

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

Document Title: Assessing the Quality of the National Crime Victimization Survey (NCVS) Supplemental Fraud Survey (SFS)

Authors: Lynn Langton, PhD, RTI International  
Christopher Krebs, PhD, RTI International  
Michael Planty, PhD, RTI International  
Marcus Berzofsky, DrPH, RTI International

BJS Project Managers: Rachel E. Morgan, PhD, Statistician  
Grace Kena, Chief, Publication and Dissemination Unit  
Heather Brotsos, Deputy Director of Statistical Operations

Document No.: NCJ 306194

Publication Date: August 2023

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

**Abstract:**

This report describes efforts to compare estimates from the Bureau of Justice Statistics' (BJS) National Crime Victimization Survey (NCVS) Supplemental Fraud Survey (SFS) to estimates and victimization patterns from other available sources of fraud data. There are numerous sources of data on the prevalence and nature of personal financial fraud. Each source uses different definitions of fraud, employs different methodologies, and suffers from a variety of limitations. BJS developed the SFS to address the major limitations and shortcomings of other existing fraud data collections. It was the first effort by BJS to estimate the prevalence and characteristics of fraud in the United States. The survey was administered to all NCVS respondents age 18 or older from October to December 2017. This paper examines initial SFS estimates of the prevalence and nature of personal financial fraud and explores the similarities and differences between the SFS and other sources of fraud data as one component of an effort to validate the SFS estimates.

**Disclaimer**

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 the U.S. Department of Justice.

**Caveat**

This report was completed in 2019. Since then, there may have been updates to the data collections described in this report, specifically methodologies and fraud types measured. Please consult the sponsors and funders of these data collections for updated information.

This page intentionally left blank.

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

# **Assessing the Quality of the National Crime Victimization Survey (NCVS) Supplemental Fraud Survey (SFS)**

**August 2023**

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

**Prepared by**  
Lynn Langton, PhD  
Christopher Krebs, PhD  
Michael Planty, PhD  
Marcus Berzofsky, DrPH

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

---

RTI International is a trade name of Research Triangle Institute.  
RTI and the RTI logo are U.S. registered trademarks of Research Triangle Institute.



## Contents

Section	Page
Executive Summary.....	1
1 Introduction .....	2
1.1 Defining Fraud .....	4
1.1.1 Aligning with the FFRC/FINRA Foundation Fraud Taxonomy.....	4
1.1.2 Aligning with Criminal Statutes .....	5
1.1.3 Estimates of Fraud.....	6
1.1.4 Cognitive Testing .....	8
2 Comparison of SFS Estimates to Other Data Sources.....	9
2.1 Prevalence of Fraud.....	9
2.1.1 Impact of How Fraud is Defined and Operationalized on Prevalence Rates.....	9
2.1.2 Impact of the Type of Data Collection on Fraud Prevalence Rates.....	12
2.1.3 Differences in Fraud Prevalence Rates because of a Top-Down Versus Bottom-Up Collection Approach.....	12
2.1.4 Impact of Including Identity Theft as a Type of Fraud on Prevalence Rates.....	14
2.1.5 Impact of Mode Effects on Prevalence Rates.....	14
2.2 Most Common Types of Fraud .....	17
2.2.1 Impact of Differences in How Fraud Types are Defined.....	17
2.3 Reporting Behaviors .....	21
2.3.1 Comparing SFS Complaint Reports to Complaints from Consumer Agencies.....	23
2.3.2 Comparing SFS Data on Fraud Reported to Police to NIBRS Law Enforcement Data .....	24
2.3.3 Impact of Capturing Victims Who Do Not Identify as Victims.....	26
2.4 Financial Losses.....	28
2.4.1 Impact of Including Incidents with No Direct Financial Loss (Attempted Fraud) in Fraud Data .....	29
2.5 Characteristics of Fraud Victims .....	29
2.5.1 Potential Impact of Sample Bias on Victim Characteristics.....	32
2.5.2 Variations in Victim Characteristics Based on the Population of Interest .....	32
3 Recommendations .....	33
References (data sources).....	34
Appendices	
Appendix A. Additional Findings From the SFS Analysis .....	A-1
Appendix B. Summary of Existing Fraud Surveys/Data Collections Examined and Summarized .....	B-1

## Figures

---

Number		Page
Figure 1-1:	Criteria for Meeting Fraud Definition, by Type of Fraud .....	7
Figure 2-1:	Fraud Prevalence Rates by Mode of Administration Among the SFS and External Surveys .....	16

## Tables

Number	Page
Table 2-1:	Data Sources Examined for Comparison to Supplemental Fraud Survey Estimates ..... 10
Table 2-2:	Prevalence of Types of Fraud by Fraud Screening Criteria, 2017 ..... 11
Table 2-3:	Fraud Prevalence Rates and Types of SFS Fraud Measured by Each Collection, by Type of Collection ..... 11
Table 2-4:	Fraud Prevalence Rates, by Source and Characteristics ..... 13
Table 2-5:	Inclusion of Identity Theft in Fraud Data ..... 15
Table 2-6:	Count of Victims and Prevalence of Fraud, by Type of Fraud and Interview Mode, 2017..... 15
Table 2-7:	Fraud Prevalence Rates and Mode of Administration Among the Surveys..... 17
Table 2-8:	Number and Percentage of Fraud Victims by Type and Fraud Screening Criteria, 2017..... 18
Table 2-9:	Number and Percentage of Fraud Victims, by Type of Fraud and Select Collections..... 19
Table 2-10:	Victim Reporting to Law Enforcement and Consumer Organizations, by Type of Fraud, 2017 ..... 21
Table 2-11:	Victim Reporting to Law Enforcement and Consumer Organizations, by Type of Fraud and Organization, 2017..... 22
Table 2-12:	Number of Fraud Victims Who Submitted Consumer Complaints Based on SFS Data and Actual Consumer Complaint Data, 2017 ..... 23
Table 2-13:	Demographic Characteristics of NIBRS and SFS Victims ..... 25
Table 2-14:	Percentage of Victims Who Believed What They Experienced was Fraud, 2017 ..... 27
Table 2-15:	Average Out of Pocket Financial Losses Experienced by Victims of Fraud, by Type of Fraud, 2017 ..... 28
Table 2-16:	Percentage of Fraud Victims Experiencing Out of Pocket Financial Losses, by Type of Fraud, 2017 ..... 28
Table 2-17:	Demographic Characteristics of Fraud Victims, by Fraud Definition, 2017 ..... 31

This page intentionally left blank.

# Executive Summary

Fraud is the intentional use of deception for monetary gain. An expanding problem, it is considered a critical area of attention, particularly given the emergence of technology that enables these incidents on a large scale. Furthermore, the problem is exacerbated by an aging population that is at a heightened risk for fraud because of the potential onset of cognitive impairment and social isolation. These concerns make the need for an accurate measure of the prevalence and nature of fraud paramount.

There are numerous data sources on the prevalence and nature of personal financial fraud. Each source uses different definitions of fraud, employs different methodologies, and suffers from a range of limitations. The Bureau of Justice Statistics (BJS) developed the Supplemental Fraud Survey (SFS) to address the major limitations and shortcomings of other existing fraud data collections. Following several years of developmental work by BJS in conjunction with RTI International, the FINRA Foundation, and the Stanford University Financial Fraud Research Center, BJS fielded the SFS as a supplement to its National Crime Victimization Survey (NCVS) from October to December 2017. At BJS's request, this report examines initial SFS estimates of the prevalence and nature of personal financial fraud and explores the similarities and differences between the SFS and other sources of fraud data to validate the SFS estimates.

Key findings include the following:

- In 2017, according to the SFS, the prevalence of personal financial fraud among persons age 18 or older was 1.2%, which translates to over 3 million victims.
- Among the 14 external data sources examined for this study, fraud prevalence rates ranged from a low of less than 0.1% to a high of 21.0%.
- The 14 external sources of fraud data varied widely from each other and the SFS in terms of the estimated magnitude and nature of fraud victimization.
- Like other crimes, estimates of the prevalence of personal financial fraud can be highly influenced by data collection.
  - How broadly or specifically financial fraud is defined has a large impact on findings related to the magnitude of the problem.
  - Including identity theft or attempted fraud in the total victim counts or prevalence rates impacts the comparability of the SFS data to the other source.
  - Although administrative data collections often cover a similar scope of fraud types as the SFS, the SFS data show that a relatively low proportion of victims report the incident to law enforcement or consumer organizations, making it difficult to compare the SFS with administrative collections.
- Because it is not possible to fully verify or triangulate the SFS findings with other data sources, additional research is necessary to identify whether methodological decisions in SFS administration suppressed reports of particular fraud types or reduced the likelihood that certain types of fraud victims would participate.
- Future research could use experimental designs to empirically and efficiently test the impact of a variety of design decisions related to SFS wording, structure, and administration on fraud prevalence estimates.

# Assessing the Quality of the NCVS Supplemental Fraud Survey

## 1 Introduction

This report describes efforts to compare estimates from the Bureau of Justice Statistics' (BJS) Supplemental Fraud Survey (SFS) with estimates and victimization patterns from other available sources of fraud data as an initial step toward validating SFS findings.<sup>1</sup> The SFS was BJS's first effort to estimate the prevalence and characteristics of financial fraud in the United States. BJS administered the survey to all National Crime Victimization Survey (NCVS) respondents age 18 or older from October to December 2017 following extensive development work, which is described in more detail in Section 2. Based on prior fraud studies, findings from cognitive testing of the SFS instrument, and rates of identity theft from the NCVS, BJS anticipated that about 12% of respondents would be identified as victims of fraud. However, the 2017 SFS fraud prevalence rate was substantially lower than expected, with 1.2% of persons 18 or older experiencing fraud in the prior year.

The discrepancy between the expected and actual prevalence rates could be attributed to several factors related to the external sources, the SFS, or both:

- Estimates from external fraud studies were based on more expansive definitions of fraud, included high rates of false positive reports, or had other sources of error that resulted in highly inflated prevalence estimates but were addressed in the SFS;
- The SFS screener questions were too narrow or specific and inadvertently screened out fraud victims who met the fraud definition but did not think that the questions addressed their experiences;<sup>2</sup>
- Aspects of the NCVS methodology (e.g., mode of administration, burden, crime context, failure by field staff to administer the question as worded) suppressed fraud reports among some victims; or
- Some combination of these.

To assess the potential reasons for the discrepancy and the reliability and validity of SFS findings, BJS initiated a proposal through the National Victimization Statistical Support Center II (award number 2017-MU-MU-K048) for RTI to identify and evaluate the factors accounting for differences in the SFS prevalence estimates and those of external data collection efforts.

---

<sup>1</sup> Two experts on financial fraud who worked with BJS on the development of the SFS—Dr. Gary Mottola from the FINRA Foundation and Dr. Marguerite DeLiema, who was at the Stanford University Financial Fraud Research Center at the time—were consultants on this project. The views and perspectives presented in this report are those of the authors and do not necessarily represent the beliefs or opinions of Dr. Mottola or Dr. DeLiema.

<sup>2</sup> Reports of fraud may also be deflated if individuals do not know, recognize, or acknowledge they have experienced victimization. The SFS took steps to mitigate this potential issue by not using the term “fraud,” not referring to individuals as victims, and allowing for affirmative responses to the screener questions even if the respondent did not have proof that the perpetrator intended to defraud them.

To set the stage for a larger validation effort, RTI conducted an initial analysis of SFS data and compiled all relevant sources of fraud data from 2010 through 2017. Knowing how the SFS estimates compare with other sources, including fraud reported to law enforcement agencies and consumer complaint data, provides a more informed understanding of the problem. This report presents the comparison between the SFS and other sources of fraud data and high-level efforts to examine potential data quality issues with the SFS that could influence the estimates, such as response rates and proxy measures of respondent fatigue.

The specific tasks undertaken include the following:

- Analyzing the SFS data for patterns in terms of who reported experiencing fraud victimization, by type of fraud, amount of loss, and other incident characteristics.
- Identifying major inconsistencies or consistencies between the SFS findings and other sources of fraud data.
- Documenting methodological and scope differences between the SFS and other collections of data on financial fraud that could potentially explain differences in findings, such as:
  - Definitional differences in fraud between law enforcement records from the Federal Bureau of Investigation's (FBI) National Incident-Based Reporting System (NIBRS) and SFS data.
  - The impact of including/excluding identity theft crimes on estimates.
- Determining how fraud cases are prosecuted, the elements that make up a prosecutable case, and how the inclusion or exclusion of these different elements impacts fraud estimates.

After a description of the development and methodology of the SFS, this report walks through key findings from the SFS on the following:

- The prevalence of fraud,
- The most common types of fraud,
- Financial losses caused by fraud,
- Victim reporting behaviors, and
- The characteristics of fraud victims.

Each section of findings also examines the comparability of SFS data to other external sources and discusses some of the potential reasons for discrepancies in the results on the level and nature of fraud by each data source.

## Background on the Project

Researchers and practitioners working in fraud prevention and consumer protection have been hindered by the major data gaps in our nation’s understanding of the prevalence and nature of personal financial fraud. Although there are many available data sources on fraud, each suggesting that fraud has a serious impact on society, these sources all suffer from major limitations. They capture a limited scope of fraud offenses, focus on a limited or specific population, depend on victim reporting of fraud experiences, or suffer from other data quality issues, such as low survey response rates.

The SFS, which BJS developed in collaboration with the Stanford Financial Fraud Research Center (FFRC), the FINRA Foundation, and practitioners from the field, was designed to address many of these data collection issues and to measure the prevalence, characteristics, and consequences of personal financial fraud and the victim’s response to fraud during the past 12 months. If the respondent met the definition of fraud based on responses to the screener questions, they were asked to answer incident-level questions about the incident, or most recent incident, experienced during the reference period. Respondents were routed to incident-level questions for each type of fraud that they screened into as a victim. Survey questions covered the following:

- The type(s) of fraud experienced,
- Financial losses associated with fraud,
- Victim reporting behaviors, and
- Negative consequences of fraud incidents.

### 1.1 Defining Fraud

#### 1.1.1 Aligning with the FFRC/FINRA Foundation Fraud Taxonomy

One of the biggest challenges to measuring financial fraud has been the lack of a clear definition of the term “fraud.” BJS set out to address this issue in multiple ways in developing the SFS. First, BJS worked with the FFRC and FINRA Foundation to develop a fraud taxonomy for systematically classifying fraudulent acts into a definitional framework.<sup>3</sup> The taxonomy, which was also largely adopted in the National Academies of Sciences’ (NAS) Modernizing Crime Statistics taxonomy,<sup>4</sup> was used to identify the types of scams asked about in the SFS and to develop the screening questions accordingly. The definition of fraud used for the fraud taxonomy, and subsequently the SFS, was acts in which someone “intentionally and knowingly deceives the victim by misrepresenting, concealing, or omitting facts about promised goods, services, or other benefits and consequences that are nonexistent, unnecessary, never intended to be provided, or deliberately distorted for the purpose of monetary gain.”<sup>3</sup> There are seven specific types of fraud measured by the SFS, which also align with key categories in the taxonomy:

- Prize or grant fraud—Expected benefit is winning a prize, grant, lottery, or other monetary windfall (e.g., prize promotion and sweepstakes scams, lottery scams, fake government grant offers, and foreign prince letter scams).
- Phantom debt collection fraud—Victim is told they owe a debt and must take action to avoid the consequences of failing to pay (e.g., government debt collection scams, medical debt scams).

