when the offender first started misusing the victim's information (start),[6]
- when the victim discovered that their information was being misused (discovery),
- the last occurrence of misuse (occurrence), and
- when the victim resolved all financial and credit problems related to the identity theft (resolution).

[5] The word "occurrence" is used rather than "incident" because of the focus on reference points *within* an incident—when it started, when it was discovered, and the most-recent time it happened/occurred (as 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 in other situations, the offender misuses the victim's information multiple times. It was necessary to make sure multiple misuses were being captured as well.

[6] 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, or other role.

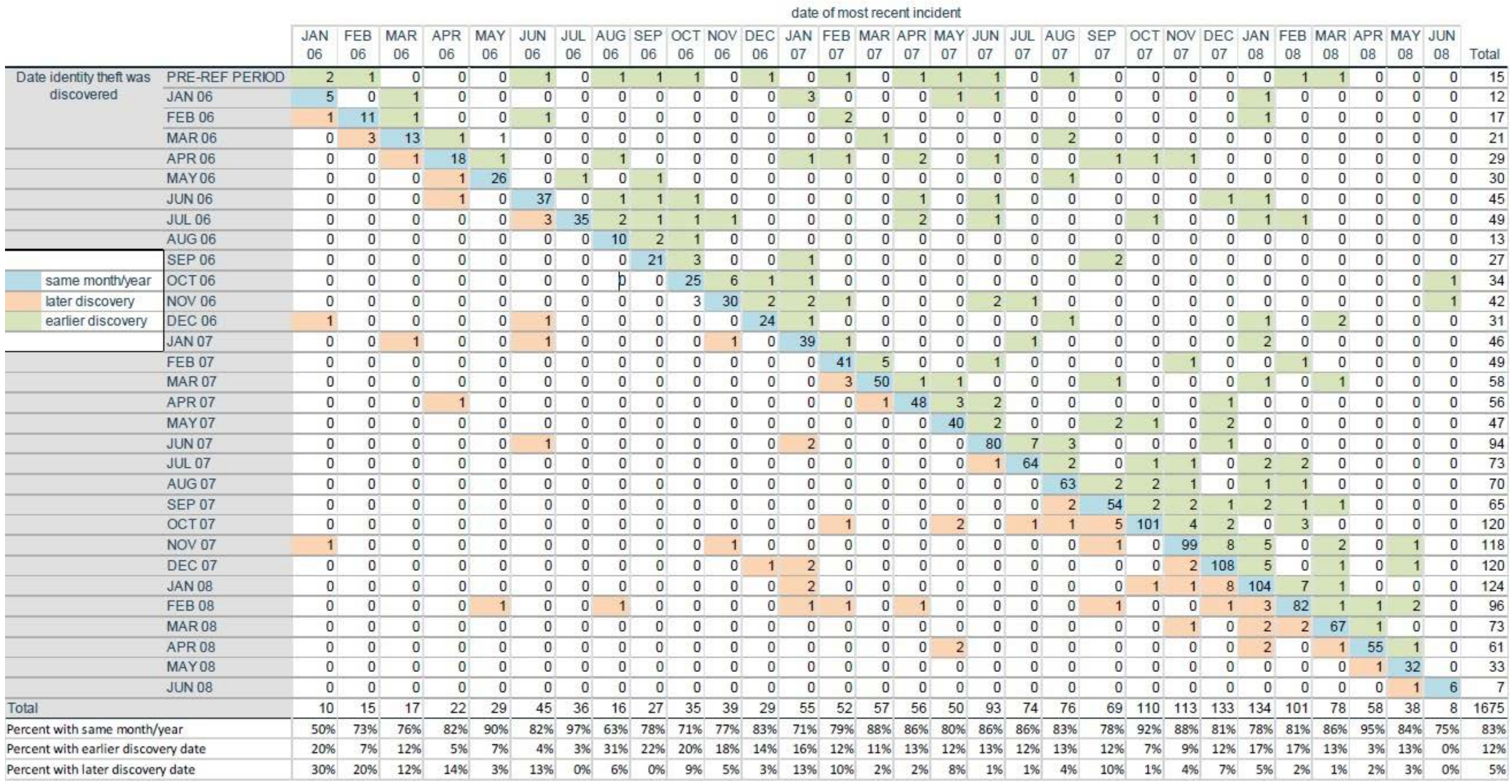
Although the last item is critical for understanding the severity and harms of identity theft, using it to date an incident is akin to dating an assault based on when the victim was released from the hospital. Additionally, when determining whether an incident is within the reference period, dating an 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 the first three points for understanding dating and whether 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 whether 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 and 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 when the offender used their information.

Part of the rationale for not asking about the most recent or last occurrence of misuse was because of 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, though, 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, the victim 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 2-year reference period and asked victims about both 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 2-1. 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 2-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 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 2-1:   Date Identity Theft was Discovered and Date of Most Recent Identity Theft Occurrence, 2008

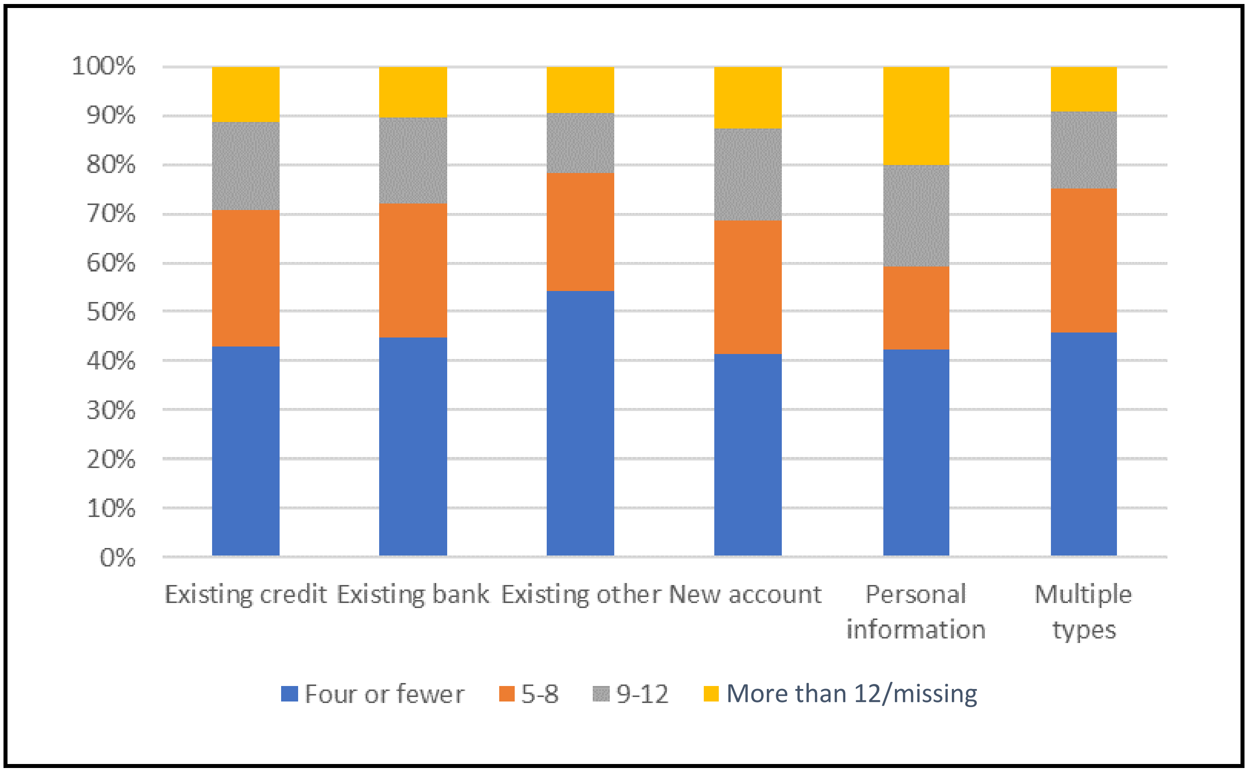


		date of most recent incident																													
		JAN 06	FEB 06	MAR 06	APR 06	MAY 06	JUN 06	JUL 06	AUG 06	SEP 06	OCT 06	NOV 06	DEC 06	JAN 07	FEB 07	MAR 07	APR 07	MAY 07	JUN 07	JUL 07	AUG 07	SEP 07	OCT 07	NOV 07	DEC 07	JAN 08	FEB 08	MAR 08	APR 08	MAY 08	JUN 08	Total
Date identity theft was discovered	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%

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2008.

Figure 2-2, 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 before the interview date (not shown).[7] This 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. Because the instrument does not ask when the actual misuse stopped, it is difficult to ascertain which explanation is more likely or prevalent.

Figure 2-2: Months from Discovery of Identity Theft to Interview, by Type of Identity Theft, 2018



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

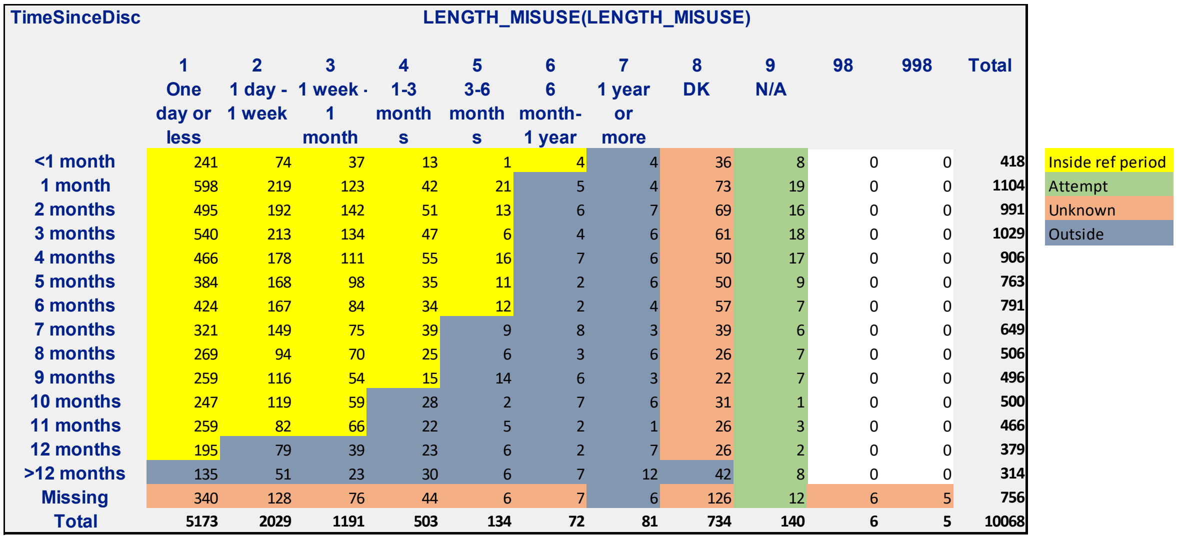
For all types of identity theft, except for personal information misuse, about 90% of victims provided a discovery date that was within the 12-month reference period.

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 (including victims who stated that their information was not actually misused) discovered the most recent incident of identity theft one day or less after misuse started. When the analysis is limited to victims who were not missing data about when the misuse started, that percentage increases to 58%.

[7] Excludes victims for whom the discovery date was missing. In the figure, the percentages for *discovery date more than 12 months before the interview date* and *missing discovery date* are combined into one category.

Figure 2-3 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 before discovery. For example, if the victim provided a date of discovery that was 3 months before the interview and then responded that the start of misuse was 3 to 6 months before discovery, both the discovery date and the start date are within the reference period because we know that the start date was no more than 9 months before 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 3 to 6 months before discovery, we assumed 6 months rather than 3 months.

Figure 2-3: Relationship Between Number of Months from Discovery to Interview and Whether the Misuse Started Inside or Outside of the Reference Period, 2018



TimeSinceDisc	LENGTH_MISUSE(LENGTH_MISUSE)											
	1 One day or less	2 1 day - 1 week	3 1 week - 1 month	4 1-3 months	5 3-6 months	6 6 month-1 year	7 1 year or more	8 DK	9 N/A	98	998	Total
<1 month	241	74	37	13	1	4	4	36	8	0	0	418
1 month	598	219	123	42	21	5	4	73	19	0	0	1104
2 months	495	192	142	51	13	6	7	69	16	0	0	991
3 months	540	213	134	47	6	4	6	61	18	0	0	1029
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

Inside ref period
Attempt
Unknown
Outside

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

Using the classification above, Table 2-1 shows the relationship between whether the discovery was inside the reference period and whether the start of misuse was inside the reference period, according to 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.

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 2-2). About 30% of victims of new account misuse and 40% of victims of personal information misuse did not know when the misuse started.

Table 2-1: 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

Number of Months Since First Discovery	Total		Start of Misuse							
			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.

Table 2-2: Incidents for Which the Start of Misuse Was Inside or Outside the 12-Month Reference Period, by Type of Identity Theft, 2018

Number of Months Since First Discovery	Start of Misuse							
	Inside Reference Period		Outside Reference Period		Attempt		Unknown	
	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 2-3 shows the impact on prevalence rates of excluding victims for whom either the discovery or start of the most recent incident was unknown or outside the reference period. Not surprisingly, the shift in reference points appears to have the greatest impact on the misuse of personal information for other purposes, reducing the number of victims by about 45%.

Table 2-3: Change in Identity Theft Prevalence Rate if Reference Period Was Based on Incident Discovery Date or Start Date, 2018

			Prevalence Based on			
Type of Most Recent Incident	**Prevalence**		**Discovery Date[a]**		**Start of Misuse[b]**	
	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

[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 before the interview.

[b] Excludes victims who experienced a single incident during the reference period and for whom the start of the misuse was unknown or more than 12 months before the interview.

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

Recommendations: To maintain trends in the prevalence of identity theft and not make major changes to the screener questions, BJS should continue to use the 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 and 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 1-year reference period.

To ensure 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 before 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 the date of discovery. If a respondent provides a date of the most recent occurrence that is outside of the reference period, that respondent 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 be asked in the screener section of the instrument (see more-detailed recommendations under *Respondent Telescoping*). Cognitive testing is 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 is also important for determining whether additional clarifying language is needed to help respondents understand the concept of the most recent occurrence of misuse.

The benefit of 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 episodes in time. The drawback to this change is that it could affect 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 being asked more-specific dating questions.

2.2 Respondent Telescoping

Measurement challenges: Unlike the core NCVS, for which interviews 2 through 7 are bounded by the prior interview, the ITS and other NCVS supplements are completely unbounded. Because the ITS is administered every 2 years, in any given ITS administration, most 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 2 years since they last completed the survey, and the reference period extends to 1 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 them.

Telescoping could occur for several different reasons: (1) it could be intentional, which occurs when respondents want to talk about their experiences even though they are outside of the reference period; (2) it could occur because of recall issues if respondents are not sure about the date of the incident and place it more recently 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, the respondent may think of that incident as ongoing and being within the reference period, particularly if the survey questions do not provide clear guidance.

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 the 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 alone cannot 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 they 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 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. Most experienced the misuse of an existing account, with 80 victims experiencing existing credit card misuse in both periods and 34 experiencing existing bank account misuse 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 2-4 compares the characteristics of the most recent incident among victims who reported the same type of incident during both interviews. It presents unweighted counts because 2014 and 2016 use different weights, which would affect the comparability. For most questions, very few respondents provided substantive responses that were consistent across both interview waves. One exception is reporting to police: most respondents said "no" across both interview waves. This cannot be taken as an indication of telescoping, however, as 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 2-4 (not shown), which suggests that they are not likely to be reporting on the same incident across both waves.

Table 2-4: 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

	Existing Credit Card	Existing Bank Account
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

Note: Table compares the characteristics of the most recent reported incident in 2014 to the most recent reported incident in 2016.

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

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 the 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, particularly long-term incidents for which they are still experiencing problems. For this analysis, we use 2018 data because of the more specific dating of incident discovery. Table 2-5 shows that between 1.1 and 1.3% of victims who discovered their most recent incident within the prior 12 months were also 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 discovered their most recent incident more than 12 months before the interview, that percentage increased to 4.2%. This apparently 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 2-5: 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, Percent			
		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% because of missing data.

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

Similarly, ***Table 2-6*** 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 with inside the reference period.

Table 2-6: 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, Percent			
		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% because of 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 victims whose most recent incident either started or was discovered outside the reference period. Table 2-7 shows that there does appear to be a relationship between 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, whereas 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, 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 that incident outside of the reference period reported the misuse of personal information to open a new account in the long-term consequences section.

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).[8] Part of this may be because of 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).

Table 2-7: 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

Most Recent Identity Theft That Started or Was Discovered Outside of Reference Period	Identity Theft Experienced Outside of Prior 12 Months					
	Existing Credit	Existing Bank	Other Existing	New Account	Other Fraudulent Purpose	None
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% because of 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.

Both sections of the instrument also asked victims a series of questions about problems they experienced as a result of the identity theft. Table 2-8 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, findings cannot be taken as conclusive evidence that the victims were reporting on the same incident in both sections.

[8] 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 give a specific monetary value. For this analysis, we compared whether the monetary value in the most-recent incident section was within the range selected in the long-term consequences section.

Table 2-8: 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 sections of the instrument and for whom the start date or discovery date was outside of the reference period. Both yes means that the respondent experienced the type of problem as a result of both the most recent and long-term incident. Both no means that the respondent did not report experiencing the problem because of the most recent or a long-term incident.

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 1-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 for 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 a yes/no answer 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. 5 years), but would otherwise flow like this:

- **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**)
- **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)**
- **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)
- **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 affecting estimates from the period of interest. Although researchers have found that natural sequence is key for internal bounding and that asking for 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, as 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 2 months followed by 6 months; 6 months followed by 2 months; and the prior month followed by the prior 2 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 (SAMHSA) 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, SAMHSA 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, asks respondents questions about lifetime, 3-year, and 1-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 control telescoping. This may be because 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 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 5-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 total pool of victims. Although asking lifetime questions first should serve to reduce any forward telescoping caused by respondents' 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 5-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 enough respondents to determine statistically significant differences in 1-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 before web-based testing to ensure that the added reference period is not overly complicated or challenging for respondents to follow.