---

<sup>3</sup> Stanford/FINRA Foundation fraud taxonomy: [Framework for a Taxonomy of Fraud—Stanford Center on Longevity](#)

<sup>4</sup> NAS Modernizing Crime Statistics report: [Modernizing Crime Statistics: Report 1: Defining and Classifying Crime](#)  
[|The National Academies Press](#)

- Charity fraud—Expected benefit is a contribution to a charitable cause or organization (e.g., bogus natural disaster relief, law enforcement charity scams, personal crowdfunding sites for bogus causes).
- Employment fraud—Expected benefit is acquiring a paid job (e.g., work-at-home scams, government job placement scams, nanny scams).
- Consumer investment fraud—Expected benefit is a large return on an investment (e.g., Ponzi schemes, penny stock fraud, oil & gas exploration scams, bond fraud).
- Consumer products or services fraud—Expected benefit is obtaining the agreed upon consumer products or services (e.g., tech support scams, auto repair scams, weight loss product scams, online marketplace scams).
- Relationship/trust fraud—Victim believes they are fostering or continuing a personal and sometimes intimate relationship (e.g., friends/relatives imposter scams and in-person/online romance scams).

### 1.1.2 Aligning with Criminal Statutes

In addition to defining fraud based on the types of scams that victims experience, it could also be defined based on whether the incident had the necessary elements to be criminally prosecuted. Although the elements required for fraud prosecution vary depending on jurisdiction and type of fraud, the Department of Justice (DOJ) *Criminal Resource Manual* provides several key elements necessary for federal prosecution<sup>5</sup>:

- Defendant voluntarily and intentionally devised or participated in a scheme to defraud another out of money and did so with the intent to defraud/injure (deceit alone is not sufficient for prosecution);
- Actual loss to victims is not required; however, proof that someone was victimized is good evidence of intent;
- Representations made with reckless indifference to truth or falsity; and
- Substantial pattern of conduct.<sup>6</sup>

At the state level, fraud statutes generally include elements similar to the federal definition but differ in terms of the criteria used to classify an offense as a felony or a misdemeanor. For instance, the key elements of a fraud offense in New York include an offender's demonstrated intent to defraud, that the offender obtained property from at least one identified victim, and that the defendant engaged in a scheme with an ongoing course of conduct.<sup>7</sup> The distinction between a felony and misdemeanor hinges on the number and type of victims and the amount of property obtained. Similarly, the key elements in Florida are that there was an ongoing course of conduct with the intent to defraud one or more persons and that the offender obtained property from at least one victim.<sup>8</sup> Whether the fraud is a first-, second-,

---

<sup>5</sup> DOJ Criminal Resource Manual: <https://www.justice.gov/jm/crm-500-999>

<sup>6</sup> Cannot be addressed through the SFS. Most victims would not know whether the same offender also defrauded other victims.

<sup>7</sup> New York fraud statute: <http://ypdcrime.com/penal.law/article190.htm#p190.65>

<sup>8</sup> Florida fraud statute: [http://www.leg.state.fl.us/Statutes/index.cfm?App\\_mode=Display\\_Statute&URL=0800-0899/0817/Sections/0817.034.html](http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0800-0899/0817/Sections/0817.034.html)

or third-degree felony or a misdemeanor depends on the value of the property that the offender obtained.

Because the definition of fraud depends heavily on the offender's intentions, the victim must have sufficient evidence of the offender's intent to defraud to build a criminal case. The SFS introduction uses language to convey the need for intentionality on the part of the offender and to set the expectations for the scope of the survey: "We are now going to ask you about experiences in which someone convinced you to pay, invest, or donate money, by tricking or lying to you, hiding information, or promising you something that you never received."

For some types of fraud—for instance, charity fraud—the introductory language paired with an affirmative response to the question, "Have you donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake?" is sufficient to demonstrate that the offender intended to defraud (i.e., they made up a fake charity or charitable cause). In the case of products and services fraud, however, unless the victim actively tried to get their money back and was unsuccessful, it would be difficult to prove that the offender had not accidentally failed to deliver the product or service. Thus, the criteria used for screening a victim for the incident report section of the survey instrument varies depending on the type of fraud. For some fraud types, the SFS screener enables a range of fraud estimates to be produced, based on an increasing likelihood that fraud occurred and could be criminally prosecuted. For product and services fraud, for example, a person is classified as a fraud victim if they provide an affirmative answer to the question, "Have you paid for any products or services that you NEVER received or that turned out to be a SCAM?" AND a negative response to the follow-up question, "Did you get all of your money back from the person or company WITHOUT filing a claim or taking legal action?"

### 1.1.3 Estimates of Fraud

Five fraud prevalence estimates can be produced with the SFS data based on different criteria used for defining types of fraud (Table 1-1). *Fraud 1* includes victims who responded affirmatively to one or more of the screening items. However, for some fraud types—prize and grant, employment, investment, and product and services fraud—a single affirmative response was not sufficient to classify the respondent as a fraud victim because the screening item alone did not demonstrate the offender's intent to defraud. In other words, *Fraud 1* includes both victims who screened into the incident report and those who did not. *Fraud 2* includes all victims who screened into the incident report. *Fraud 3* includes victims who met the criteria for being classified as a victim, but in the case of prize and grant, employment, investment, and product and services fraud, the victim had to additionally confirm that they tried to get their money back from the perpetrator. *Fraud 4* is more exclusive than *Fraud 3* in that victims of employment fraud and product and services fraud had to also believe that there was no chance of getting their money back. Finally, *Fraud 5* includes all victims who screened into the incident report (*Fraud 2*) and self-identified as a fraud victim when asked the question, "Thinking about the same incident [the most recent incident of that type], do you think you were a victim of fraud?" Though not specified in the criminal statute, the criteria that the victim believes the incident was fraud is important because the victim is unlikely to report the incident to police if they do not believe a crime occurred. *Fraud 2* is the recommended definition to produce prevalence estimates because it fits the legal definition of fraud (victims did not receive their money back) and provides sufficient sample sizes to produce reliable estimates.

**Figure 1-1: Criteria for Meeting Fraud Definition, by Type of Fraud**

Type of Fraud	SFS Definitional Categories and Corresponding Questions				
	Fraud 1	Fraud 2	Fraud 3	Fraud 4	Fraud 5
<b>Prize and grant</b>	<ul style="list-style-type: none"> <li>• Paid money</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Tried to get money back</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Victim believed incident was fraud</li> </ul>
<b>Phantom debt</b>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Victim believed incident was fraud</li> </ul>
<b>Charity</b>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Victim believed incident was fraud</li> </ul>
<b>Employment</b>	<ul style="list-style-type: none"> <li>• Paid money</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Tried to get money back</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Tried to get money back +</li> <li>• No chance of getting money back</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Victim believed incident was fraud</li> </ul>
<b>Investment</b>	<ul style="list-style-type: none"> <li>• Paid money</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Tried to get money back</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Victim believed incident was fraud</li> </ul>
<b>Product and services</b>	<ul style="list-style-type: none"> <li>• Paid money</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Tried to get money back</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Tried to get money back +</li> <li>• No chance of getting money back</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Victim believed incident was fraud</li> </ul>
<b>Relationship and trust</b>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return*</li> </ul>	<ul style="list-style-type: none"> <li>• Paid money +</li> <li>• Didn't get promised return +</li> <li>• Victim believed incident was fraud</li> </ul>

\*Respondents were asked a single question that encompassed both paying money and learning that the promised benefit did not exist.

+ Denotes the addition of another criteria to meet fraud definition.

#### 1.1.4 Cognitive Testing

Before fielding the SFS, RTI collaborated with BJS to conduct intensive cognitive testing of the SFS instrument.<sup>9</sup> Cognitive testing is the process of ensuring that potential respondents consistently understand and interpret the survey questions as worded and that the responses provided are valid and accurate. A major focus of the cognitive testing process for the SFS was ensuring that the fraud screening questions would elicit reports of incidents that were in scope and correctly classified by fraud type.

RTI conducted approximately 300 cognitive interviews online using crowdsourcing techniques and another 40 were conducted in person. The crowdsourcing effort used volunteers who signed up for the Cint opinion web panel<sup>10</sup> and involved administering the SFS screener and collecting a brief description about the incident after all affirmative responses to screener questions. Trained researchers from RTI conducted the in-person interviews. The crowdsourcing and in-person interviews were conducted over multiple rounds, with refinements made to the survey questions between each round.

The initial rounds revealed that large proportions of respondents were answering screener questions affirmatively based on negative financial experiences that did not rise to the level of fraud. Examples included legitimate investments in which the respondent lost money, fast food items that did not look the way they did in pictures, and loans made to family or friends that were used for something other than the stated need. Incidents of identity theft and physical theft were also commonly captured by the screener in initial rounds of testing. Based on these findings, RTI and BJS continued to refine and clarify the screeners throughout the testing period until these errors were diminished. This process was critical for reducing the rates of false positive responses or respondents answering screener questions affirmatively because of negative financial experiences that did not rise to the level of fraud based on the SFS definition.

---

<sup>9</sup> RTI conducted cognitive testing of the SFS instrument in collaboration with BJS under the National Victimization Statistical Support Program cooperative agreement (award number 2011-NV-CX-K068).

<sup>10</sup> Additional information about the Cint panel is available at [www.cint.com](http://www.cint.com).

## 2 Comparison of SFS Estimates to Other Data Sources

Like other crimes, estimates of the prevalence of personal financial fraud can be highly influenced by methodological and definitional differences in how survey questions are worded and data are collected. To better understand how SFS estimates of the prevalence of fraud compare with estimates generated from other sources, RTI identified and examined 14 different sources of fraud data. These 14 sources represent the major collections of fraud data conducted during the 9-year period from 2010 to 2018 for which data are publicly available.<sup>11</sup> **Table 2-1** lists each of the sources and includes brief descriptive information about the years available, reference period, and the type of collection. **Appendices B** and **C** provide more detailed information about the data sources.

Methodological differences among the sources of fraud data that impact the comparability of prevalence estimates include the type of collection (administrative data versus survey data), the scope of the collection (types of fraud included, inclusion of identity theft or other types of white-collar crime, inclusion of attempted and completed, fraud), the data collection approach, survey mode and response rates; the population of interest, the reference year, reference period of the data, and whether the data are representative of the U.S. population (e.g., one data collection focused on Arizona and Florida only, one focused on persons outside of the United States, and one was international). These methodological differences are discussed in the context of key findings from the SFS and how they compare with findings from the other data sources.

### 2.1 Prevalence of Fraud

Based on findings from the SFS, the prevalence of personal financial fraud in 2017 among persons age 18 or older was 1.2% but could be as high as 1.6% or as low as 0.8% depending on how conservatively fraud was defined (**Table 2-2**). Among the 14 external data sources, fraud prevalence rates ranged from a low of less than 0.1% to a high of 21.0% (**Table 2-3**).

#### 2.1.1 Impact of How Fraud is Defined and Operationalized on Prevalence Rates

As noted previously, a significant challenge in measuring fraud is the lack of a consistent definition. How inclusive or exclusive data collections are in terms of the types of fraud examined can have a major impact on prevalence rates and the comparability of findings. Putting aside measurement error and other definitional differences, one would expect that a collection that covers a subset of fraud—for instance, one that focuses specifically on investment fraud—would result in lower overall prevalence rates than the SFS, which includes investment fraud as one of seven fraud types. This assumption did not hold true among the data sources examined, however. The two collections with the highest prevalence rates—the Investment Fraud and Vulnerability Study (18.3%) and the Microsoft Tech Support Scam Survey (21.0%)—each focused on a single fraud type but showed rates of fraud about 15 times higher than the SFS (**Table 2-3**). If the SFS findings are limited to investment fraud to be more comparable to the Investment Fraud and Vulnerability Study, the difference between the estimates is even larger (less than 0.1% vs. 18.3%).<sup>12</sup>

---

<sup>11</sup> The Federal Trade Commission conducted the Consumer Fraud in the U.S. survey in 2017, but the results had not been released at the time of the analysis.

<sup>12</sup> For additional information on the American Association of Retired Persons (AARP) Investment Fraud Vulnerability Study, see [https://www.aarp.org/content/dam/aarp/research/surveys\\_statistics/econ/2017/investment-fraud-vulnerability.doi.10.26419%252Fres.00150.001.pdf](https://www.aarp.org/content/dam/aarp/research/surveys_statistics/econ/2017/investment-fraud-vulnerability.doi.10.26419%252Fres.00150.001.pdf).

**Table 2-1: Data Sources Examined for Comparison to Supplemental Fraud Survey Estimates**

Name	Sponsor	Data Year <sup>a</sup>	Reference Period <sup>b</sup>	Type of Collection	Coverage	Prevalence Rate
Supplemental Fraud Survey	Bureau of Justice Statistics	2017	12 months	Survey	U.S.	1.25%
Crime Survey of England and Wales	Office for National Statistics (U.K.)	2017	12 months	Survey	U.K.	1.50
Investment Fraud and Vulnerability Study	AARP <sup>c</sup>	2017	12 months	Survey	U.S.	18.30
Identity Fraud Survey	Javelin Research	2017	12 months	Survey	U.S.	6.64
Microsoft Tech Support Scam Survey	IPSOS Public Affairs	2016	12 months	Survey	11 countries, including U.S.	21.00
Fraud Watch Network Survey	AARP	2013	12 months	Survey	U.S.	2.08
Financial Fraud and Fraud Susceptibility in the U.S.	FINRA Foundation	2012	Lifetime	Survey	U.S.	11.00
Consumer Fraud in the United States	Federal Trade Commission	2011	12 months	Survey	U.S.	10.77
Exploitation of the Elderly in Arizona and Florida	Holtfreter and colleagues	2011	12 months	Survey	AZ & FL	13.58
National Public Survey on White-Collar Crime	National White Collar Crime Center	2010	12 months	Survey	U.S.	16.50
National Incident-Based Reporting System	Federal Bureau of Investigation	2016	12 months	Law Enforcement	6,570/17,429 agencies	0.07
ScamTracker Risk Report	Better Business Bureau	2017	12 months	Consumer complaints	U.S.	0.01
Consumer Sentinel Network	Federal Trade Commission	2017	12 months	Consumer complaints	U.S.	0.47
Internet Crime Complaint Center	Federal Bureau of Investigation	2017	12 months	Consumer complaints	U.S.	0.08
Fraud.org Top Scams of 2018	National Consumers League	2018	12 months	Consumer complaints	U.S.	N/A

N/A = Not available.