2.3 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 on identity theft 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:

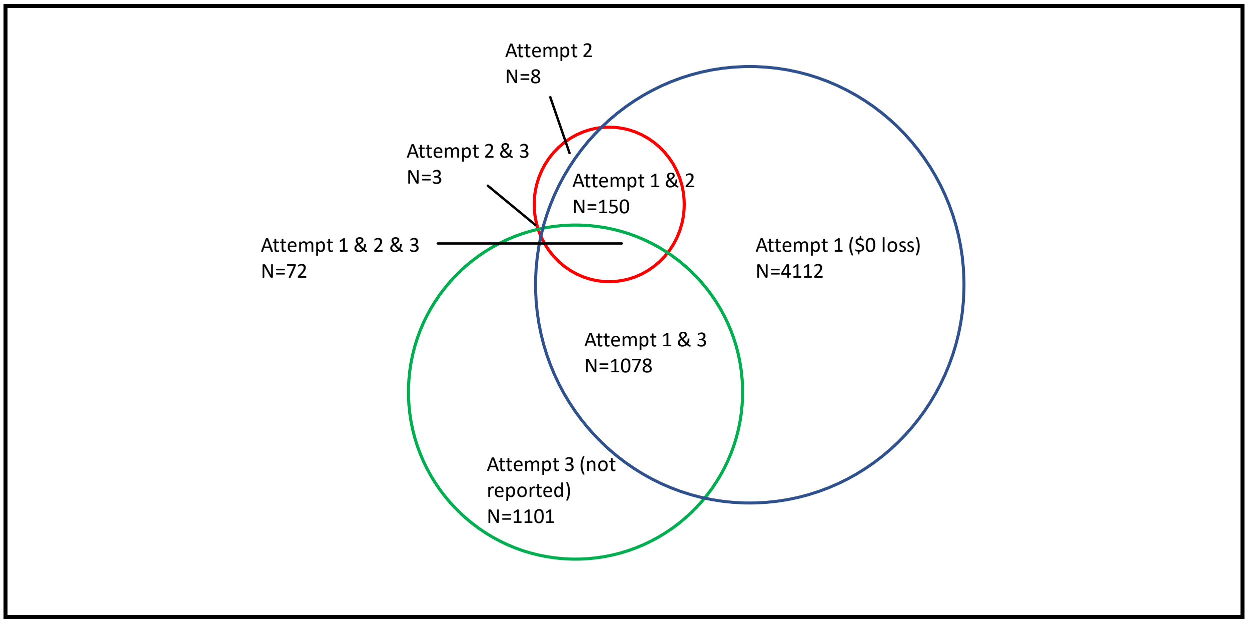
1. The distinction could be based on whether the offender was able to obtain something of value (money, products, services, benefits) from the victim.[9] If the offender was not able to obtain anything from the misuse, we assume that third-party intervention stopped the attempt. However, although this distinction works for existing account misuse, it 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 the offender 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.

[9] 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.

2. The survey asks respondents (Q10) how long their information was misused before they discovered it, and one of the response options (option 9) 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. Victims who did not report the incident to law enforcement can give "I did not lose any money/it was an attempt" as a reason for not reporting. 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 2-4 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 2-4: Venn Diagram of Identity Theft Incidents That Met at Least One of Three Potential Definitions of an Attempt, 2014 and 2016



Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 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 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 2-9). About 23% of victims who experienced $0 in losses from existing account misuse said that they did not report it 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 a 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.

Table 2-9: 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
1 day or less	2,312	53.3	305	28.3
More than 1 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
1 day or less	1,180	58.2	89	39.6
More than 1 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.

In 2014 and 2016, for 2,029 incidents of existing account misuse, victims stated that they did not report to the police because they 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 ”did not suffer a loss” when their direct losses have been reimbursed by a financial institution in addition to when there were no direct losses.

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 because of either of the following:

- Recall failure – victims may be less likely to remember attempted incidents, meaning a higher risk of false negative error 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 2-10 compares the nature of incidents and victim experiences across successful incidents and attempts. Attempts are measured in three ways. From most to least conservative, the measurement approaches are as follows:

1. Victims who answered Q10 (how long was your information misused before you discovered it) with response option 9, “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)

Table 2-10: Harms Associated with Attempted ID Theft Incidents Compared to Successfully Completed Incidents, 2014 and 2016

	Attempt definition 1				Attempt definition 2				Attempt definition 3			
	Attempts		Completed Incidents[a]		Attempts		Completed Incidents		Attempts		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 difference at 95% confidence between successful and attempt. See Appendix Table B-1 for standard errors

[a] Excludes incidents for which the victim did not respond or gave a “do not know” response.

! Interpret with caution. Estimate based on 10 or fewer sample cases or the coefficient of variation is greater than 50%.

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

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 two of the three criteria in #2 above

On the flip side, the completed incident counts associated with attempt definition 1 include any victims who did not select response option 9 in Q10. The completed incident counts associated with attempt definition 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 attempt definition 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.

Even with the most-inclusive definition of attempts (attempts 3), these incidents account for less than half of the most recent incidents victims experienced. 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, victims may not be made aware of or may 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 are asked to think about the most recent incident of identity theft. Either way, the low number of attempts relative to completed incidents likely suggests that attempts are not being fully enumerated through the NCVS.

Differences in victim experiences: When victims report attempted incidents, combining these with completed incidents may 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 prevalent and less severe than for victims of completed identity theft.

Table 2-10 (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, that 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 2-11). 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 the most recent incident was an attempt. 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.

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 attempts 3 definition would significantly reduce the prevalence of identity theft. However, based on findings from Table 2, it appears likely that attempts 2 is a more-accurate reflection of attempts captured in the survey than attempts 3.

Table 2-11: Change in Identity Theft Prevalence Rate with Removal of Attempted Incidents, 2014 and 2016

			Prevalence Minus Attempts					
	Original Prevalence		Definition 1		Definition 2		Definition 3	
Most Recent ID Theft	Number	Percent	Number	Percent	Number	Percent	Number	Percent
				2014				
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				
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.

The removal of attempts based on any of the three definitions appears to have a larger, though not statistically significant, 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: Given 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:

- 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.” Respondents who say “no” would be treated the same way as respondents who said “no” to the initial screener. In other words, respondents who do not report any other types of identity theft would be treated as nonvictims, with the survey ending after the screener. Respondents who say “yes,” when prompted to think about the most recent incident would also receive an instruction to exclude any incidents in which the offender was not successful in obtaining money, goods, or services.
- 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?” Respondents who say “no” would be treated the same as respondents who said “no” to the initial screener. In other words, if they do not report any other types of identity theft, they would be treated as nonvictims, with the survey ending after the screener. Respondents who say “yes,” when prompted to think about the most recent incident would also receive 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.[10] This might affect BJS' ability to compare trends over time in the nature of and victim 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, 10,068 unweighted persons 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.

2.4 Time in Sample

In a panel design survey like the NCVS, respondent fatigue can affect survey estimates and data quality.[11] 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 before 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 affected by how many NCVS interviews the respondent has participated in. To understand 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 2-12 examines the 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)—response rates did not vary much 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%) than among those who had not (8.9%). Except for 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 those in TIS 1 than for those in TISs 2 through 7. However, this pattern did not hold true among people 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 2-13 shows 2018 prevalence rates by most recent type of identity theft and TIS. Rates of existing bank account misuse were higher in TIS 1 than TISs 2 through 7, and rates of people experiencing multiple types of identity theft during the same incident were higher in TIS 1 than TISs 3 through 7. Otherwise, there were no clear patterns in prevalence rates by TIS.

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

[11] 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 2-12: Identity Theft Supplement Response and Prevalence Rates, by Person TIS and Interview Number, 2018

		Percent								
		Response Rate (unweighted-eligible persons)			ITS Rate (weighted)			ITS Rate (standard errors)		
TIS	Eligible Un-weighted 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 Inter-view 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 2-13: 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.

2.5 Next Steps

Based on the findings and resulting recommendations in this chapter, RTI developed several versions of a revised instrument screener and a testing plan. The next chapter describes efforts 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). These cognitive interviews were used to recommend additional changes to the instrument to better account for potential telescoping. As described in Chapter 4, these proposed changes were then tested through an online pilot test designed to compare the ability of the different versions of the instrument to control telescoping and to assess the effect of changing the ordering of the screener on the types of incidents reported.

3 Cognitive Interviewing

This chapter summarizes RTI findings from 27 adult cognitive interviews on the redesigned version of the BJS 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 because of the COVID-19 pandemic. These findings were used to inform recommendations around changes to the ITS to improve the measurement of identity theft and were incorporated into the subsequent pilot-testing efforts.

3.1 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 an 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 the type of identity theft experienced. An informed consent form was emailed 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 whether they had questions, and received verbal consent to conduct the interview and be recorded.

Table 3-1: 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

Table 3-1 shows the cumulative demographics of participants. Though still a diverse group of participants, some diversity was lost because of participants who changed their minds or did not attend their interviews. Table 3-2 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:

- 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?
- 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?
- 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?
- 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 Table 3.2 consecutively as *Existing (bank), Existing (other), New account,* and *Personal info*. Three of the recruited "nonvictims" 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 3-2: Participant Demographic, Recruitment, and Final Identity Theft Type Data (n=27)

	Time	Age				Identity Theft Type	
P#	**Zone**	**Range**	**Education**	**Gender**	**Race**	**Recruited**	**Final**
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)
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)

AI/AN = American Indian/Alaska Native

3.2 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.