<sup>a</sup> 2017 used, when possible, for comparability with SFS; otherwise, reflects most recent year available.

<sup>b</sup> 12 months used when available for comparability.

<sup>c</sup> American Association of Retired Persons

**Table 2-2: Prevalence of Types of Fraud, by Fraud Screening Criteria, 2017**

Type of Fraud	Percentage				
	Fraud 1 <sup>a</sup>	Fraud 2 <sup>b</sup>	Fraud 3 <sup>c</sup>	Fraud 4 <sup>d</sup>	Fraud 5 <sup>e</sup>
Total	1.60%	1.25%	0.95%	0.78%	0.95%
Prize and grant	0.17	0.11	0.11	0.11	0.11
Phantom debt	0.12	0.12	0.12	0.12	0.12
Charity	0.14	0.14	0.14	0.14	0.14
Employment	0.09	0.06	0.05	0.04	0.06
Investment	0.03	0.01	0.01	0.01	0.01
Product and services	1.08	0.81	0.52	0.34	0.81
Relationship and trust	0.06	0.06	0.06	0.06	0.06

Note: Types do not sum to total because of victims who experienced multiple types of fraud. See **Table A-10** for standard errors.

<sup>a</sup> Includes all respondents who answered affirmatively to one of the screening questions, regardless of whether the response was enough to screen them into the incident report.

<sup>b</sup> Respondents who screened into the survey as victims of fraud.

<sup>c</sup> Respondents who screened into the survey as victims of fraud and, for prize and grant, employment, investment, and product and services fraud, additionally answered affirmatively that they tried to get their money back.

<sup>d</sup> Respondents who met the criteria for Fraud 3 and for employment and product and services fraud and additionally did not believe they would ever get their money back.

<sup>e</sup> Respondents who screened into the survey as victims of fraud and answered affirmatively that they believed the incident was fraud.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table 2-3: Fraud Prevalence Rates and Types of SFS Fraud Measured by Each Collection, by Type of Collection**

Type of Collection and Name	Prevalence Rate <sup>a</sup>	Types of Fraud Measured						
		Prize and Grant	Phantom Debt	Charity	Employment	Investment	Product and Services	Relationship and Trust
Survey								
Supplemental Fraud Survey	1.25%	●	●	●	●	●	●	●
Crime Survey of England and Wales	1.50						●	
Fraud Watch Network Survey	2.08	●			●		●	●
Identity Fraud Survey	6.64							
Consumer Fraud in the United States	10.77	●			●		●	
Financial Fraud and Fraud Susceptibility in the U.S.	11.00	●				●		
Exploitation of the Elderly in Arizona and Florida	13.58	●		●	●		●	
National Public Survey on White-Collar Crime	16.50					●	●	
Investment Fraud and Vulnerability Study	18.30					●		
Microsoft Tech Support Scam Survey	21.00						●	
Law Enforcement								
National Incident-Based Reporting System <sup>b</sup>	0.07%	●	●	●	●	●	●	●
Consumer Complaints								
ScamTracker Risk Report	0.01	●	●	●	●	●	●	●
Internet Crime Complaint Center	0.08	●	●	●	●	●	●	●
Consumer Sentinel Network	0.47	●	●	●	●	●	●	●
Fraud.org Top Scams of 2018	N/A	●	●				●	●

Notes: Across collections there may be differences in the definitions and specific scams included under each broader fraud type. N/A = Not available.

<sup>a</sup> Rates exclude identity theft and other crimes, such as fraud against businesses, that are not included in the SFS.

<sup>b</sup> NIBRS captures incidents of wire fraud, which encompass any type of fraud perpetrated using an electronic communication platform.

In general, data collections that covered a more complete range of the fraud types included in the SFS had lower prevalence rates than the collections that focused on a limited subset of fraud. For example, both the Better Business Bureau's (BBB) Scam Tracker and the Internet Crime Complaint Center (IC3) included the full scope of fraud types included in the SFS but had prevalence rates of less than 0.1% whereas the National Public Survey on White-Collar Crime, which covered two fraud types, showed a prevalence rate of 16.5%. This suggests that other factors beyond the definition are impacting the comparability of findings. One apparent difference is that the collections covering the full range of SFS fraud but with lower prevalence rates are administrative record collections rather than self-report surveys.

### 2.1.2 Impact of the Type of Data Collection on Fraud Prevalence Rates

A key methodological difference among fraud data collections that can impact the comparability of findings is whether data are collected through a self-report survey or through official administrative records from consumer agency complaints or police reports. Unlike surveys, which often collect data on incidents that were not formally reported to an investigative or enforcement entity, complaint and law enforcement data only capture formally reported incidents. Fraud prevalence rates from the administrative data collections ranged from less than 0.1% to 0.5%. Unlike survey data where the unit of analysis is individuals within a population of interest, the unit of analysis for these administrative collections is each report submitted, meaning that one victim could submit multiple reports about different incidents or multiple reports about the same incident (**Table 2-4**). It was not possible to identify the number of reports or complaints from unique victims, so these estimates may be an overestimation because they assumed that each report was associated with a unique victim.<sup>13</sup> Still, they are considerably lower than rates generated from fraud surveys, as expected. Among the estimates from self-report surveys, the SFS was at the low end of the range at 1.2%, whereas the Microsoft Tech Support Scam Survey was at the high end at 21.0%. The estimate closest to the SFS (1.5%) was from the Crime Survey of England and Wales (CSEW) (1.5%), which only covered one of the seven fraud types included in the SFS but did have a larger sample size (nearly 17,000) than the other fraud surveys.

### 2.1.3 Differences in Fraud Prevalence Rates because of a Top-Down Versus Bottom-Up Collection Approach

The SFS uses a top-down approach to identify and classify fraud victims. The survey screens for broad categories of fraud and then drills down to more specific types. Most of the other fraud collections gather data about very specific fraud experiences and then roll the responses into an "overall" fraud estimate. The SFS approach is intended to produce a more comprehensive and exhaustive estimate of fraud. However, one downside of this approach is that the broad screener questions may be too vague to trigger recall adequately.

Comparing the FTC's Consumer Fraud Survey and the SFS exemplifies the distinction between the top-down and bottom-up measurement approaches. Using the bottom-up approach, the FTC measures the prevalence of credit repair service fraud with the question: "In the past YEAR, have you paid money to anyone who promised to remove negative, but true, information from your credit record?"

---

<sup>13</sup> The NCVS-weighted population of persons 18 or older was used as the denominator for the rate calculations.

**Table 2-4: Fraud Prevalence Rates, by Source and Characteristics**

Type of Collection and Name	Unit of Analysis	Sample Size/ Number of Reports	Weighted Estimates Provided <sup>a</sup>	Number of Victims/ Comparable Reports <sup>b</sup>	Denominator	Prevalence Rate <sup>c</sup>
<b>Survey</b>						
<b>Supplemental Fraud Survey</b>	Person	66,229	Yes	3,039,199	244,067,296	1.25%
Crime Survey of England and Wales	Person	16,849	Yes	909,000	59,000,000	1.50
Fraud Watch Network Survey	Person	11,741	No	233	11,217	2.08
Identity Fraud Survey	Person	5,000	Yes	16,700,000	250,000,000	6.64
Consumer Fraud in the United States	Person	3,638	Yes	25,600,000	237,660,000	10.77
Financial Fraud and Fraud Susceptibility in the U.S.	Person	2,364	No	260	2,364	11.00
Exploitation of the Elderly in Arizona and Florida	Person	2,000	No	211	1,553	13.58
National Public Survey on White-Collar Crime	Person	2,503	No	413	2,503	16.5
Investment Fraud and Vulnerability Study	Investors	1,028	No	214 known + 149 identified	814	18.30
Microsoft Tech Support Scam Survey	Person	1,000	No	210	1,000	21.00
<b>Law Enforcement</b>						
National Incident-Based Reporting System	Report	402,974	~	160,495	244,067,296	0.07
<b>Consumer Complaints</b>						
ScamTracker Risk Report	Report	47,827	~	31,320	244,067,296	0.01
Internet Crime Complaint Center	Report	301,580	~	197,431	244,067,296	0.08
Consumer Sentinel Network	Report	2,680,000	~	1,138,306	244,067,296	0.47
Fraud.org Top Scams of 2018	Report	N/A	~	N/A	N/A	N/A

~ = Not applicable; N/A = Not available.

<sup>a</sup> Sample counts are adjusted to reflect the larger population.

<sup>b</sup> Weighted estimates shown where possible. All attempts were made to include victims/reports that are comparable with the SFS definition of fraud and to exclude those that were outside of that scope (e.g., identity theft incidents).

<sup>c</sup> Rates exclude identity theft and other crimes, such as fraud against businesses, that are not included in the SFS.

Respondents who answered affirmatively to this question are combined with respondents who answered affirmatively to similar questions about 17 different fraud types, including imposter scams, shop-at-home scams, travel, vacations or timeshare scams, foreign money offer scams, and mortgage foreclosure relief scams, to generate an overall prevalence of fraud. In contrast, to measure credit repair service fraud in the SFS, respondents were first asked a broad screener question about any experiences with product and services fraud: “In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you paid for any products or services that you NEVER received or that turned out to be a SCAM?” If the respondent answered affirmatively to be screened in as a victim of product and services fraud, they were then asked to think about the most recent incident of product and services fraud experienced during the prior 12 months and given the question: “Which ONE of the following BEST DESCRIBES the type of service you were trying to purchase? Was it... A service to remove negative information from your credit report?” The latter exemplifies the top-down approach of leading with a broader question and then drilling down to more specific questions.

#### 2.1.4 Impact of Including Identity Theft as a Type of Fraud on Prevalence Rates

Another issue that could impact the comparability of prevalence rates is the inclusion of identity theft in the fraud estimates. BJS separately defines and measures identity theft and personal financial fraud, with the distinction being whether respondents willingly provided personal information. In the case of identity theft, the victim’s personal information (e.g., account information, social security number) is obtained and used without their permission whereas in the case of personal financial fraud, the victim provides personal information willingly but has been deceived about what they will receive in return for providing that information. Rates of identity theft, which are derived from the BJS Identity Theft Supplement to the NCVS and include the misuse of someone’s existing account or the misuse of someone’s personal information to open a new account or for other reasons, were considerably higher than SFS rates of personal financial fraud (**Table 2-5**). For most of the 14 data sources reviewed, it was possible to separate identity theft from financial fraud, at least to generate counts of victims or reports. However, sometimes events like monetary losses are not separately reported for fraud and ID theft. Five surveys—Investment Fraud and Vulnerability, Microsoft Tech Support Scam, FraudWatch Network, Financial Fraud and Fraud Susceptibility, and Consumer Fraud in the U.S.—are comparable to the SFS in that they did not ask about identity theft. On the other hand, the majority of “fraud” in the CSEW and the NIBRS actually meets the BJS definition of identity theft, rather than fraud. When identity theft is separated from SFS-comparable frauds, the prevalence of fraud declined from 0.2% to 0.01% based on NIBRS data and from 6.4% to 1.5% based on CSEW data.

#### 2.1.5 Impact of Mode Effects on Prevalence Rates

Because BJS collected SFS data as a supplement to the NCVS, the survey used a combination of in-person and telephone interview modes. Approximately 45.6% of the interviews were conducted in person by Census Bureau interviewers going to the respondent’s residence, and the other 54.4% were conducted over the phone. Because the SFS used this mixed-mode approach, the estimates could be subject to mode effects. However, there were no statistically significant differences in the fraud prevalence rates regardless of whether SFS interviews were conducted in person or over the phone (**Table 2-6**).

Among the nine external surveys RTI examined, there were no discernible patterns of prevalence rates by mode (**Figure 3-1**). The SFS was the only mixed-mode survey; the others were largely split between telephone interviews and web-based self-administration. The CSEW, the survey with the closest prevalence rate to the SFS, was the only other survey that involved in-person data collection (**Table 2-7**).

**Table 2-5: Inclusion of Identity Theft in Fraud Data**

Collection Name	Includes	Can Be Broken Out	ID Theft			
			Count of Victims/Reports		Fraud Prevalence	
			With	Without	With	Without
Supplemental Fraud Survey	No	~	~	3,039,199	~	1.25%
BJS Identity Theft Supplement (2016)	Yes	~	25,952,400	~	10.2%	~
Crime Survey of England and Wales	Yes	Yes	3,775,000	909,000	6.4	1.50
Investment Fraud and Vulnerability Study	No	~	~	363	~	18.30
Identity Fraud Survey	Yes	No	16,700,000	~	6.64	~
Microsoft Tech Support Scam Survey	No	~	~	210	~	21.00
Fraud Watch Network Survey	No	~	~	233	~	2.08
Financial Fraud and Fraud Susceptibility in the U.S.	No	~	~	260	~	11.00
Consumer Fraud in the United States	No	~	~	25,600,000	~	10.77
Exploitation of the Elderly in Arizona and Florida	Yes	Yes	211	161	13.58	10.37
National Public Survey on White-Collar Crime	Yes	No	413	~	16.5	~
National Incident-Based Reporting System	Yes	Yes	411,304	160,495	0.17	0.07
ScamTracker Risk Report	Yes	Yes	47,827	31,320	0.02	0.01
Consumer Sentinel Network	Yes	Yes	1,509,367	1,138,306	0.61	0.47
Internet Crime Complaint Center	Yes	Yes	261,191	197,431	0.11	0.08
Fraud.org Top Scams of 2018	No	~	~	N/A	~	N/A

~Not applicable; N/A = Not available.

**Table 2-6: Count of Victims and Prevalence of Fraud, by Type of Fraud and Interview Mode, 2017**

Type of Fraud	In Person		Telephone	
	Number of Victims	Prevalence Rate	Number of Victims	Prevalence Rate
N	114,448,386	100.00%	129,618,909	100.00%
Total fraud	1,337,157	1.17	1,702,042	1.31
Prize and grant	133,089	0.12	130,601	0.10
Phantom debt	128,007	0.11	168,615	0.13
Charity	118,530	0.10	223,420	0.17
Employment	55,232	0.05	95,230	0.07
Investment	31,002 !	0.03	5,008 !	/
Product and services	837,519	0.73	1,144,718	0.88
Relationship and Trust	83,197	0.07	71,991	0.06

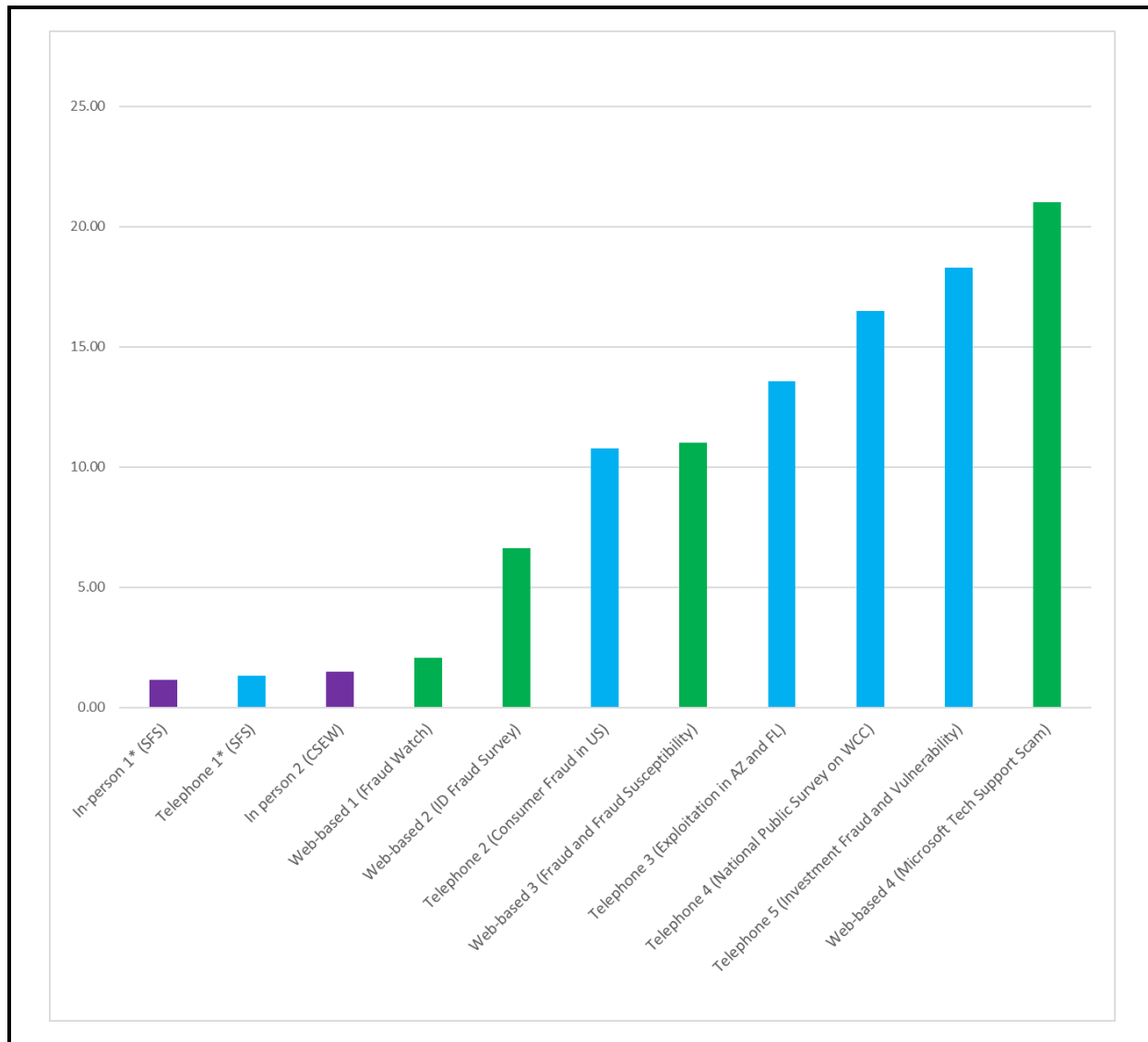
Note. See **Table A-11** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

/Less than 0.005%

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Figure 2-1: Fraud Prevalence Rates by Mode of Administration Among the SFS and External Surveys**



Note: Color of bars corresponds with survey mode. Purple bars = in-person or face-to-face interview; blue bars = telephone; green bars = web.

\*Denotes the SFS prevalence rate for each mode.

**Table 2-7: Fraud Prevalence Rates and Mode of Administration Among the Surveys**

Collection	Prevalence Rate*	Mode
Supplemental Fraud Survey (SFS)	1.25%	In-person and telephone interviews
<b>SFS in person</b>	1.17	In-person interview
<b>SFS telephone</b>	1.31	Telephone interview
Crime Survey of England and Wales	1.50	In-person interview
Fraud Watch Network Survey	2.08	Web-based self-administration
Identity Fraud Survey	6.64	Web-based self-administration
Consumer Fraud in the United States	10.77	Telephone interview
Financial Fraud and Fraud Susceptibility in the U.S.	11.00	Web-based self-administration
Exploitation of the Elderly in Arizona and Florida	13.58	Telephone interview
National Public Survey on White-Collar Crime	16.50	Telephone interview
Investment Fraud and Vulnerability Study	18.30	Telephone interview
Microsoft Tech Support Scam Survey	21.00	Web-based self-administration

\*Rates exclude identity theft and other crimes, such as fraud against businesses, that are not included in the SFS.

## 2.2 Most Common Types of Fraud

A prevalence rate of 1.2% translates to over 3 million victims of fraud during a 12-month period (**Table 2-8**). The most common type of fraud identified by the SFS was consumer product and services fraud, in which the victim paid for a product or service that they never received or that turned out to be a scam. Nearly 2 million victims, or 65.2% of fraud victims, experienced products and services fraud. About 1 in 10 fraud victims experienced charity fraud (11.3%; donating money to a charity or a charitable cause that later turned out to be or was suspected to be fake), phantom debt fraud (9.8%; paying money to settle or pay off taxes or a debt that was not real or was not actually the victim's), and prize and grant fraud (8.7%; paying money to receive a prize, grant, inheritance, lottery winning, or sum of money that was not actually received). About 5.0% of fraud victims experienced relationship and trust fraud (giving money to someone who pretended to be a family member, friend, caregiver, or romantic interest) and employment fraud (paying money to get a job or get into a business opportunity that was not what was promised); 1.2% of victims experienced investment fraud (investing money with a person or company that lied about what would be received in return).

### 2.2.1 Impact of Differences in How Fraud Types are Defined

To understand how the distributions of types of fraud in the SFS data compared with other sources, RTI examined the four collections arguably most like the SFS in terms of the scope of crimes covered. In three of four collections, products and services fraud accounted for the largest proportion of total fraud, but the percentages ranged from 44.7% according to ScamTracker data to 65.2% in the SFS (**Table 2-9**). Relationship and trust fraud was the most common fraud reported to the Consumer Sentinel, accounting for 30.6% of all fraud reports compared with 5.1% in the SFS. Charity fraud was one of the more common frauds experienced by SFS victims (11.3%) but accounted for 1.0% or fewer of ScamTracker, Consumer Sentinel, and IC3 reports.

**Table 2-8: Number and Percentage of Fraud Victims by Type and Fraud Screening Criteria, 2017**

Type of Fraud	Fraud 1 <sup>a</sup>		Fraud 2 <sup>b</sup>		Fraud 3 <sup>c</sup>		Fraud 4 <sup>d</sup>		Fraud 5 <sup>e</sup>	
	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims
Total	3,909,727	100.00%	3,039,199	100.00%	2,308,803	100.00%	1,908,041	100.00%	2,328,714	100.00%
Prize and grant	405,847	10.38	263,690	8.68	263,690	11.42	263,690	13.82	214,701	9.22
Phantom debt	296,623	7.59	296,623	9.76	296,623	12.85	296,623	15.55	218,230	9.37
Charity	341,949	8.75	341,949	11.25	341,949	14.81	341,949	17.92	242,335	10.41
Employment	209,060	5.35	150,462	4.95	110,019	4.77	97,440	5.11	125,339	5.38
Investment	80,872	2.07	36,010	1.18 !	36,010	1.56 !	36,010	1.89 !	27,128	1.16 !
Product and services	2,634,527	67.38	1,982,237	65.22	1,267,442	54.90	832,244	43.62	1,554,320	66.75
Relationship and trust	155,188	3.97	155,188	5.11	155,188	6.72	155,188	8.13	121,548	5.22

Note: Types do not sum to total because of victims who experienced multiple types of fraud. See **Table A-12** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

<sup>a</sup> Includes all respondents who answered affirmatively to one of the screening questions, regardless of whether the response was enough to screen them into the incident report.

<sup>b</sup> Respondents who screened into the survey as victims of fraud.

<sup>c</sup> Respondents who screened into the survey as victims of fraud and, for prize and grant, employment, investment, and product and services fraud, additionally answered affirmatively that they tried to get their money back.

<sup>d</sup> Respondents who met the criteria for Fraud 3 and for employment and product and services fraud and additionally did not believe they would ever get their money back.

<sup>e</sup> Respondents who screened into the survey as victims of fraud and answered affirmatively that they believed the incident was fraud.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table 2-9: Number and Percentage of Fraud Victims, by Type of Fraud and Select Collections**

Type of Fraud	SFS <sup>a</sup>		ScamTracker Risk Report		Consumer Sentinel Network		Internet Crime Complaint Center		Consumer Fraud in the United States	
	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims
Total	3,039,199	100.00%	31,320	100.00%	1,138,306	100.00%	231,134	100.00%	25,600,000	100.00%
Product and services	1,982,237	65.22	13,988	44.66	290,104	25.49	126,884	54.90	15,600,000	60.94
Charity	341,949	11.25	419	1.34	3,703	0.33	436	0.19	~	~
Phantom debt	296,623	9.76	5,894	18.82	~	~	9,149	3.96	~	~
Prize and grant	263,690	8.68	6,041	19.29	180,636	15.87	26,147	11.31	3,000,000	11.72
Relationship and trust	155,188	5.11	485	1.55	347,829	30.56	15,372	6.65	~	~
Employment	150,462	4.95	2,429	7.76	145,089	12.75	15,784	6.83	4,100,000	16.02
Investment	36,010	1.18 !	238	0.76	15,079	1.32	3,089	1.34	~	~
Other <sup>b</sup>	~	~	1,826	5.83	~	~	34,264	14.82	3,600,000	14.06

Note: Types do not sum to total because of victims who experienced multiple types of fraud and missing data. See **Table A-12** for SFS standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

~Not applicable.

<sup>a</sup> Includes respondents who screened into the survey as victims of fraud.

<sup>b</sup> Includes unauthorized billing and other unclassified frauds.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

Some of the differences among the collections are likely attributed to the fact that the self-report surveys capture crimes that go unreported to official sources and the administrative sources differ in terms of which official sources they get their reports from. However, there are differences in the distribution of fraud types even between the two self-report surveys (Consumer Fraud in the U.S. Survey and SFS). For instance, employment fraud accounted for 16.0% of fraud in the Consumer Fraud in the U.S. Survey and 5.0% of fraud in the SFS. This demonstrates that even when similar types of collections cover one or more of the same fraud types, caution should be used when making comparisons because of potential differences in how those types are defined. For instance, both the SFS and the National Public Survey on White-Collar Crime collected data on products and services fraud (not shown). However, the White-Collar Crime Survey asked about two types of products and services fraud—price misrepresentation and unnecessary repairs—whereas the SFS screener question was designed to encompass a much broader range of products or services that were paid for but were never received or that turned out to be a scam (see **Appendix A** for detail on the types of scams included under each fraud type category).

Another challenge in comparing estimates of individual fraud types is the potential of including false positive reports by respondents. Before fielding the SFS, BJS, and RTI engaged in extensive cognitive testing of the survey questions to ensure they were accurately aligned with the FFRC/FINRA Foundation fraud taxonomy. A major focus of the cognitive testing efforts was on reducing the likelihood of false positives—respondents reporting about negative financial experiences that did not rise to the level of fraud according to the taxonomy’s and BJS’s definition. Other collections and surveys may not make the same effort to distinguish between negative financial experiences and incidents that rise to a criminal level of fraud. For instance, the threshold for defining fraud may account for differences in the level of employed fraud captured in the Consumer Fraud Survey versus the SFS:

- SFS: “Have you paid money to get a job or get into a business opportunity but were tricked or lied to about how the money would be used or what you would receive in return AND you did not get all your money back?”
- FTC: “Have you paid anyone for an opportunity to operate your own business, such as a small business opportunity or a franchise AND you made less than half as much money as you had been led to expect?”

The SFS threshold for fraud is that the respondent was tricked or lied to and did not get all their money back. The Consumer Fraud Survey does not have the same requirement that the respondent was tricked or lied to or that they receive all their money. Thus, the Consumer Fraud Survey could be capturing respondents who made less money than they expected to simply because they did not work hard enough or for some other non-fraudulent reason. Similarly, with other fraud types, such as products and services fraud and investment fraud, cognitive testing of the SFS instrument revealed high rates of false positive reporting by respondents who answered screener questions affirmatively based on negative financial experiences that did not rise to the level of fraud.

A challenge for both survey data and complaint data is the extent to which the information provided is verified. Typically, there are no further investigative follow-up efforts for survey data. On the complaint side, the extent to which the reports are verified through additional investigation likely differs from one agency to the next, and the sources are often not clear about the process used to review reports and eliminate those that cannot be confirmed to be fraud.

## 2.3 Reporting Behaviors

One of the major challenges with comparing SFS estimates with data from law enforcement and complaint records is that these sources may not capture a representative sample of victims. In other words, the victims who report to a law enforcement agency or consumer organization may be different and have experienced different types of fraud than those who do not report.

In 2017, about 20% of SFS fraud victims reported the crime to at least one law enforcement agency or consumer organization (**Table 2-10**). About 13.8% of personal financial fraud victims reported the incident to law enforcement (**Table 2-11**).<sup>14</sup> Victims of relationship and trust (37.0%) and phantom debt (31.5%) fraud were the most likely to report to police. In contrast, about 1 in 10 victims of employment fraud (12.7%), products and services fraud (10.0%), and charity fraud (8.9%) reported the incident to police.

**Table 2-10: Victim Reporting to Law Enforcement and Consumer Organizations, by Type of Fraud, 2017**

Type of Fraud <sup>a</sup>	Any Reporting <sup>b</sup>	
	Number	Percentage of Victims
Total	635,404	20.91%
Prize and grant	54,288	20.59
Phantom debt	115,077	38.80
Charity	47,758	13.97
Employment	26,024	17.30 !
Product and services	364,519	18.39
Relationship and trust	57,442	37.01

Note: Details may not sum to total because victims who experienced multiple types of fraud. See **Table A-13** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

<sup>a</sup> Investment fraud is included in the total but not shown separately because of small sample sizes.