Before conducting any interviews, all interviewers completed training on the cognitive interview protocol and project logistics. All interviews were conducted using a cognitive interview protocol 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.

Before 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.

3.3 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. For many questions, none of the 27 participants had difficulty understanding and answering them as intended. These items did not appear to be problematic and have no recommended changes, so they are not discussed below.

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 EXISTING 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 that listing the types of accounts helped them think about the types of accounts we are asking about but mentioned that they focused on the specific service provider name and then forgot things said after that. Keeping any 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 login attempts they were alerted to on their accounts, but they all knew not to include those.

Several respondents who had their Facebook or Instagram accounts taken over were not sure whether to include that because the language at the end of the question focuses on charges made to the account. 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 theft of an entertainment or social media account.

Recommendation: Move "online payment accounts" to the end of the list and include Venmo with the PayPal example. Revise examples 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 categories, either combined or separate?

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 types of accounts? YES NO
[If yes] What other types 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 because of priming effects from all of the previous questions referring to losing money.

Recommendation: Consider adding, "Include times 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

Some may find the word "actually" from the final sentence 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 because "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 participant 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 because this question is in relation to the past 12 months, we might not need response option 7. However, because of the possibility of reoccurring incidents of identity theft, we see this response option as necessary.

Recommendation: Leave question as-is.

3.4 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, where we try to identify the date of discovery and length of misuse (relative to the date of the most recent incident). For the questions on whether someone had ever experienced identity theft, we probed respondents on how far back they were thinking when answering those questions. One said “lifetime,” and one said, “30 years, since I had my account,” but most 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 because once they recalled an event, they had their answer and did not need to think further. Table 3-3 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 3-3: Responses to “Ever” and “12 Months” Questions

	Existing									
	Bank		Credit Card		Other		New Account		Personal Information	
P#	Ever	12 Mos	Ever	12 Mos	Ever	12 Mos	Ever	12 Mos	Ever	12 Mos
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 and 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 experiences, and all appeared to understand the concepts (see Table 3-4). With the exception of one respondent, all of the participants were able to stop the identity theft relatively quickly after they discovered it.

Table 3-4: 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

4 ITS Screener Online Testing

4.1 The Need for Online Testing

The cognitive interviews were useful for improving the wording and structure of Version 2. However, the BJS and RTI 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.

4.2 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 members from more than 40,000 households and provides sample coverage of approximately 97% of the household population.[12] 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

[12] 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.

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[13] 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 a sample from Amazon's Mechanical Turk (MTurk) nonprobability panel. RTI has considerable experience working with MTurk and has previously found 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 the 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.[14] 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, that it would take between 5 and 15 minutes to complete, and that participation was voluntary, and they 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.

4.3 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 4-1 and 4-2 show the demographic distribution of respondents across the different survey modes and panels.

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

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

Table 4-1: 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 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 4-2: 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 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.

The final sample was weighted using NORC's TrueNorth Calibration approach that benchmarks 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 4-3 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 4-3: 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 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.

4.4 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 6-7 through 6-12). 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)[15] 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 4-18 and 4-19 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,[16] 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 those generated through in-person interviews. The next section of the report describes these findings.

[15] See https://aapor.org/wp-content/uploads/2023/05/Standards-Definitions-10th-edition.pdf for AAPOR response rate definitions.

[16] 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/sites/rvap.uiowa.edu/files/imports/Uploads/2898aa5950/Campus-Climate-Survey-2016.pdf (pp 130-136).

4.5 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.

4.6 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 4-4).

- 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 4-4; 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 4-4).

- 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 4-5).

- 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 4-6).

- 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 4-6).

Table 4-4: 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 Respondent [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 B.
*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 U.S. residents age 18 or older.
Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table 4-5: 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 ++

(continued)

Table 4-5: 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 (continued)

	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]
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 B. 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 U.S. 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 4-6: 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		Number of Victims	Percent of All		Number of Victims	Percent of All	
		Respondents[a]	Victims		Respondents[a]	Victims		Respondents[a]	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 B.

* 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 U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

4.7 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 significantly 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 4-7).

- 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 Black or two or more races were more likely than those who are White to experience identity theft in the prior 12 months, 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 4-8).

- 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 4-8).

- 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 4-8).

- 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 4-9).

- Across most demographic characteristics, most lifetime victims also experienced identity theft during the past 12 months. Black respondents, Hispanic respondents, and respondents 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 4-10).

Table 4-7: Prevalence of Identity Theft, by Type of Identity Theft, Instrument Version, and Reference Period

	12-Month							
	Version 1		Version 2		Version 3		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
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 B.
* 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 U.S. residents age 18 or older.
Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table 4-8: Persons Age 18 or Older Who Experienced One or More Incidents of Identity Theft, by Victim Characteristics, Instrument Version, and Reference Period

	12-Month							
	Version 1		Version 2		Version 3		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 ++

(continued)

Table 4-8: Persons Age 18 or Older Who Experienced One or More Incidents of Identity Theft, by Victim Characteristics, Instrument Version, and Reference Period (continued)

	12-Month							
	Version 1		Version 2		Version 3		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]
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 B.

* 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 U.S. 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 4-9: Relationship Between Lifetime Prevalence and 12-Month Prevalence, by Type of Identity Theft (Version 2)

	Prevalence				Percent of Lifetime Victims,
	Lifetime		12-Month		
	Number of Victims	Percent of All Respondents[a]	Number of Victims	Percent of All Respondents[a]	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 U.S. residents age 18 or older.
Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table 4-10: Relationship Between Lifetime Prevalence and 12-Month Prevalence of Identity Theft, by Victim Characteristics (Version 2)

	Prevalence (Any Identity Theft)				Percent of Lifetime Victims
	Lifetime		12-Month Prevalence		
	Number of Victims	Percent of All Respondents[a]	Number of Victims	Percent of All Respondents[a]	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 B.
* 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 U.S. 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.

4.8 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 on 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 4-11).

- 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 4-11).

Table 4-11: Prevalence of Identity Theft During the Past 12 Months, by Type of Identity Theft, Instrument Version, and Exclusion of Attempts

	Version 1				Version 2		Version 3	
	All		Attempts Excluded*,[a]					
	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[b]
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	~	~	~	~	782	7.16	~	~
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 B.

* 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 U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

4.9 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 types 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 4-12).

- 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 4-13).

- 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 4-1).

- 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.[17]

- 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 4-14). 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 most victims (see Table 4-14).

- 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 differences in the types of identity theft experienced by different

[17] Findings from the secondary data analysis of ITS data conducted by RTI in early 2020.

subpopulations (see Table 4-15). 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.

- All three versions of the questionnaire ask victims to provide the month and year 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 than 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 4-16).

- 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 4-17).

Table 4-12: 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 4-13: 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				
	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
Sex										
Male*	697	17.34	1.14	1.50	80.02	791	20.92	1.80	1.66	75.61
Female	652	15.23	0.82	2.67	81.28	850	18.10	0.77	1.88	79.25
Race/Hispanic origin[c]										
White*	762	14.32	0.53	2.70	82.45	800	15.44	0.10	2.12	82.33
Black	168	24.21 ++	1.81	1.35	72.63 ++	280	22.01 +	1.64	2.43	73.91
Asian	59	17.11	0.00 ++	0.00 ++	82.89	46	19.76	4.10	0.00 ++	76.14
Hispanic	313	17.27	1.99	1.48	79.26	443	27.02 ++	3.06 ++	1.12	68.80 ++
Other[b]	16	6.28 +	0.00 ++	0.00 ++	93.72 ++	15	24.19	0.00 +	0.00 ++	75.81
Two or more races	32	16.80	0.00 ++	1.27	81.94	56	2.72 ++	0.00 +	0.72	96.55 ++
Age										
18–24	122	28.50	0.00 +	0.50	71.00	221	23.45	2.41	2.01	72.14
25–34	269	22.18	1.00	1.35	75.47	398	21.93	0.53	1.77	75.77
35–49*	359	18.84	0.93	0.94	79.29	496	21.28	1.88	0.58	76.27
50–64	330	12.58 +	1.74	3.42 +	82.26	352	16.94	1.16	1.51	80.40
65 or older	270	6.19 ++	0.58	3.33 +	89.91 ++	174	8.62 ++	0.00 ++	5.48 ++	85.89
Household income										
$24,999 or less	227	25.22 ++	0.28 +	1.99	72.51 ++	388	24.08 ++	2.69	2.87	70.36
$25,000–$49,999	330	12.02	1.54	2.21	84.23	451	16.76	1.45	0.84	80.95
$50,000–$74,999	268	21.73 ++	0.88	2.11	75.28 ++	328	22.82 ++	0.25	2.05	74.88
$75,000 or more*	524	12.41	0.99	1.99	84.61	474	15.91	0.64	1.59	81.86

(continued)

Table 4-13: 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) (continued)