<sup>b</sup> Includes victims who reported to the Federal Trade Commission, Better Business Bureau, Consumer Financial Protection Bureau, the office of their state's attorney general, the Internet Crime Complaint Center, or directly to a law enforcement agency.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

SFS fraud victims were less likely to report the incident to the BBB (5.6%), the office of their state's attorney general (5.0%), the Consumer Financial Protection Bureau (3.2%), the Federal Trade Commission (3.1%), or the IC3 (1.9%) than to a law enforcement agency (13.8%). This suggests that fraud data from these administrative records may significantly underestimate the total number of victims who experience fraud each year.

<sup>14</sup> Victims who experienced more than one incident of fraud during the 12-month reference period were asked about the most recent incident.

**Table 2-11: Victim Reporting to Law Enforcement and Consumer Organizations, by Type of Fraud and Organization, 2017**

Type of Fraud*	Federal Trade Commission		Better Business Bureau		Consumer Financial Protection Bureau		State Attorneys General Offices		Internet Crime Complaint Center		Law Enforcement Agencies	
	Number	Percentage of Victims	Number	Percent of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims
Total	93,429	3.07%	168,932	5.56%	96,387	3.17%	152,373	5.01%	57,619	1.90%	418,758	13.78%
Prize and grant	6,532	2.48 !	5,555	2.11 !	2,765	1.05 !	14,472	5.49 !	/	/ !	45,359	17.20
Phantom debt	29,385	9.91 !	29,097	9.81 !	22,237	7.50 !	34,815	11.74 !	/	/ !	93,362	31.47
Charity	10,201	2.98 !	18,009	5.27 !	17,107	5.00 !	5,461	1.60 !	/	/ !	30,470	8.91 !
Employment	/	/	1,717	0.11 !	10,518	6.99 !	12,714	8.45 !	5,219	3.47 !	19,088	12.69 !
Product and services	50,314	2.53	127,571	6.40	47,205	2.37 !	82,115	4.12	49,942	2.52 !	198,405	9.96
Relationship and trust	7,919	5.10 !	5,461	3.52 !	7,477	4.82 !	15,914	10.25 !	2,458	1.58 !	57,442	37.01

Note: Details may not sum to total because of victims who experienced multiple types of fraud. See **Table A-14** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

/Less than 1 or 0.005%.

\*Investment fraud is included in the total but not shown separately because of small sample sizes.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

### 2.3.1 Comparing SFS Complaint Reports to Complaints from Consumer Agencies

To have a more fair and direct comparison between the complaint data and the SFS data, SFS data can be restricted to victims who said in the survey that they reported the incident to a particular consumer agency. This enables comparison of the number of victims who said they reported to an organization to the number of complaints recorded by that organization. For example, about 170,000 SFS victims said that they reported the incident to the BBB in 2017 (**Table 2-12**). In contrast, the BBB's ScamTracker Database collected about 31,000 reports in 2017. The overall count difference between the two collections was largely driven by products and services fraud. About 128,000 SFS victims said they reported products and services fraud to the BBB, although the BBB showed about 14,000 products and services complaints. This difference could be attributed to the following: false positive SFS responses; victims confusing the BBB for another consumer agency when answering the SFS survey; definitional or scope differences between the two collections; not all legitimate complaints submitted to the BBB being submitted through the ScamTracker tool, or the BBB screening out complaints in the process of making determinations about which complaints are legitimate or in scope.

**Table 2-12: Number of Fraud Victims Who Submitted Consumer Complaints Based on SFS Data and Actual Consumer Complaint Data, 2017**

Type of Fraud	Better Business Bureau		Internet Crime Complaint Center		Consumer Sentinel	
	SFS	ScamTracker Risk Report	SFS	Internet Crime Complaint Center	SFS*	Consumer Sentinel Network
Total	168,932	31,320	57,619	231,134	619,443	1,138,306
Prize and grant	5,555	6,041	/	26,147	54,288	180,636
Phantom debt	29,097	5,894	/	9,149	115,077	~
Charity	18,009	419	/	436	47,758	3,703
Employment	1,717	2,429	5,219	15,784	20,805	145,089
Product and services	127,571	13,998	49,942	126,884	353,776	290,104
Relationship and trust	5,461	485	2,458	15,372	57,442	347,829
Other	~	1,826	~	34,264	~	~

Note: Details may not sum to total due to victims who experienced multiple types of fraud. See **Table A-14** for SFS standard errors.

/Less than 0.005 or 0.005%.

~ Not applicable.

\* Includes victims who reported to the Federal Trade Commission, Better Business Bureau, Consumer Financial Protection Bureau, states' attorneys general, or a law enforcement agency. The Consumer Sentinel Network includes each of these sources.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2017; Better Business Bureau, ScamTracker Risk Report, 2017; Federal Bureau of Investigation, Internet Crime Complaint Center, 2017; Federal Trade Commission, Consumer Sentinel Network, 2017.

In contrast, the number of SFS victims who said they reported to the IC3 or an entity included in the Consumer Sentinel Network<sup>15</sup> was lower than the number of reports recorded in each of these data collections. About 58,000 SFS victims claimed to have reported to the IC3 in 2017, but the IC3 recorded about 230,000 complaints. A large part of the difference between the SFS and IC3 was also driven by product and services fraud but with the IC3 reporting more than double the number of complaints (127,000) as SFS victims who said they reported to the IC3. Differences between the SFS and Consumer Sentinel data were not because of product and services fraud but rather relationship and trust fraud, for which the Consumer Sentinel (348,000) reported about six times more complaints than suggested by

<sup>15</sup> The Consumer Sentinel Network data includes reports of fraud from the Federal Trade Commission, Better Business Bureau, Consumer Financial Protection Bureau, States Attorneys Generals, and law enforcement agencies.

SFS data (57,000). These discrepancies between the SFS and the complaint data could also be attributed to a host of reasons from differences in the scope and definitions of the different fraud types, to the inability to tease out unique victims in the complaint data, to response error on the part of SFS respondents, and the inclusion of attempted fraud in the complaint data (see section 3.4.1 for more information about the impact of attempted fraud).

### 2.3.2 Comparing SFS Data on Fraud Reported to Police to NIBRS Law Enforcement Data

The FBI's NIBRS collection gathers incident-level data on financial fraud reported to law enforcement agencies around the country. The FBI defines fraud as "the intentional perversion of the truth for the purpose of inducing another person, or another entity, in reliance upon it to part with something of value or to surrender a legal right" (see **Table A-15** for NIBRS fraud definitions). The NIBRS collection does not cover the entire population of the United States. In 2016, the most recent year for which detailed fraud data were available at the time the analyses were conducted, 6,570 agencies (about 38%) submitted data to NIBRS on 402,974 victims of financial fraud. The 38% of NIBRS agencies represented about 30% of the U.S. population. Approximately 77.6% (312,757) of those victims were individuals; 17.3% (69,561) were businesses; 2.2% (8,940) were financial institutions; 2.1% (8,449) were government entities; and the remainder were law enforcement agencies, religious institutions, and other or unknown entities (see **Table A-16** for trends in the number of NIBRS fraud victims from 2013 to 2017). To compare to SFS data, the remainder of the analysis focuses on the individual victims of fraud.

The NIBRS definition of fraud includes several categories, such as hacking, credit card and ATM fraud, impersonation, other identity theft, and welfare fraud, which are out of scope for the SFS. The two types of NIBRS fraud also captured by the SFS are (1) false pretenses/swindle/confidence game frauds, which encompass any intentional misrepresentation of facts or the use of deceptive schemes or devices to obtain money, goods, or things of value and (2) wire fraud, which involves the use of electronic communication to intentionally transmit false or deceptive messages to facilitate fraudulent activity. Both frauds overlap to an unknown degree with the categories of fraud captured in the SFS.

To assess whether the SFS and NIBRS tell a consistent picture of who experienced fraud victimization, it was necessary to limit the SFS data to just victims who reported the crime to police, because victims who did not report may have a different profile from those who did. We compared the characteristics of SFS victims who reported the fraud to police with the demographic characteristics of victims who experienced the two NIBRS frauds consistent across both collections. We did not include Hispanic origin in the assessment because data on Hispanic origin were missing for 26% of NIBRS fraud victims (National Archive of Criminal Justice Data, 2016).

The NIBRS distribution of victims across the demographic categories of gender, race, and age was generally within the SFS margin of error (**Table 2-13**). The one statistically significant difference between the two collections was that among SFS victims who reported to police, a higher percentage were ages 50 to 64 (37.3%) compared with the proportion of victims ages 50 to 64 in the NIBRS data (24.5%) (see **Table A-17** for the full scope of NIBRS fraud offenses by demographic characteristics of victims).

**Table 2-13: Demographic Characteristics of NIBRS and SFS Victims**

Characteristic	Total NIBRS Fraud Victims <sup>a</sup>	2016 NIBRS Frauds Captured in SFS				SFS Fraud <sup>b</sup>			
		Number		Percent		Reported to Police		Not Reported to Police	
		False Pretenses/ Swindle/ Confidence Game	Wire Fraud	Total Comparable Fraud Victims	Total	Number	Percentage	Number	Percentage
Total Individual victims	312,757	94,104	8,346	102,450	100.00%	426,165	100.00%	2,613,034	100.00%
Sex									
Male	145,124	44,577	3,733	48,310	47.15	178,598*	41.91	1,194,454	45.71
Female	164,514	48,557	4,571	53,128	51.86	247,567*	58.09	1,418,580	54.29
Unknown	3,119	990	42	1,032	1.01	~	~	~	~
Race									
White	240,201	69,865	6,480	76,345	74.52	351,855*	82.56	1,963,030	75.12
Black	41,665	14,973	1,067	16,040	15.66	41,912 !	9.83	439,425	16.82
American Indian/ Alaska Native	6,160	326	40	366	0.36	10,518 !	2.47	16,083	0.62
Asian/Pacific Islander	1,117	2,050	212	2,262	2.21	16,708 !	3.92	116,995	4.48
Asian	1,056	2,037	210	2,247	2.19	~	~	~	~
Native Hawaiian/ Other Pacific Islander	61	13	2	15	0.01	~	~	~	~
Two or more races	~	~	~	~	~	5,173 !	1.21	77,501	2.97
Unknown	23,614	6,910	547	7,457	7.28	~	~	~	~
Age									
Juvenile	3,494	1,143	101	1,244	1.21	~	~	~	~
18–34 Years	86,288	25,297	2,187	27,484	26.83	73,089*	17.15	831,160	31.81
35–49 Years	84,159	22,616	1,931	24,547	23.96	76,204*	17.88	625,602	23.94
50–64 Years	81,488	23,056	2,075	25,131	24.53	159,087*	37.33	681,068	26.06
65+ Years	51,810	19,959	1,945	21,904	21.38	117,785*	27.64	475,205	18.19
Unknown	5,553	2,053	107	2,160	2.11	~	~	~	~

Note: Subgroups may not sum to total because of missing data and NIBRS victims experiencing multiple types of fraud. See **Table A-18** for SFS standard errors.

! Interpret with caution. Estimate based on 10 or fewer sample cases.

<sup>a</sup> Includes individual victims, excluding frauds committed against businesses, governments, religious organizations, financial institutions, and other entities. Frauds included in NIBRS definition but not the SFS include hacking/computer invasion (512 individual victims), credit card and ATM fraud (100,319 victims), impersonation (88,008 victims), identity theft (30,007 victims), and welfare fraud (412 victims).

<sup>b</sup> Includes prize and grant, phantom debt, charity, employment, product and services, and relationship and trust fraud.

\*Significantly different from the comparable NIBRS total number/percentage at the 95% confidence level.

~ Not available/applicable.

Sources: Bureau of Justice Statistics, National Crime Victimization Survey, 2017; Federal Bureau of Investigation, National Incident-Based Reporting System, 2016.

### 2.3.3 Impact of Capturing Victims Who Do Not Identify as Victims

The SFS screening questions are behaviorally specific, asking respondents about experiences they may have had, rather than asking them to define themselves as fraud victims. This approach may also contribute to differences between the SFS and administrative sources of fraud data. Victims who experienced fraud but did not think of themselves as victims are unlikely to report their experiences to law enforcement or a consumer complaint agency.

To get a sense of how victim perceptions of their own victim status varied across different types of fraud, respondents who screened into the survey were asked toward the end of the interview, “Do you think you were a victim of fraud?” Among the high-level fraud categories (seven fraud types measured in SFS), the percentage of victims who answered the question affirmatively ranged from 81.4% of prize and grant fraud victims to 68.7% of charity fraud victims (**Table 2-14**). However, there was more variation across different types of scams. About a third of victims of medical billing fraud (32.2%) and almost half of business growth services fraud victims (42.1%) believed they were victims. In contrast, more than 90% of victims of a government loan or grant scam (93.4%), a loan debt scam (>99.5%), insurance services fraud (>99.5%), and credit repair services fraud (>99.5%) believe that the incident was fraud.

**Table 2-14: Percentage of Victims Who Believed What They Experienced Was Fraud, 2017**

Type of Fraud	Percentage	Type of Fraud	Percentage
Prize and grant fraud	81.40%	Product and services	78.00%
Lottery scam	88.40 !	Product type	
Sweepstakes scam	73.80	Weight loss or health supplements	79.70
Inheritance scam	/ !	Clothing or accessories	75.40
Government loan or grant scam	93.40	Collectibles or memorabilia	73.00 !
Other prize and grant fraud/a	89.80 !	Electronics or software	83.90
Phantom debt fraud	72.40	Auto parts	87.00
Unpaid taxes fraud	55.90	Other products/d	76.30
Loan debt scam	// !	Service type	
Unpaid fine fraud	87.20 !	Insurance	// !
Unpaid credit card charges fraud	58.70 !	Computer repair services	88.60
Medical billing fraud	32.20 !	Home or auto repairs	72.90
Other phantom debt fraud/b	92.90	Internet or phone services	84.80 !
Charity fraud	68.70	Online gaming services	67.70 !
Bogus charitable organization scam	70.60	Identity theft protection services	57.90 !
Crowdfunding under false pretenses/c	81.80 !	Credit repair services	// !
Employment fraud	83.30	Vacation rental services	87.80 !
Business opportunities fraud	77.70	Business growth services	42.10 !
Work-at-home scam	83.80 !	Adoption services	/
Government job placement scam	/	Other services/e	64.90
Investment fraud	75.30 !	Relationship and trust	76.50
		Romantic	65.60 !
		Family member	84.10 !

Note: See **Table A-19** for standard errors.

! Interpret with caution. Estimate based on 10 or fewer cases.

/ Less than 0.005%.

// Greater than 99.5%.

<sup>a</sup> Includes tax refund scam, Nigerian letter fraud, and other frauds in which the victim was promised money or prizes that he or she never received.

<sup>b</sup> Includes other frauds in which the victim paid money to settle a debt but found out the charges did not exist.