	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
Total	570	26.11	2.51	2.06	69.32	333	25.57	2.68	4.31	67.45
Sex										
Male*	299	28.97	3.74	0.67	66.62	184	25.54	3.16	4.58	66.72
Female	271	22.95	1.15	3.61 +	72.30	150	25.60	2.09	3.97	68.34
Race/Hispanic origin[c]										
White*	231	24.49	1.26	0.47	73.78	139	24.47	2.10	2.67	70.76
Black	119	24.73	1.90	6.85 +	66.51	54	31.72	0.00 +	9.91	58.37
Asian	15	11.14 +	0.00	0.00	88.86 ++	9	10.19 +	0.00 +	0.00 ++	89.81 ++
Hispanic	189	30.78	4.84	1.34	63.04 +	124	25.67	4.87	4.26	65.20
Other	2	0.00 ++	0.00	0.00	100.00 ++	2	36.99	0.00 +	0.00 ++	63.01
Two or more races	14	21.73	0.00	0.00	78.27	5	9.45	0.00 +	0.00 ++	90.55 +
Age										
18–24	66	35.58	3.21	0.52	60.69	37	36.21	0.00	5.68	58.11
25–34	150	21.94 ++	3.27	0.15	74.64 +	97	27.60	4.40 +	2.03	65.97
35–49*	194	32.81	1.77	1.27	64.16	102	24.09	0.37	3.18	72.37
50–64	114	17.03 ++	3.37	3.21	76.39 +	73	25.56	5.92	5.21	63.31
65 or older	45	20.07	0.00	11.25	68.69	25	7.63 ++	0.00	13.11	79.26
Household income										
$24,999 or less	168	27.51	1.57	5.11	65.81 +	96	28.81	0.41	4.59	66.19
$25,000–$49,999	162	23.99	2.46	0.84	72.72	92	20.42	4.17	4.61	70.80
$50,000–$74,999	102	34.98 ++	4.75	0.41	59.86 ++	67	26.44	2.88	4.67	66.02
$75,000 or more*	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.

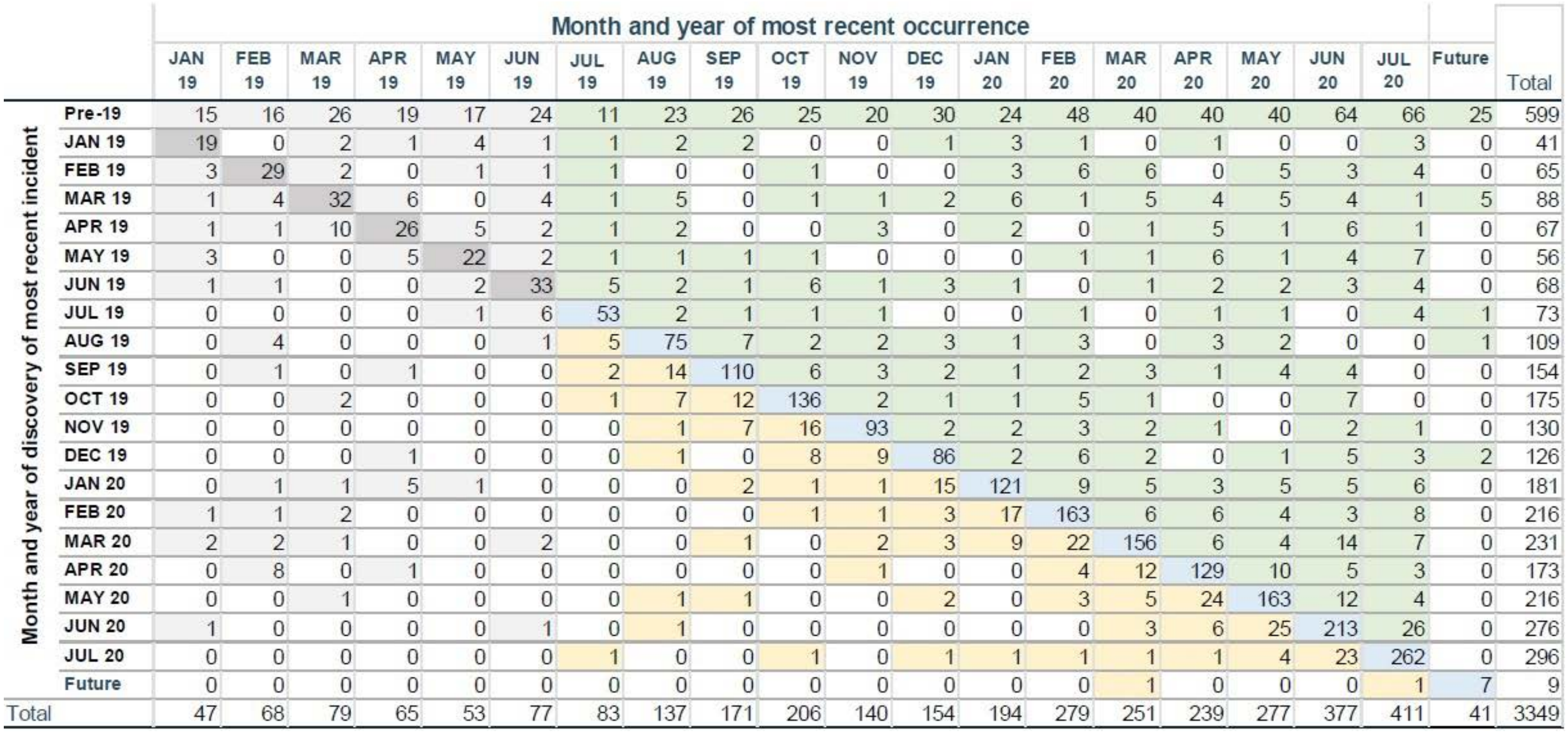
[a] Includes victims who provided a date of June 2019 or earlier.

[b] Includes victims who provided a date before the interview (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 4-1: Relationship Between the Date of Most Recent Occurrence and the Date of Discovery of Identity Theft (Version 2)



	Month and year of most recent occurrence																				
Month and year of discovery of most recent incident	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	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 4-14: 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 B.
* 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 4-15: Relationship Between the Date of Most Recent Occurrence and the Date of Discovery, by Victim Characteristics

		Percentage of Victims		Missing/Don't Know/ Out of Reference Period
	Total Number	Same Month/Year	Different Month/Year	
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	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 B.
* 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 4-16: 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; for Version 2, about 1.5%; and for 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 4-17: Relationship Between the Time of Most Recent Occurrence and How Long the Identity Theft Had Been Happening When It Was Discovered

How Long ID Theft Had Been Happening When Discovered	Length of Time from Interview to Most Recent Occurrence—Version 2							
	Month			Out of Reference Period, %	Dating Error, %[a]	Total, %	Version 1, %*	Version 3, %
	Same, %	1 to 6, %	7 to 12, %					
1 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 1 month (7–30 days)	10.66	14.45 ++	13.33 +	14.19	9.81	13.61 ++	10.83	13.46 ++
1 month to less than 3 months	7.44	9.83 ++	9.67 ++	12.39 ++	21.23 +	9.95 ++	6.49	9.66 ++
3 months to less than 6 months	6.10 +	3.85	3.86	5.45 +	24.02 ++	4.58 ++	2.89	3.37
6 months to less than 1 year	3.25	2.37	3.10	2.74	15.41	2.89	2.26	1.74
1 year or more	1.52	2.30	1.65	4.65 ++	0.70 ++	2.29	1.78	1.63
Not applicable, not actually misused	~	~	~	~	~	~	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 B. 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.

~Not applicable.

[a] Includes victims who provided a date in the future, after the interview occurred (August/September 2020 or later).

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

4.10 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 4-18).
- 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 4-19).
- This was also true across most demographics for AmeriSpeak respondents who participated via telephone interview. Among Hispanics, persons of other races, and persons 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 4-18: Prevalence of Identity Theft in the Past 12 Months, by Type of Identity Theft, Survey Administrator, and Mode

			AmeriSpeak					
	2018 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 +

Note: Standard errors are provided in Appendix B.
* 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 U.S. residents age 16 or older.
[b] Based on a representative sample of U.S. residents age 18 or older.
Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018; 2020 RTI/AmeriSpeak Identity Theft Survey.

Table 4-19: Persons Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics, Survey Administrator, and Mode

					AmeriSpeak					
	2018 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 B. 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 U.S. 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, National Crime Victimization Survey, Identity Theft Supplement, 2018; 2020 RTI/AmeriSpeak Identity Theft Survey.

5 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) 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 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 outside of the 12-month reference period, there is evidence that some telescoping still occurred despite the dual reference period. Table 5-1 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 solely based on the question of whether the incident occurred during the past 12 months (referred to as Version 2—NEW in Table 5-1). With the removal of these cases, which BJS could do during data analysis, the new Version 2 estimates are significantly lower than both Versions 1 and 3.

Although Version 2 is recommended, several downsides to moving to Version 2 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 5-2 shows the mean and median times that respondents spent completing each of the survey versions.

Table 5-1: 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	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[b]								
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 B.

~ 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 U.S. 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 5-2: **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.

Although Version 3 also appeared to result in lower prevalence rates than Version 1, possibly because of 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.

6 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 evaluated the effectiveness of three different screener options for a larger survey about identity theft that RTI conducted for BJS. This study was offered in English only and conducted online and over the phone.

6.1 Sampling

6.1.1 AmeriSpeak/Lucid

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. Approximately 34% of respondents were from Amerispeak, 35% from Lucid, and 31% from MTurk (see Table 4-2).

6.1.2 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 a Human Intelligence Task (HIT). When the HIT is published on the platform, interested MTurk workers can accept 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 high-quality participants who tend to put in the effort to produce good-quality 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, we leveraged RTI's past experiences with MTurk 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.