<sup>c</sup> Crowdfunding is the practice of collecting online contributions to fund a project or cause. Crowdfunding websites include GoFundMe and Kickstarter.

<sup>d</sup> Includes products such as gemstones, medical devices, cemetery plots, and online marketplace products.

<sup>e</sup> Includes services such as debt relief and immigration services.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

Unfortunately, there may be other reasons for not reporting the incident through formal channels, even among victims who believed the incident was fraud. Therefore, limiting the analysis to just those victims who believed they experienced fraud will not necessarily make the findings comparable to the administrative data sources. However, when comparing across sources, whether the collection captures victims who do not self-identify as victims is another potential source of difference in estimates.

## 2.4 Financial Losses

Because of the focus on aligning with the fraud taxonomy and ensuring that the survey captures criminal fraud rather than negative financial experiences, BJS designed the SFS to capture completed frauds—those in which the victim experienced a financial loss—and exclude attempted frauds in which the victim received a fraudulent offer but did not pay money to the fraudster. To avoid capturing these attempted incidents, each of the SFS screening questions includes language essentially asking, “Did you pay money for \_\_\_\_\_” with follow-up questions to ascertain whether the person got what they were promised for their payment or received all their money back.

SFS victims experienced \$3.3 billion in out-of-pocket losses in 2017 (**Table 2-15**). The average direct out-of-pocket losses were highest among victims of relationship and trust fraud (\$3,600). Charity fraud victims averaged the lowest financial loss compared with other types of victims (\$70).

**Table 2-15: Average Out-of-Pocket Financial Losses Experienced by Victims of Fraud, by Type of Fraud, 2017**

Financial Losses	Types of Fraud						
	Prize or Grant,	Phantom Debt	Charity	Employment	Investment	Product and Services	Relationship and Trust
Mean	\$430	1,320	70	850	1,810	880	3,610
Median	\$200	700	30	400	3,000	100	400
Total Sum*	\$120,878,250	454,972,040	27,307,440	122,681,720	56,045,480	1,874,150,330	614,422,290

Note: Dollar amounts rounded to the nearest ten. See **Table A-20** for standard errors.

\*For each fraud type, approximately 2% of victims experienced the fraud multiple times during the reference period. To account for these losses, the average loss in each category was multiplied by the number of multiple victims and added to the total sum.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

Nearly 80% of charity fraud victims had out-of-pocket losses of less than \$100 (**Table 2-16**). In comparison, nearly 50% of investment fraud victims and 40% of phantom debt fraud victims lost \$1,000 or more. About 30% of employment fraud and relationship and trust fraud victims were defrauded of \$1,000 or more.

**Table 2-16: Percentage of Fraud Victims Experiencing Out-of-Pocket Financial Losses, by Type of Fraud, 2017**

Financial Losses	Types of Fraud						
	Percentage					Percentage	
	Prize or Grant	Phantom Debt	Charity	Employment	Investment	Product and Services	Relationship and Trust
Less than \$100	32.13%	11.68%	78.56%	16.83%!	24.67%!	47.40%	39.82%
\$100–\$499	34.33	27.04	16.06	35.41!	/!	28.52	7.19!
\$500–\$999	13.88!	19.54!	4.76!	12.21!	/!	10.12	15.41!
\$1,000 or more	10.35!	39.23	/!	31.52!	61.43!	13.04	31.18
Unknown	9.32	2.51	0.63	4.04	13.91	0.92	6.40
Got any money back	0.80!	6.30!	6.54!	/	/!	10.08	12.71!

Note: See **Table A-21** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer.

/Less than 0.005 or 0.005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

#### 2.4.1 Impact of Including Incidents with No Direct Financial Loss (Attempted Fraud) in Fraud Data

Unlike the SFS, many of the 14 external fraud data collections examined included both attempted fraud (also referred to as fraud susceptibility) and fraud that resulted in a direct financial loss. The inclusion of attempted fraud in the total victim counts or prevalence rates can impact the comparability of these sources to the SFS. For instance, the BBB ScamTracker data showed that 16% of all reported fraud in 2017 resulted in a financial loss (see **Appendix C**).<sup>16</sup> In other words, the majority of the 31,701 ScamTracker reports were attempted incidents that did not actually result in a financial loss for the targeted victim. Similarly, 21% of 2017 Consumer Sentinel reports involved a financial loss, meaning that the majority of reports captured attempted incidents.

Generally, the fraud prevalence rates from survey data could be limited to just victims who suffered a financial loss. For instance, the 2% prevalence rate based on the Fraud Watch Network survey includes only victims who experienced a financial loss. Expanding the definition to include those who responded to a fraud offer but did not lose money increases the prevalence rate to 6.8% and expanding it even further to include all who received a fraudulent offer increases the rate to 67%.<sup>17</sup> The FTC Consumer Fraud in the U.S. survey focused specifically on victims who paid money in connection with an incident of fraud. However, the FTC does not report on whether any victims still reported incidents that resulted in \$0 losses and explicitly notes that many prize and grant fraud victims did not incur monetary losses because “the injury is often the value of the time spent attending a sales presentation.”<sup>18</sup>

#### 2.5 Characteristics of Fraud Victims

The SFS data showed no statistically significant<sup>19</sup> differences in the demographic distributions of fraud victims defined by *Fraud 1* (most inclusive definition), *Fraud 2* (screening definition), *Fraud 4* (most exclusive), or *Fraud 5* (respondent identified as a victim).<sup>20</sup> For example, regardless of which definition was used, the percentage of female fraud victims was slightly higher than 50% and the percentage of male victims was slightly lower than 50%. In other words, using a different definition of fraud does not provide a different picture of the characteristics of fraud victims.

Regardless of the fraud definition used, there were also no statistically significant differences across demographic groups in the prevalence of personal financial fraud. Male respondents (1.2%) and female respondents (1.3%) were equally likely to experience personal financial fraud and accounted for a similar percentage of victims (~50%) (**Table 2-17**). White respondents accounted for the majority of victims (62%) but had a statistically similar prevalence rate (1.2%) as black respondents (1.7%) and Hispanic (1.2%) respondents. Likewise, persons age 50 or older accounted for nearly 50% of all fraud victims, but the prevalence rates for persons ages 50 to 64 (1.4%) and 65 or older (1.2%) were not

---

<sup>16</sup> <https://www.bbb.org/globalassets/local-bbbs/council-113/media/scam-tracker/risk-report/bbbcamtrackerannualreport-final-2017.pdf>

<sup>17</sup> [https://www.aarp.org/content/dam/aarp/research/surveys\\_statistics/econ/2014/Caught-Scammer-Net-Risk-Factors-Internet-Fraud-Victims.doi.10.26419%252Fres.00076.001.pdf](https://www.aarp.org/content/dam/aarp/research/surveys_statistics/econ/2014/Caught-Scammer-Net-Risk-Factors-Internet-Fraud-Victims.doi.10.26419%252Fres.00076.001.pdf)

<sup>18</sup> [https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey\\_0.pdf](https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf), page 41.

<sup>19</sup> All references to statistically significant findings are based on statistical testing at the 95% confidence level.

<sup>20</sup> Fraud 3 is excluded because there is only a difference in definition from Fraud 2 in four of the fraud types (prize and grant fraud, employment fraud, consumer investment fraud, and products and services fraud).

statistically different from those in the younger age groups. There were also no statistically significant differences in the prevalence of fraud across different levels of household income.

**Table 2-17: Demographic Characteristics of Fraud Victims, by Fraud Definition, 2017**

Characteristics	Percentage							
	Fraud 1		Fraud 2		Fraud 4		Fraud 5	
	Experiencing Fraud	Fraud Victims	Experiencing Fraud	Fraud Victims	Experiencing Fraud	Fraud Victims	Experiencing Fraud	Fraud Victims
Total	1.60%	100.00%	1.25%	100.00%	0.78%	100.00%	0.95%	100.00%
Sex								
Male	1.53	46.48	1.16	45.18	0.75	46.37	0.86	43.84
Female	1.67	53.52	1.33	54.82	0.81	53.63	1.04	56.16
Race/Hispanic origin								
White <sup>a</sup>	1.57	63.52	1.19	62.01	0.76	63.11	0.91	61.65
Black <sup>a</sup>	2.03	14.69	1.67	15.60	1.01	15.08	1.44	17.47
Hispanic	1.41	14.13	1.15	14.80	0.77	15.68	0.82	13.79
Other <sup>a,b</sup>	1.61	7.66	1.24	7.58	0.63	6.14	0.89	7.08
Age								
18–19	2.03	4.38	1.01	2.81	0.49	2.15!	0.91	3.30
20–24	1.69	9.11	1.39	9.62	0.82	9.04	1.05	9.48
25–34	1.55	17.07	1.22	17.33	0.72	16.24	0.94	17.30
35–49	1.45	21.93	1.19	23.09	0.76	23.48	0.95	24.14
50–64	1.72	27.40	1.35	27.64	0.92	29.86	0.98	26.18
65 or older	1.57	20.12	1.18	19.51	0.73	19.23	0.91	19.60
Household income								
Less than \$25,000	1.89	22.97	1.51	23.54	1.04	25.88	1.28	26.11
\$25,000–\$49,999	1.62	26.70	1.29	27.35	0.74	25.14	0.96	26.59
\$50,000–\$74,999	1.33	15.37	1.09	16.19	0.69	16.40	0.83	16.12
\$75,000–\$99,999	1.30	12.53	0.93	11.51	0.59	11.58	0.66	10.71
\$100,000–\$149,999	1.73	11.61	1.34	11.56	0.78	10.78	1.06	11.99
\$150,000 or more	1.83	10.83	1.29	9.85	0.84	10.23	0.85	8.49

Note: Demographic characteristics are imputed to account for missing data. See **Table A-22** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer.

<sup>a</sup> Excludes persons of Hispanic origin.

<sup>b</sup> Includes American Indians and Alaska Natives; Asians, Native Hawaiians, and Other Pacific Islanders; and persons of two or more races.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

### 2.5.1 Potential Impact of Sample Bias on Victim Characteristics

The SFS sample was selected using an address-based cluster sampling approach, and the survey had an overall response rate of 77.3%.<sup>21</sup> Five of the nine surveys examined reported their response rates. The CSEW had a relatively high response rate of 73%. Both the Consumer Fraud Survey and the National Public Survey on White-Collar Crime had response rates around 15%. The Fraud Watch Survey had a response rate of 51% and the survey on the Exploitation of the Elderly in Arizona and Florida obtained a response rate of 48%, but a completion rate of 83%.<sup>22</sup>

Lower response rates may suggest the presence of bias in the sample, which could in turn impact the picture of victimization that emerges. For example, the Consumer Fraud Survey showed differences in prevalence rates across different subgroups (e.g., blacks and Hispanics were significantly more likely than whites to experience fraud) that were not present in the SFS data.<sup>23</sup> Although the FTC did not find any differences in the demographic characteristics of those who refused to complete the survey, the characteristics of the 17,000 households that did not answer the phone were unknown. Differences in the characteristics of households that answered the phone and their likelihood of experiencing fraud victimization could impact the picture of victimization that emerges.

### 2.5.2 Variations in Victim Characteristics Based on the Population of Interest

BJS administered the SFS to a nationally representative sample of persons age 18 or older. Findings from data collections that include victims of all ages or victims in a narrower age range (e.g., 40 or older) may not be directly comparable with the SFS in terms of prevalence estimates or the profile of victims. None of the complaint databases explicitly exclude reports involving juveniles under the age of 18, so it is likely that some portion of the complaint data includes reports for persons under age 18. Often, the complaint reports ask for the age of the person submitting the complaint, but there is no way to know whether that person was also the victim or is submitting on behalf of a victim. Similarly, the FBI collects fraud reports from victims of all ages through NIBRS, but juvenile victims can be identified in those data. In 2016, approximately 1,200 fraud victims (1.2% of victims) in NIBRS were under the age of 18.

Additionally, data collections that are not nationally representative, such as the Exploitation of the Elderly in Arizona and Florida survey and NIBRS, will not produce estimates of the number of financial fraud victims that are directly comparable with the national SFS estimates. Caution should also be used when comparing fraud data from the United States with fraud data from another country (e.g., CSEW) for the purpose of estimate validation.

---

<sup>21</sup> For more information on the NCVS methodology, see [National Crime Victimization Survey \(NCVS\) | Bureau of Justice Statistics \(ojp.gov\)](#).

<sup>22</sup> Of those who responded to the phone call, 83% completed the survey.

<sup>23</sup> Consumer Fraud in the United States, 2011: [https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey\\_0.pdf](https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf).

### 3 Recommendations

The 14 other external sources of fraud data vary widely from the SFS and from each other in terms of their estimates of the prevalence and nature of fraud. These differences can be attributed to the broad range of definitions used to identify and classify fraud and the methodological approaches used to collect the data. Unfortunately, because of differences among the collections, it is not possible to make direct comparisons across the estimates or to determine which factors contribute to differences to the greatest degree. Although it is possible to control for some differences between the collections, it is not possible to control for all of them. For example, the SFS data could be restricted to just incidents that were reported to the police or a consumer agency to make the data more comparable to administrative data from NIBRS or the Consumer Sentinel. However, NIBRS is not nationally representative, the Consumer Sentinel collects data from a different population (e.g., all persons, regardless of age) than the SFS, and both collections use different definitions of fraud and include attempted incidents that do not result in financial loss. Because it is unknown to what extent these differences should result in counts of victims that are higher or lower than the SFS, it is not possible to further adjust these sources for true comparability.

Without having a way to verify the SFS findings or triangulate with other data sources, there is no way to know whether methodological decisions in the administration of the SFS could have suppressed reporting of particular fraud types or reduced the likelihood that certain types of fraud victims would participate. Because the 2017 SFS was the first attempt at conducting an NCVS fraud supplement, additional research is necessary to fully understand the impact of a variety of design decisions related to the wording, structure, and administration of the SFS on fraud prevalence estimates. To be most effective, this research should use experimental approaches that enable most survey characteristics to be held constant to isolate the effect of a particular design decision. For example, to understand whether the top-down measurement approach used in the SFS (i.e., using broad screener questions and drilling down to more specific fraud types) results in more false negative responses compared with a bottom-up approach (i.e., asking about specific fraud types in the survey and then rolling the responses up into larger categories), BJS could select a representative sample of persons age 18 or older and randomly assign them to receive one of two sets of screener questions reflecting the different approaches. Because of the experimental design, any differences in the estimate generated from the two screeners would be attributable specifically to the screener design. This approach could be replicated by varying multiple treatments randomly across respondents (e.g., mode, survey context, target sample).