6.2 Fielding

6.2.1 AmeriSpeak/Lucid

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. NORC reviewed the initial data from the pretest and delivered it 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 and 1,276 by phone—during the field period, July 16 to August 4, 2020.

Response Rate Reporting for AmeriSpeak Sample

- Weighted AAPOR Response Rate 3 (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%

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.

6.2.2 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 according to 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 6-1).

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 2,000. When the pace of completion slowed 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 completing tasks could complete the survey. The lowest eligibility threshold for the final HIT before achieving the recruitment goal was a 98% approval rate or better for all work completed on MTurk with a minimum of 50 approved HITs.

Table 6-1: Detailed Breakdown of the Survey Recruitment HITs

	Number of		Approval Rate
	Submissions	Approvals	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

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. The final sample was 10,062 workers after validating the survey completion and engaging in data cleaning.

6.2.3 Tables Presenting Sample Sizes by Mode and Platform

Earlier in the report, tables 4-1 and 4-2 presented the unweighted sample characteristics by mode of completion and sample platform. Tables 6-2 and 6-3 show the unweighted prevalence rates of the different types of identity theft, mode, and platform. Tables 6-4 and 6-5 show the unweighted prevalence rate of identity theft overall, by demographic characteristics of victims, and by mode and platform.

Table 6-2: 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 B.

[a] Based on a representative sample of the population of U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table 6-3: 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 U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table 6-4: 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[b]						
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 U.S. 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 6-5: 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[b]								
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 U.S. 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.

6.3 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 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 the number of households obtained from the CPS. Next, 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: Homeowner 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 for 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 five topline sociodemographic characteristics—age, sex, education, race/Hispanic ethnicity, and Census Division—and three 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 are done during the weighting process such that the weighted demographic distribution of the survey completes resemble the demographic distribution in the target population (see Table 6-6). 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 6-6: Census CPS (Feb 2020) Used for Benchmarking

	Percent
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+	21.41
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 Diploma	9.77
High School Diploma	28.25
Some College	27.73
College Degree	34.26
Race/Ethnicity	
Non-Hispanic White	62.79
Non-Hispanic Black	11.93
Hispanic	16.66
Non-Hispanic Other	8.62

6.4 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 describe the statistical corrections made to the nonprobability sample via NORC’s TrueNorth calibration weighting service.

6.4.1 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.

6.4.2 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 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. 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 data from the U.S. Census Bureau's American Community Survey (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.

6.4.3 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 4-3.

6.5 Assessment of Item Nonresponse, Speeders, and Skippers

Tables 6-7 through 6-12 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. While the last question appeared to have higher levels of missingness compare to other questions regardless of version or mode, overall, for most items across all three versions, levels of item missingness were low.

Table 6-13 shows the average number of missing or “don’t know” responses, by respondent demographics and instrument version.

Table 6-7: Instrument Version 1 Item Nonresponse, by Key Items and Survey Platform

	Total			AmeriSpeak			Lucid			MTurk			Total (Excluding Speeders and Skippers)*		
	Number			Number			Number			Number			Number		
	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	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 6-8: Instrument Version 2 Item Nonresponse, by Key Items and Survey Platform

	Total			AmeriSpeak			Lucid			MTurk			Total (Excluding Speeders and Skippers)*		
	Number			Number			Number			Number			Number		
	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent
Q1	26	11,037	0.24	12	3,813	0.31	6	3,775	0.16	8	3,449	0.23	16	10,926	0.15
Q2	29	10,670	0.27	9	3,728	0.24	14	3,552	0.39	6	3,390	0.18	27	10,576	0.26
Q3	12	4,312	0.28	4	1,350	0.30	4	1,327	0.30	4	1,635	0.24	10	4,265	0.23
Q4a	14	1,916	0.73	9	394	2.28	5	701	0.71	0	821	0.00	13	1,897	0.69
Q4b	19	1,916	0.99	6	394	1.52	9	701	1.28	4	821	0.49	18	1,897	0.95
Q5	30	11,037	0.27	12	3,813	0.31	9	3,775	0.24	9	3,449	0.26	18	10,926	0.16
Q6	36	9,528	0.38	8	3,447	0.23	19	3,054	0.62	9	3,449	0.26	35	9,455	0.37
Q7	18	4,279	0.42	7	1,564	0.45	4	1,196	0.33	7	1,519	0.46	16	4,243	0.38
Q8a	17	1,680	1.01	14	444	3.15	3	517	0.58	0	716	0.00	15	1,664	0.90
Q8b	19	1,680	1.13	8	444	1.80	7	517	1.35	4	716	0.56	18	1,664	1.08
Q9	38	11,037	0.34	24	3,813	0.63	13	3,775	0.34	1	3,449	0.03	25	10,926	0.23
Q10	33	3,368	0.98	9	1,028	0.88	9	1,042	0.86	15	1,298	1.16	32	3,346	0.96
Q10a	18	1,626	1.11	12	425	2.82	3	529	0.57	3	672	0.45	16	1,613	0.99
Q10b	19	1,626	1.17	7	425	1.65	7	529	1.32	5	672	0.74	18	1,613	1.12
Q11	51	11,037	0.46	24	3,813	0.63	11	3,775	0.29	16	3,449	0.46	34	10,926	0.31
Q12	18	2,432	0.74	5	640	0.78	8	730	1.10	5	1,062	0.47	17	2,402	0.71
Q14a	13	1,286	1.01	6	249	2.41	4	396	1.01	3	641	0.47	13	1,277	1.02
Q14b	19	1,286	1.48	7	249	2.81	5	396	1.26	7	641	1.09	19	1,277	1.49
Q15	58	11,037	0.53	26	3,813	0.68	12	3,775	0.32	20	3,449	0.58	43	10,926	0.39
Q16	12	1,778	0.67	2	411	0.49	1	579	0.17	9	788	1.14	12	1,759	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	11,037	0.62	30	3,813	0.79	20	3,775	0.53	18	3,449	0.52	49	10,926	0.45
Q20	6	1,527	0.39	0	320	0.00	2	492	0.41	4	715	0.56	6	1,509	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	3,805	1.52	31	1,112	2.79	20	1,227	1.63	7	1,466	0.48	55	3,776	1.46
Q25b	61	3,805	1.60	31	1,112	2.79	22	1,227	1.79	8	1,466	0.55	58	3,776	1.54
Q26	244	3,805	6.41	94	1,112	8.45	91	2,548	3.57	59	1,466	4.02	237	3,776	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 6-9: Instrument Version 3 Item Nonresponse, by Key Items and Survey Platform

	Total			AmeriSpeak			Lucid			MTurk			Total (Excluding Speeders and Skippers)*		
	Number			Number			Number			Number			Number		
	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent
Q1	34	10,758	0.32	12	3,706	0.32	13	3,737	0.35	9	3,315	0.27	27	10,642	0.25
Q1a	39	10,174	0.38	10	3,531	0.28	16	3,425	0.47	13	3,218	0.40	37	10,080	0.37
Q2	197	10,758	1.83	39	3,706	1.05	121	3,737	3.24	37	3,315	1.12	180	10,642	1.69
Q2a	28	8,837	0.32	5	3,218	0.16	9	2,741	0.33	14	2,878	0.49	27	8,758	0.31
Q3	76	10,758	0.71	29	3,706	0.78	26	3,737	0.70	21	3,315	0.63	61	10,642	0.57
Q4	40	10,758	0.37	19	3,706	0.51	14	3,737	0.37	7	3,315	0.21	25	10,642	0.23
Q5	61	10,758	0.57	23	3,706	0.62	21	3,737	0.56	17	3,315	0.51	45	10,642	0.42
Q9a	155	4,128	3.75	88	1,120	7.86	47	1,415	3.32	20	1,593	1.26	147	4,111	3.58
Q9b	145	4,128	3.51	71	1,120	6.34	54	1,415	3.82	20	1,593	1.26	138	4,111	3.36
Q10	303	4,128	7.34	90	1,120	8.04	138	1,415	9.75	75	1,593	4.71	297	4,111	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 6-10: Instrument Version 1 Item Nonresponse, by Key Items and Mode

	Total			Web			Phone			Total (Excluding Speeders and Skippers)*		
	Number			Number			Number			Number		
	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent
Q1	38	10,738	0.35	36	10,302	0.35	2	436	0.46	31	10,609	0.29
Q1a	85	10,095	0.84	81	9,726	0.83	4	369	1.08	84	9,989	0.84
Q2	236	10,738	2.20	235	10,302	2.28	1	436	0.23	224	10,609	2.11
Q2a	15	8,775	0.17	15	1,854	0.81	0	109	0.00	14	1,933	0.72
Q3	51	10,738	0.47	47	8,448	0.56	1	334	0.30	45	8,688	0.52
Q4	49	10,738	0.46	47	10,302	0.46	4	436	0.92	38	10,609	0.36
Q5	59	10,738	0.55	45	10,302	0.44	4	436	0.92	35	10,609	0.33
Q7	59	10,738	0.55	53	10,302	0.51	6	436	1.38	44	10,609	0.41
Q9a	109	4,667	2.34	85	4,560	1.86	24	107	22.43	103	4,635	2.22
Q9b	84	4,667	1.80	80	4,560	1.75	4	107	3.74	79	4,635	1.70
Q10	313	4,667	6.71	302	4,560	6.62	11	107	10.28	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 6-11: Instrument Version 2 Item Nonresponse, by Key Items and Mode