Using an online probability-based panel would be an inexpensive and efficient way to conduct this type of experimentation. With an online probability panel, BJS could also explore other approaches to triggering recall in the survey using language related to the victim's being "scammed," "tricked," or "lied to" and could test the impact of differences in question-wording between the Consumer Fraud Survey and the SFS, all other factors held constant.

BJS designed the SFS to address many of the limitations identified in these other sources of data, so there are reasons to have confidence in the SFS data and results. Unfortunately, because of the wide variation in other external sources of fraud data, secondary data analysis is not sufficient to confirm whether differences between the SFS and other sources are because of improved measurement and lower rates of false positives in the SFS data or suppression effects from the methodology or design that result in higher rates of false negatives. Without additional experimental research, it is not possible to fully address this issue and validate the findings.

## References (data sources)

- Anderson, G. O. (2014, September 26). Identity theft: Who's at risk? *AARP Research*.  
<https://www.aarp.org/research/topics/economics/info-2014/identity-theft-incidence-risk-behaviors.html>
- Anderson, K. B. (2013). *Consumer fraud in the United States, 2011: The third FTC survey. Staff report*.  
<https://www.ftc.gov/reports/consumer-fraud-united-states-2011-third-ftc-survey>
- Applied Research & Consulting. (2013). *Financial fraud and fraud susceptibility in the United States research report*. <https://www.finrafoundation.org/files/financial-fraud-and-fraud-susceptibility-united-states-research-report-2012-national-survey>
- Better Business Bureau. (2018). *2017 BBB scam tracker annual risk report: New trends in scam risk*.  
<http://bbbfoundation.images.worldnow.com/library/a3949f5c-93cc-4e31-803b-bb77bf2e2c86.pdf>
- Federal Bureau of Investigation Internet Crime Complaint Center. (2018). *2017 internet crime report*.  
[https://www.ic3.gov/Media/PDF/AnnualReport/2017\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2017_IC3Report.pdf)
- Gregoire, C. (2016, October 17). Tech support scams are a growing problem. *Microsoft on the Issues*.  
<https://blogs.microsoft.com/on-the-issues/2016/10/17/tech-support-scams-growing-problem/#sm.0001el20x2191qf2dwnrwxckmqxzd>
- Holtfreter, K., Reisig, M. D., Mears, D. P., & Wolfe, S. E. (2014). *Financial exploitation of the elderly in a consumer context. Final report* (NCJ No. 245388). <https://nij.ojp.gov/library/publications/financial-exploitation-elderly-consumer-context>
- Huff, R., Desilets, C., & J., K. (2010). *The 2010 National Public Survey on White-Collar Crime. National White Collar Crime Center report*. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-public-survey-white-collar-crime-0>
- Marchini, K., & Pascual, A. (2019). *2019 identity fraud study: Fraudsters seek new targets and victims bear the brunt. Javelin strategy report*. <https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt>
- National Archive of Criminal Justice Data (2018, August 17). *National Incident-Based Reporting System, 2016: Extract files*. Inter-university Consortium for Political and Social Research.  
<https://doi.org/10.3886/ICPSR37066.v1>
- National Consumer League. (2019). *Top scams of 2018: Fraud.org report*.  
[https://fraud.org/romance\\_scams\\_2018topten/](https://fraud.org/romance_scams_2018topten/)
- Office for National Statistics. (2019). *Crime survey for England and Wales, 1996-2018: Secure access*. (8th ed.)
- Sauer, J. H. (2014, March). Caught in the scammer's net: Risk factors that may lead to becoming an internet fraud victim. *AARP Research*. <https://www.aarp.org/research/topics/economics/info-2014/internet-fraud-victimization-attitudes-behavior-national.html>

## Appendix A.

### Additional Findings From the SFS Analysis

#### Product and Services Fraud

In 2017, nearly 2 million persons experienced product and services fraud, the most common type of fraud (**Table A-1**). On the product side, over 320,000 victims purchased clothing or accessories that were never received or were not as promised. Almost 200,000 victims purchased fraudulent electronics or software, followed by over 130,000 victims who purchased fraudulent weight loss or health supplements. About 70,000 victims purchased automotive parts that were not what they were expecting to get and about 54,000 lost money on fraudulent collectibles or memorabilia.

**Table A-1: Prevalence of Product and Services Fraud, by Type of Product or Service Purchased, 2017**

Type of Fraud	Number	Percentage	
		Prevalence Rate	Fraud Victims
Total	3,039,199	1.25%	100.00%
Product and services fraud	1,982,237	0.81	65.22
Type of product purchased			
Clothing or accessories	320,189	0.13	10.50
Electronics or software	194,036	0.08	6.40
Weight loss or health supplements	133,996	0.05	4.40
Auto parts	70,404	0.03	2.30
Collectibles or memorabilia	54,271 !	0.02 !	1.80 !
Other products*	510,351	0.21	16.80
Type of service purchased			
Home or auto repairs	106,007	0.04	3.50
Computer repair services	96,740	0.04	3.20
Vacation rental services	62,742 !	0.03 !	2.10 !
Internet or phone services	30,086 !	0.01 !	1.00 !
Business growth services	25,349 !	0.01 !	0.80 !
Online gaming services	24,818 !	0.01 !	0.80 !
Identity theft protection services	16,523 !	0.01 !	0.50 !
Credit report repair services	15,967 !	0.01 !	0.50 !
Insurance	12,998 !	0.01 !	0.40 !
Adoption services	/ !	/ !	/ !
Other services**	169,494	0.07	5.60

Note: Details may not sum to total due to missing data. See **Table A-23** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

/Less than 0.005 or 0.005%.

\*Includes products such as gemstones, medical devices, cemetery plots, and online marketplace products.

\*\*Includes services such as debt relief and immigration services.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

On the services side, the most commonly purchased fraudulent service was home or auto repair services, which over 100,000 victims experienced. Nearly 100,000 victims lost money on fraudulent computer repair services in 2017, followed by about 63,000 who were defrauded on vacation rental services. About 30,000 victims purchased internet or phone services that turned out to be a scam and about 25,000 victims lost money on fraudulent business growth services and online gaming services.

## Charity Fraud

Of the approximately 340,000 victims who experienced charity fraud in 2017, over 280,000 (82.9%) had attempted to donate to an organization that they later found out was not real (**Table A-2**). Another 56,000 victims lost money donating to a fraudulent cause through a crowdfunding website, such as GoFundMe or Kickstarter, where individuals try to collect online contributions to fund a project or cause.

**Table A-2: Prevalence of Charity Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Percentage	
		Prevalence Rate	Fraud Victims
Total fraud	3,039,199	1.25%	100.00%
Charity fraud	341,949	0.14	11.25%
Bogus charitable organization scam	283,397	0.12	9.30
Crowdfunding under false pretenses*	55,906	0.02	1.80

Note: Details may not sum to total due to missing data. See **Table A-24** for standard errors.

\*Crowdfunding is the practice of collecting online contributions to fund a project or cause. Crowdfunding websites include GoFundMe and Kickstarter.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

## Phantom Debt Fraud

The most common phantom debt scheme that victims experienced in 2017 was unpaid taxes fraud, in which the perpetrator pretended to be a tax collector, claiming that the victim owed back taxes (**Table A-3**). About 32.0% of phantom debt fraud victims (about 95,000 victims) lost money to this type of scam. Over 50,000 victims (17.3%) lost money to a scam in which they were told that they had outstanding loan payments due. Another 41,000 victims paid money to resolve unpaid credit card charges that were not actually theirs, 24,000 lost money through medical billing scams, and 15,000 lost money through a scam in which they were told they had an unpaid fine.

**Table A-3: Prevalence of Phantom Debt Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Percentage	
		Prevalence Rate	Fraud Victims
Total fraud	3,039,199	1.25%	100.00%
Phantom debt fraud	296,623	0.12	9.76%
Unpaid taxes fraud	94,962	0.04	3.10
Loan debt scam	51,195 !	0.02 !	1.70 !
Unpaid credit card charges fraud	40,848 !	0.02 !	1.30 !
Medical billing fraud	23,585 !	0.01 !	0.80 !
Unpaid fine fraud	15,487 !	0.01 !	0.50 !
Other phantom debt fraud*	70,545	0.03	2.30

Note: Details may not sum to total because of missing data. See **Table A-25** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

\*Includes other frauds in which the victim paid money to settle a debt but found out the charges did not exist.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

## Prize and Grant Fraud

Of the over 260,000 victims who experienced prize and grant fraud in 2017, about 90,000 (34.2% of prize and grant fraud victims) lost money to a sweepstakes scam (**Table A-4**). Another 79,000 paid money to receive a government loan or grant that turned out to be fraudulent, and about 30,000 lost money in a lottery scam. About 53,000 victims experienced some other form of prize or grant fraud, including Nigerian letter fraud and tax refund scams.

**Table A-4: Prevalence of Prize and Grant Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Percentage	
		Prevalence Rate	Fraud Victims
Total fraud	3,039,199	1.25%	100.00%
Prize and grant fraud	263,690	0.11	8.68%
Sweepstakes scam	90,444	0.04	2.98
Government loan or grant scam	78,857	0.03	2.59
Lottery scam	30,235 !	0.01!	0.99 !
Inheritance scam	/ !	/ !	/ !
Other phantom debt fraud*	53,084!	0.02!	1.70!

Note: Details may not sum to total because of missing data. See **Table A-26** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

/Less than 0.005 or 0.005%.

\*Includes tax refund scam, Nigerian letter fraud, and other frauds in which the victim was promised money or prizes that he or she never received.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

## Relationship and Trust Fraud

Of the 155,000 victims who lost money as victims of relationship and trust fraud, a similar number were scammed by someone pretending to be a family member (about 45,000) or someone pretending to have a romantic interest in the victim (about 50,000) (**Table A-5**). The remaining victims were scammed into believing they had some other connection with or reason to trust the offender.

**Table A-5: Prevalence of Relationship and Trust Fraud, by Nature of the Falsified Relationship and Mode of Contact, 2017**

Type of Fraud	Number	Percentage	
		Prevalence Rate	Fraud Victims
Total fraud	3,039,199	1.25%	100.00%
Relationship and trust fraud	155,188	0.06	5.11%
Type of falsified relationship			
Romantic	49,712	0.02	1.60
Family member	45,444 !	0.02 !	1.50 !
Mode of contact			
Text or phone call	35,164 !	0.01 !	1.20 !
Mutual friend	27,443 !	0.01 !	0.90 !
Social media site	26,351 !	0.01 !	0.90 !
Another website or email	11,466 !	/ !	0.40 !
Dating app/website	11,096 !	/ !	0.40 !
Chat room	/ !	/ !	/ !
Other	40,879 !	0.02 !	1.30 !

Note: Details may not sum to total due to missing data. See **Table A-27** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

/Less than 0.005 or 0.005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

For about 35,000 victims, the offender made the initial contact via text message or phone. About 27,000 were contacted by the offender through a mutual friend; 26,000 were contacted on a social media site; 11,000 were contacted through email; and 11,000 were contacted through a dating app or website.

## Employment Fraud

The survey asked about experiences with three specific types of employment fraud scams (**Table A-6**). About half of victims of employment fraud (77,000) paid money for a business opportunity that turned out to be fraudulent. About one-third (50,000) were victims of a work-at-home scam. Government job placement scams were very rare in 2017.

**Table A-6: Prevalence of Employment Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Percentage	
		Prevalence Rate	Fraud Victims
Total fraud	3,039,199	1.25%	100.00%
Employment fraud	150,462	0.06	4.95
Business opportunities fraud	76,986	0.03	2.50
Work-at-home scam	49,662 !	0.02 !	1.60 !
Government job placement scam	/ !	/ !	/ !

Note: Details may not sum to total because the categories do not reflect an exhaustive list of employment fraud scams. See **Table A-28** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

/Less than 0.005 or 0.005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

## Investment Fraud

The SFS asked about a broad range of different types of investment fraud from penny stock fraud to real estate investment fraud, to alternative energy company investment fraud and foreign currency exchange fraud (**Table A-7**). However, the sample size of investment fraud victims was too small to be able to generate estimates of the different types of fraud experienced. To protect respondent confidentiality, all victims (about 36,000) were consolidated into the “other” category.

**Table A-7: Prevalence of Investment Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Percentage	
		Prevalence Rate	Fraud Victims
Total fraud	3,039,199	1.25%	100.00%
Investment fraud	36,010	0.01 !	1.18 !
Penny stock fraud	/ !	/ !	/ !
Pre-initial public offering company scam	/ !	/ !	/ !
Real estate investment fraud	/ !	/ !	/ !
Oil and gas exploration scam	/ !	/ !	/ !
Alternative energy company scam	/ !	/ !	/ !
Government bond fraud	/ !	/ !	/ !
Foreign currency exchange fraud	/ !	/ !	/ !
Precious metals fraud	/ !	/ !	/ !
Other investment scam*	36,010 !	0.01 !	1.20 !

Note: See **Table A-29** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer cases.

/Less than 0.005 or 0.005%.

\*Includes other scams in which the victim invested money with a person or company, but the investment was fictional or the money was never invested.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

## Other Consequences of Fraud

In addition to financial losses, victims of financial fraud may experience socioemotional harms and difficulties managing financial responsibilities because of the victimization. The majority of victims of prize and grant fraud (61.5%), phantom debt fraud (69.0%), employment fraud (63.3%), investment fraud (75.3%), and relationship and trust fraud (52.9%) experienced moderate to severe distress as a result of the incident (**Table A-8**). About one-third of charity fraud victims thought the incident was not at all distressing. Similarly, 92.6% of charity fraud victims reported that they had no difficulty paying bills because of the incident (**Table A-9**). More than half of victims of phantom debt fraud (51.7%), relationship and trust fraud (67.6%), and product and services fraud (72.3%) also reported no difficulty paying bills because of the money lost through fraud. In contrast, about 35.8% of employment fraud victims and 49.9% of investment fraud victims had some to a lot of difficulty paying bills because of the incident.

**Table A-8: Percentage of Victims Who Experienced Distress and Other Problems as a Result of Fraud, by Type of Fraud, 2017**

Type of Fraud	Total	Distressing				Impact on	
		Not at All	Mildly	Moderately	Severely	Job or School	Family or Friends
Prize and grant	100%	16.10 !	18.20	25.00	36.50	9.00 !	9.90 !
Phantom debt	100%	14.30 !	15.00 !	24.40	44.60	4.10 !	14.50 !
Charity	100%	33.00	38.50	23.50	4.10 !	/ !	5.80 !
Employment	100%	6.10 !	26.60 !	26.50 !	36.80 !	14.40 !	24.50 !
Investment	100%	/ !	24.70 !	41.90 !	33.40 !	29.30 !	16.50 !
Product and services	100%	15.20	37.90	22.50	23.00	3.20	4.50
Relationship and trust	100%	18.30 !	27.00 !	26.20	26.70	5.80 !	13.40 !