	Total			Web			Phone			Total (Excluding Speeders and Skippers)*		
	Number			Number			Number			Number		
	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent
Q1	26	11,037	0.24	26	10,621	0.24	0	416	0.00	16	10,926	0.15
Q2	29	10,670	0.27	28	10,286	0.27	1	384	0.26	27	10,576	0.26
Q3	12	4,312	0.28	11	4,204	0.26	1	108	0.93	10	4,265	0.23
Q4a	14	1,916	0.73	10	1,881	0.53	4	35	11.43	13	1,897	0.69
Q4b	19	1,916	0.99	19	1,881	1.01	0	35	0.00	18	1,897	0.95
Q5	30	11,037	0.27	30	10,621	0.28	0	416	0.00	18	10,926	0.16
Q6	36	9,528	0.38	36	9,183	0.39	0	345	0.00	35	9,455	0.37
Q7	18	4,279	0.42	16	4,170	0.38	2	109	1.83	16	4,243	0.38
Q8a	17	1,680	1.01	13	1,643	0.79	4	37	10.81	15	1,664	0.90
Q8b	19	1,680	1.13	18	1,643	1.10	1	37	2.70	18	1,664	1.08
Q9	38	11,037	0.34	29	10,621	0.27	9	416	2.16	25	10,926	0.23
Q10	33	3,368	0.98	31	3,322	0.93	2	46	4.35	32	3,346	0.96
Q10a	18	1,626	1.11	12	1,600	0.75	6	26	23.08	16	1,613	0.99
Q10b	19	1,626	1.17	18	1,600	1.13	1	26	3.85	18	1,613	1.12
Q11	51	11,037	0.46	48	10,621	0.45	3	416	0.72	34	10,926	0.31
Q12	18	2,432	0.74	17	2,397	0.71	1	416	0.24	17	2,402	0.71
Q14a	13	1,286	1.01	11	1,276	0.86	2	10	20.00	13	1,277	1.02
Q14b	19	1,286	1.48	19	1,276	1.49	0	10	0.00	19	1,277	1.49
Q15	58	11,037	0.53	55	10,621	0.52	3	416	0.72	43	10,926	0.39
Q16	12	1,778	0.67	11	1,743	0.63	1	35	2.86	12	1,759	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	11,037	0.62	66	10,621	0.62	2	416	0.48	49	10,926	0.45
Q20	6	1,527	0.39	6	1,503	0.40	0	24	0.00	6	1,509	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	3,805	1.52	56	3,736	1.50	2	69	2.90	55	3,776	1.46
Q25b	61	3,805	1.60	61	3,736	1.63	0	69	0.00	58	3,776	1.54
Q26	244	3,805	6.41	240	3,736	6.42	4	69	5.80	237	3,776	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 6-12: Instrument Version 3 Item Nonresponse, by Key Items and Mode

	Total			Web			Phone			Total (Excluding Speeders and Skippers)*		
	Number			Number			Number			Number		
	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent	Missing	Eligible	Percent
Q1	34	10,758	0.32	33	10,320	0.32	1	438	0.23	27	10,642	0.25
Q1a	39	10,174	0.38	38	9,799	0.39	1	375	0.27	37	10,080	0.37
Q2	197	10,758	1.83	196	10,320	1.90	1	438	0.23	180	10,642	1.69
Q2a	28	8,837	0.32	28	8,492	0.33	0	345	0.00	27	8,758	0.31
Q3	76	10,758	0.71	74	10,320	0.72	2	438	0.46	61	10,642	0.57
Q4	40	10,758	0.37	39	10,320	0.38	1	438	0.23	25	10,642	0.23
Q5	61	10,758	0.57	61	10,320	0.59	0	438	0.00	45	10,642	0.42
Q9a	155	4,128	3.75	140	4,049	3.46	15	79	18.99	147	4,111	3.58
Q9b	145	4,128	3.51	141	4,049	3.48	4	79	5.06	138	4,111	3.36
Q10	303	4,128	7.34	296	4,049	7.31	7	79	8.86	297	4,111	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 6-13: 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.

6.6 Feedback from MTurk Workers

One of the features of MTurk was workers' ability to communicate with survey requesters. A few workers took 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, most thought our pay was fair or generous. One reviewer liked that no one gets screened out as long as they qualify for the survey. Another reviewer mentioned that the demographics page was annoying but thought it was a simple HIT and asked us to keep up the good work.

7 References

American Association for Public Opinion Research. (2015). *Standard definitions: Final dispositions of case codes and outcome rates for surveys*. https://aapor.org/wp-content/uploads/2023/05/Standards-Definitions-10th-edition.pdf

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

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 73rd Annual Conference of the American Association for Public Opinion Research, Denver, CO. May 16–19, 2018.

Identity Theft Task Force. (2008). *The President's Identity Theft Task Force Report*. https://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf

Johnson, E. O., & 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.

Langton, L. & Planty, M. (2010). *Victims of Identity Theft, 2008*. Bureau of Justice Statistics.

Loftus, E. F., Klinger, M. R., Smith, K. D., & 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., & Belli, R. F. (1998). Forward telescoping: The question matters. *Memory, 6*(4), 455-465.

Stambaugh, L., Hsieh, Y. P., Sanders, H., & Morgan, J. (2018). Building an On-Line Sample of United States Military Veterans. Paper presented at the 73rd Annual Conference of the American Association for Public Opinion Research, Denver, Co. Hsieh, Y. P., Murphy, J., Kim, A., Guillory, J., & Bradfield, B. (2017, May). Developing and evaluating a gradation assessment index for survey data quality assurance practices. American Association for Public Opinion Research, New Orleans, LA.

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

This page intentionally left blank.

Appendix A: Assessment of State Identity Theft Laws

Introduction

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

- 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—the thresholds for felony versus misdemeanor acts of identity theft
- The statute of limitations for charging identity theft offenders

This appendix 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, "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 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 the District of Columbia. 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, as victims are unlikely to know that their information is being shopped around until 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 the District of Columbia 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 Arkansas credit card fraud statute uses language similar to 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 canceled;
>
> (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, not just 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 a 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 of 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 of different types of PII and identity theft activities. Manual text review captured other details, such as the length of the statute of limitations. Note 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 A-1 presents the states that use 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).

Table A-1: List of States with a Broad Legal Definition of PII and Those with an Explicit Definition, 2020

PII Definition		PII Definition		PII Definition	
Broader	**Explicit**	**Broader**	**Explicit**	**Broader**	**Explicit**
AL	AK	KS	NE	NY	
AZ	AR	MD	OH	OK	
CO	CA	ME	OR	RI	
CT	DE	MO	PA	SD	
DC	GA	MT	SC	TN	
FL	KY	NC	VT	TX	
HI	LA	ND	WV	UT	
IA	MA	NH		VA	
ID	MI	NJ		WA	
IL	MN	NM		WI	
IN	MS	NV		WY	

Most states (65%) define PII more broadly, presenting examples of the types of information that are classified as PII along with 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:

> “D.C. 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)

In terms of the specific types of PII that are covered by the state statutes, more than 90% of states specifically identify a victim’s name as PII. More than 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 email 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 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 misuse 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 obtain false documents, open accounts, get or maintain employment, conceal the commission of a crime, or 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 identify these activities as forms of identity theft.

The vast majority of states' identity theft statutes (about 75%) 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. More than 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).[18] 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.[19] 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.[20] About a quarter of states use a grading system for offenses. These states specifically assign

[18] 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.

[19] 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).

[20] For example, Pennsylvania classifies an act of identity theft involving property with a value of $2,000 or less as a misdemeanor of the first degree but classifies an offense involving property worth $2,000 or more as a felony of

certain acts of identity theft involving a specific dollar amount or that involve other specific factors as a first-degree, second-degree, or third-degree offense, or as a "Class [B, C, D, E] felony or misdemeanor."

Among the states that have both misdemeanor and felony offenses, 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 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 the 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 affect the classification of offense severity. Rather, 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. 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 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 statute of limitations time period from the date the identity theft was committed. The other 30% of states establish the beginning of the statute of limitations as the date the 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" (N.D. 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 identity theft "has been completed or terminated" (D.C. 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 time frame 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 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.

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 DC 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, we created targeted Boolean search strings and applied them within the subscription-based LexisNexis legal database to identify any additional, relevant state identity theft laws.

We created the Boolean search strings and intentionally included or excluded laws based on two 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; or laws that criminalize fraudulent access or use of access device.

Some states have enacted additional laws that specifically criminalize certain aspects of identity fraud. To maintain internal consistency within each of the categories for 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., N.H. 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 whether 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 string 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 whether 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.

Appendix B: Standard Error Tables

Table B-1: Standard Errors for Table 2-10: Harms Associated with Attempted ID Theft Incidents Compared to Successfully Completed Incidents, 2014 and 2016

	Attempts - Based on Q10		Completed Incidents		Attempts 2		Completed Incidents		Attempts		Completed Incidents	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Type of ID theft	57,718	~	675,601	~	144,763	~	672,845	~	294,195	~	582,843	~
Existing credit card account	27,481	2.92	339,674	0.57	87,525	1.63	332,370	0.54	155,706	0.88	303,102	0.61
Existing bank account	30,905	3.28	375,095	0.57	85,757	1.72	366,506	0.57	197,301	0.99	284,862	0.57
Other existing account	20,786	2.50	91,983	0.22	46,288	1.04	94,563	0.23	29,436	0.57	61,027	0.19
New account	15,573	1.99	68,941	0.17	29,436	0.70	70,798	0.17	18,076	0.22	70,798	0.22
Personal information	12,302	1.59	56,116	0.15	18,076	0.45	69,134	0.18	27,637	0.14	69,134	0.23
Multiple types	10,750	1.41	128,003	0.29	27,637	0.67	132,989	0.30	27,637	0.21	132,989	0.38
Indirect financial loss >$0	9,315	1.27	98,599	0.24	17,336	0.42	102,420	0.24	36,348	0.27	96,387	0.29
Reported to police	10,513	1.42	107,608	0.26	10,513	0.26	115,996	2.75	57,331	0.41	100,738	0.31
Problems with school/work	0	0.00	40,696	0.10	8,969	0.23	39,705	0.10	22,763	0.17	34,095	0.11
Problems with family/friends	4,571	0.61	65,569	0.16	14,424	0.35	67,081	0.16	47,781	0.35	52,015	0.17
Moderate to severe distress	26,952	3.38	283,949	0.49	52,871	1.21	288,474	0.49	128,032	0.75	256,915	0.57

~Not applicable.

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

Table B-2: Standard Errors for Table 2-13: Identity Theft Supplement Prevalence Rates, by Type of Identity Theft and Person TIS Number, 2018

	ITS Rate (standard errors)						
TIS	Overall	Existing Credit	Existing Bank	Other Existing	New Account	Other Fraudulent Purpose	Multiple Types
Person TIS	0.266	0.079	0.079	0.030	0.023	0.020	0.027
1	0.266	0.149	0.176	0.064	0.042	0.046	0.067
2	0.259	0.142	0.146	0.069	0.052	0.040	0.069
3	0.280	0.185	0.166	0.064	0.064	0.041	0.067
4	0.295	0.188	0.153	0.070	0.047	0.054	0.086
5	0.264	0.204	0.146	0.060	0.063	0.036	0.065
6	0.418	0.313	0.312	0.144	0.101	0.100	0.119
7	0.566	0.484	0.254	0.145	0.122	0.038	0.144

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

Table B-3: Standard Errors for Table 4-1. 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	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

~Not applicable.

* 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 B-4: Standard Errors for Table 4-2. 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	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

~Not applicable.

*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 B-5: Standard Errors for Table 4-3. Weighted Sample, by Demographic Characteristics

	Version 1		Version 2		Version 3	
	Number	**Percent**	**Number**	**Percent**	**Number**	**Percent**
Total	111.71	0.00	112.90	0.00	115.70	0.00
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.

Table B-6: Standard Errors for Table 4-4: Prevalence of Identity Theft in 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	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

~Not applicable.

[a] Based on a representative sample of U.S. residents age 18 or older.

Source: 2020 RTI/Amerispeak Identity Theft Survey.

Table B-7: Standard Errors for Table 4-5: 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.

[a] Based on a representative sample of U.S. 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 B-8: Standard Errors for Table 4-6. 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	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

~Not applicable.

[a]Based on a representative sample of U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-9: Standard Errors for Table 4-7. 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[a]
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

~Not applicable.

[a]Based on a representative sample of U.S. residents age 18 or older.

Table B-10: Standard Errors for Table 4-8. 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.

[a] Based on a representative sample of U.S. 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 B-11: Standard Errors for Table 4-9. 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 U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-12: Standard Errors for Table 4-10. 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 Respondents[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

[a] Based on a representative sample of U.S. 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 B-13: Standard Errors for Table 4-11: 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	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

~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 U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-14: Standard Errors for Table 4-12. 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

[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 B-15: Standard Errors for Table 4-14. Relationship between 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	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	24.01	2.85	2.68	1.99
New account	15.68	4.53	4.71	4.49
Personal information	9.34	5.30	5.46	3.74
Multiple types	24.05	3.19	2.99	2.82

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-16: Standard Errors for Table 4-15. Relationship Between Date of Most Recent Occurrence and 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	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

[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 B-17: Standard Errors for Table 4-16. Time from Discovery of 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	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%.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-18: Standard Errors for Table 4-17. Relationship Between Time of Most Recent Occurrence and How Long Identity Theft Had Been Happened 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)	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 months	1.52	0.86	1.12	2.31	8.03	0.62	0.51	0.67
Three months to less than six months	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 misused	~	~	~	~	~	~	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%.

~Not applicable.

[a] Includes victims who provided a date prior to when the interview occurred (August/September 2020 or later).

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-19: Standard Errors for Table 4-18. Prevalence of Identity Theft in the Past 12 Months, by Type of Identity Theft and Survey Administrator and Mode

			AmeriSpeak					
	2018 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[a]
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

~Not applicable.

[a] Based on the population of U.S. residents age 16 or older.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018; 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-20: Standard Errors for Table 4-19. Persons Who Experienced One or More Incidents of Identity Theft During the Past 12 Months, by Victim Characteristics, Survey Administrator, and Mode

			AmeriSpeak					
	2018 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.

~Not applicable.

[a] Based on a representative sample of U.S. 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, National Crime Victimization Survey, Identity Theft Supplement, 2018; 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-21: Standard Errors for Table 5-1. Prevalence of Identity Theft in the 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

	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	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.

[a] Based on a representative sample of U.S. 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.

Table B-22: Standard Errors for Table 6-2. 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 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 U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-23: Standard Errors for Table 6-3. 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 U.S. residents age 18 or older.

Source: 2020 RTI/AmeriSpeak Identity Theft Survey.

Table B-24: Standard Errors for Table 6-4. 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[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
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	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 U.S. 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 B-25: Standard Errors for Table 6-5. 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[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
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	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 U.S. 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 C: Original and Revised Versions of ITS for Testing

Identity Theft Supplement Questionnaire - v1 (current survey)

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 are 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

Identity Theft Supplement Questionnaire – v2

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. 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 account, regardless of whether you were reimbursed later.
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 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.
YES
NO (skip to Q9)

6. 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.
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. Has anyone EVER, without your permission used another of your accounts, such as your telephone, internet or electric 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)

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 Q13)

11. 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)

12a. Please think about the most recent time someone misused [this/one of these] existing accounts. In what year did this most recently occur? ______________________________

12b. In what month [was this existing account/were these existing accounts] most recently misused? __________________________

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

13. *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, online payment accounts, entertainment accounts, such as for music or games, email or social media accounts, utilities accounts or some other type of account?

YES
NO (skip to Q17)

14. 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 Q17)

15. Which of the following types of NEW accounts did someone successfully open during the past 12 months? Did someone open…

15a. New telephone or internet accounts? YES NO
15b. New credit card accounts? YES NO
15c. New checking or savings accounts? YES NO
15d. New loans or mortgages? YES NO
15e. New insurance policies? YES NO

15f. New online payment accounts, such as Paypal? YES NO
15g. New entertainment accounts, such as for movies, music, or games? YES NO
15h. New email or social media accounts? YES NO
15i. New utilities accounts, such as cable, gas, or electric? YES NO
15j. Some other type of new account? YES NO
[If yes] What other type of new account was opened? __________

(If any 15a-15j = yes, ask Q16a; else skip to Q17)

16a. Please think about the most recent time an offender successfully opened [this/one of these] new accounts. In what year was this?______________________________

16b. And in what month? *If there was an account open in your name for multiple months or years, think about the when the account was most recently open.* ___________________________

17. *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)

18. 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)

19. In which of the following ways has someone used your personal information during the prior 12 months? Was your personal information used….
19a. To file a fraudulent tax return? YES NO
19b. To get medical treatment? YES NO
19c. To apply for a job? YES NO
19d. To provide false information to the police? YES NO
19e. To apply for government benefits? YES NO
19f. In some other way we haven't already mentioned? YES NO
[If yes] How else was your personal information misused? __________

(If any 19a-19f = yes, ask Q20a; else skip to Check Item A)

20a. 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? __________________________

20b. 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, Q13, and Q17
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, Q14, AND Q18
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, Q14, AND Q18
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, Q12a/b, Q16a/b, and Q20a/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 Q21

21. You said that in <autofill most recent month/year provided in Q4a/b, Q8a/b, Q12a/b, Q16a/b AND Q20a/b> someone <autofill applicable "yes" responses from Q3, Q7, Q10, Q14, AND Q18>. Were these the result of one related incident, or was your personal information misused multiple times in separate unrelated incidents?
    1. Multiple Incidents (ask Q22)
    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.

22. Which of these happened most recently?

(Mark all that apply, and only read response items that match autofill from Q3, Q7, Q10, Q14, and Q18)

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, Q14, Q18) OR Q22, if applicable] you experienced on [autofill most recent month/year from Q4a/b, Q8a/b, Q12a/b, Q16a/b, or Q20a/b].

25. 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)

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

Identity Theft Supplement Questionnaire - v3

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 account, regardless of whether you were reimbursed later.
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 charges were actually made on the account, regardless of whether you were reimbursed later.
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?
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? YES NO
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? __________
NEW_OTHER_SP

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