Note: See **Table A-30** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer.

/Less than 0.005 or 0.005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-9: Percentage of Victims Who Experienced Difficulty Paying Bills as a Result of Fraud, by Type of Fraud, 2017**

Type of Fraud	Total	Difficulty with Bills			
		None	A little	Some	A lot
Prize and grant	100%	41.30	29.40	14.30 !	10.90 !
Phantom debt	100%	51.70	16.60 !	16.20 !	11.70 !
Charity	100%	92.60	6.60 !	/ !	/ !
Employment	100%	37.00	23.20 !	11.80 !	24.00 !
Investment	100%	36.20 !	13.90 !	16.50 !	33.40 !
Product and services	100%	72.30	16.00	3.70	6.60
Relationship and trust	100%	67.60	14.00 !	3.50 !	13.00 !

Note: See **Table A-30** for standard errors.

! Interpret with caution. Estimate based on sample sizes of 10 or fewer.

/Less than 0.005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Tables A-10** through **A-14** and **A-18** through **A-30** present standard errors for the SFS estimates presented in tables embedded in the report.

**Table A-10: Standard Errors for Table 2-2: Prevalence of Types of Fraud, by Fraud Screening Criteria, 2017**

Type of Fraud	Fraud 1	Fraud 2	Fraud 3	Fraud 4	Fraud 5
Prize and grant	0.02%	0.02%	0.02%	0.02%	0.02%
Phantom debt	0.02	0.02	0.02	0.02	0.02
Charity	0.02	0.02	0.02	0.02	0.02
Employment	0.01	0.01	0.01	0.01	0.01
Investment	0.01	0.01	0.01	0.01	0.01
Product and services	0.05	0.05	0.05	0.03	0.05
Relationship and trust	0.01	0.01	0.01	0.01	0.01

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-11: Standard Errors for Table 2-6: Prevalence of Fraud, by Type of Fraud and Interview Mode, 2017**

Type of Fraud	Prevalence Rate	
	In Person	Telephone
Total fraud	0.10%	0.08%
Prize and grant	0.03	0.02
Phantom debt	0.03	0.03
Charity	0.02	0.03
Employment	0.02	0.02
Investment	0.01	0.00
Product and services	0.07	0.07
Relationship and trust	0.02	0.01

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-12: Standard Errors for Tables 2-8 and 2-9: Prevalence of Types of Fraud, by Fraud Screening Criteria**

Type of Fraud	Fraud 1		Fraud 2		Fraud 3		Fraud 4		Fraud 5	
	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims
Total fraud	170,389	~	157,474	~	152,622	~	136,700	~	140,128	~
Prize and grant	57,472	1.36%	47,870	1.45%	47,870	1.85%	47,870	2.15%	43,644	1.73%
Phantom debt	47,792	1.17	47,792	1.50	47,792	1.90	47,792	2.22	40,996	1.70
Charity	47,037	1.09	47,037	1.38	47,037	1.69	47,037	2.04	42,637	1.68
Employment	36,798	0.91	32,191	1.03	28,241	1.21	26,915	1.40	29,603	1.25
Investment	23,163	0.59	14,219	0.46	14,219	0.61	14,219	0.73	12,404	0.52
Product and services	131,194	2.03	114,939	2.37	98,511	2.60	75,129	2.87	106,934	2.84
Relationship and trust	30,532	0.76	30,532	0.97	30,532	1.26	30,532	1.50	27,684	1.16

~Not applicable.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2017.

**Table A-13: Standard Errors for Table 2-10: Victim Reporting to Law Enforcement and Consumer Organizations, by Type of Fraud, 2017**

Type of Fraud	Any Reporting	
	Number	Percentage of Victims
Total fraud	66,898	1.93%
Prize and grant	16,194	6.24
Phantom debt	27,589	6.99
Charity	16,899	4.32
Employment	12,140	7.50
Product and services	45,912	2.13
Relationship and trust	16,145	9.18

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2017.

**Table A-14: Standard Errors for Tables 2-11 and 2-12: Victim Reporting to Law Enforcement and Consumer Organizations, by Type of Fraud, 2017**

Type of Fraud	Federal Trade Commission		Better Business Bureau		Consumer Financial Protection Bureau		State Attorneys General Offices		Internet Crime Complaint Center		Law Enforcement Agencies	
	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims	Number	Percentage of Victims
Total fraud	27,024	0.85%	36,502	1.12%	30,974	0.96%	30,783	0.97%	21,283	0.70%	54,931	1.68%
Prize and grant	4,886	1.86	3,928	1.51	2,765	1.05	10,350	3.93	~	~	14,723	5.70
Phantom debt	15,493	4.94	15,515	4.78	13,698	4.31	12,950	3.97	~	~	25,343	6.70
Charity	7,231	2.05	10,220	2.76	10,304	2.81	5,461	1.56	~	~	12,255	3.29
Employment	~	~	1,717	1.15	10,518	6.65	10,745	6.76	5,219	3.43	10,826	6.78
Product and services	20,926	1.03	29,858	1.43	19,878	0.01	21,377	1.08	20,486	1.04	33,693	1.62
Relationship and trust	5,989	3.79	5,461	3.46	5,821	3.69	7,616	4.82	2,458	1.59	16,145	9.18

~ Not applicable.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2017.

**Table A-15: NIBRS Fraud Offense Definitions**

<b>Fraud Offenses (Except Counterfeiting Forgery and Bad Checks)</b>	The intentional perversion of the truth for the purpose of inducing another person, or other entity, in reliance upon it to part with something of value or to surrender a legal right.
<b>False Pretenses/ Swindle/Confidence Game</b>	The intentional misrepresentation of existing fact or condition, or the use of some other deceptive scheme or device, to obtain money, goods, or other things of value.
<b>Credit Card/Automated Teller Machine Fraud</b>	The unlawful use of a credit (or debit) card or automated teller machine for fraudulent purposes.
<b>Impersonation</b>	Falsely representing one's identity or position, and acting in the character or position thus unlawfully assumed, to deceive others and thereby gain a profit or advantage, enjoy some right or privilege, or subject another person or entity to an expense, charge, or liability which would not have otherwise been incurred.
<b>Welfare Fraud</b>	The use of deceitful statements, practices, or devices to unlawfully obtain welfare benefits.
<b>Wire Fraud</b>	The use of an electric or electronic communications facility to intentionally transmit a false and/or deceptive message in furtherance of a fraudulent activity.
<b>Identity theft</b>	Wrongfully obtaining and using another person's personal data (e.g., name, date of birth, Social Security number, driver's license number, credit card number).
<b>Hacking/Computer Invasion</b>	<b>Wrongfully gaining access to another person's or institution's computer software, hardware, or networks without authorized permissions or security clearances.</b>

Source: Federal Bureau of Investigation, National Incident-Based Reporting System, 2013–2017.

**Table A-16: Trends in NIBRS Fraud Incidents and Victims, 2013–2017**

Fraud Offenses	Incidents					Offenses					Victims				
	2013	2014	2015	2016	2017	2013	2014	2015	2016	2017	2013	2014	2015	2016	2017
Total fraud	271,969	300,577	342,023	364,892	374,409	285,636	315,820	356,490	346,664	374,409	301,432	333,358	382,440	402,974	411,355
Subtypes															
False Pretenses/Swindle/ Confidence Game	112,474	122,514	128,155	140,680	N/A	116,254	126,626	132,037	140,680	N/A	121,134	131,757	138,248	150,878	N/A
Credit Card/ Automated Teller Machine Fraud	88,048	89,317	96,021	109,466	N/A	89,859	91,218	98,019	109,466	N/A	101,638	103,317	108,636	124,970	N/A
Impersonation	71,010	88,470	116,058	86,521	N/A	72,027	89,597	117,099	86,521	N/A	76,637	96,673	131,872	94,979	N/A
Welfare Fraud	1,089	1,177	938	900	N/A	1,256	1,386	1,133	900	N/A	1,142	1,239	1,012	957	N/A
Wire Fraud	6,177	6,945	8,144	9,097	N/A	6,240	6,993	8,202	9,097	N/A	6,680	7,692	8,840	9,617	N/A
Identity theft	N/A	N/A	689	28,807	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	841	30,860	N/A
Hacking/Computer Invasion	N/A	N/A	15	604	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	15	658	N/A
Total agencies*	6,119	6,251	6,278	6,570		6,119	6,251	6,278	6,570		6,119	6,251	6,278	6,570	

Notes: Subtype counts are not shown because the data were not available from the FBI at the time of analysis. N/A = Not available.

\*Includes all agencies with at least one crime incident report (of any type, not limited to fraud) in the NIBRS extract files.

Source: Federal Bureau of Investigation, National Incident-Based Reporting System, 2013–2017.

**Table A-17: Full Scope of Fraud Offenses Included in NIBRS, by Victim Characteristics, 2016**

	Total Victims of Fraud	2016 NIBRS Fraud—Out of Scope for SFS					2016 NIBRS Fraud—In Scope for SFS			
		Hacking/Computer Invasion	Credit Card/Automated Teller Machine Fraud	Impersonation	Identity Theft	Welfare Fraud	False Pretenses/Swindle/Confidence Game	Wire Fraud	Total in Scope Count	Percent-age*
Victims	402,974	658	124,970	94,979	30,860	957	150,878	9,617	160,495	
<b>Sex</b>										
Unknown	3,119	1	830	1,071	261	27	990	42	1,032	1.0
Male	145,124	224	42,531	43,715	14,256	153	44,577	3,733	48,310	47.2
Female	164,514	287	56,958	43,237	15,490	232	48,557	4,571	53,128	51.9
<b>Race</b>										
Unknown	23,614	51	7,374	7,126	2,231	62	6,910	547	7,457	7.3
White	240,201	414	78,877	69,342	22,218	281	69,865	6,480	76,345	74.5
Black	41,665	29	12,102	9,587	4,628	66	14,973	1,067	16,040	15.7
American Indian/Alaska Native	6,160	2	271	358	87	2	326	40	366	0.4
Asian/Pacific Islander	1,117	16	1,695	1,610	843	1	2,050	212	2,262	2.2
Asian	1,056	16	1,682	1,594	823	1	2,037	210	2,247	2.2
Native Hawaiian or Other Pacific Islander	61	N/A	13	16	20	N/A	13	2	15	0.0
<b>Age</b>										
Unknown	5,553	10	1,355	1,903	274	21	2,053	107	2,160	2.1
Juvenile	3,494	25	940	1,055	322	10	1,143	101	1,244	1.2
18–34 Years	86,288	137	30,545	22,622	7,610	138	25,297	2,187	27,484	26.8
35–49 Years	84,159	130	27,479	25,428	8,976	95	22,616	1,931	24,547	24.0
50–64 Years	81,488	121	25,250	24,430	8,768	87	23,056	2,075	25,131	24.5
65+ Years	51,810	89	14,750	12,585	4,057	61	19,959	1,945	21,904	21.4
<b>Type of Victim</b>										
Unknown	1,973	1	283	1,201	46	3	421	37	458	0.3
Individual	312,757	512	100,319	88,008	30,007	412	94,104	8,346	102,450	63.8
Business	69,561	116	18,755	3,323	646	86	46,371	998	47,369	29.5
Financial Institution	8,940	6	5,168	388	93	4	3,276	160	3,436	2.1
Government	8,449	11	257	1,846	32	447	5,874	46	5,920	63.8
Law Enforcement	35	N/A	N/A	N/A	N/A	N/A	20	N/A	20	0.0
Religious Organization	194	3	57	20	5	N/A	101	12	113	0.1
Other	1,065	9	131	178	31	5	711	18	729	0.5

Notes. N/A = Not available. \*Percentages for sex, race, and age are based on total number of **individual** victims. Percentages by type of victim are based on the total number of victims.

Source: Federal Bureau of Investigation, National Incident-Based Reporting System, 2016.

**Table A-18: Standard Errors for Table 2-13: Demographic Characteristics of NIBRS and SFS Victims**

Characteristic	SFS Fraud			
	Reported to Police		Not Reported to Police	
	Number	Percentage	Number	Percentage
Total Individual victims	426,165	100.0%	2,613,034	100.0%
Sex				
Male	30,335	5.6	98,553	2.4
Female	43,836	5.6	91,852	2.4
Unknown	~	~	~	~
Race				
White	50,070	4.7	114,446	2.6
Black	16,877	3.6	74,502	2.5
American Indian/Alaska Native	10,518	2.4	9,825	0.4
Asian/Pacific Islander	11,836	2.8	25,140	0.9
Asian	~	~	~	~
Native Hawaiian/Other Pacific Islander	~	~	~	~
Two or more races	3,765	0.9	21,408	0.8
Unknown	~	~	~	~
Age				
Juvenile	~	~	~	~
18–34 Years	25,403	5.0	86,298	2.3
35–49 Years	23,799	5.0	60,183	2.0
50–64 Years	31,625	5.6	67,131	2.1
65+ Years	24,228	5.2	51,270	1.9
Unknown	~	~	~	~

~ Not applicable.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2017.

**Table A-19: Standard Errors for Table 2-14: Percentage of Victims Who Believed What They Experienced Was Fraud, 2017**

Type of Fraud	Percentage	Type of Fraud	Percentage
Prize and grant fraud	6.22%	Product and services	2.76%
Lottery scam	8.58	Product type	
Sweepstakes scam	10.38	Weight loss or health supplements	7.98
Inheritance scam	/	Clothing or accessories	5.91
Government loan or grant scam	4.68	Collectibles or memorabilia	15.65
Other prize and grant fraud	10.89	Electronics or software	6.22
Phantom debt fraud	6.53	Auto parts	7.79
Unpaid taxes fraud	12.37	Other products	4.68
Loan debt scam	0.00	Service type	
Unpaid fine fraud	13.01	Insurance	/
Unpaid credit card charges fraud	18.78	Computer repair services	6.51
Medical billing fraud	21.84	Home or auto repairs	10.67
Other phantom debt fraud	6.98	Internet or phone services	10.43
Charity fraud	5.49	Online gaming services	18.87
Bogus charitable organization scam	5.75	Identity theft protection services	28.67
Crowdfunding under false pretenses	10.56	Credit repair services	0.00
Employment fraud	8.39	Vacation rental services	11.94
Business opportunities fraud	13.56	Business growth services	24.68
Work-at-home scam	14.71	Adoption services	/
Government job placement scam	/	Other services	10.21
Investment fraud	16.84	Relationship and Trust	8.12
		Romantic	16.47
		Family member	14.36

/ Less than 0.005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-20: Standard Errors for Table 2-15: Average Out-of-Pocket Financial Losses Experienced by Victims of Fraud, by Type of Fraud, 2017**

Financial Losses	Types of Fraud						
	Prize or Grant	Phantom Debt	Charity	Employment	Investment	Product and Services	Relationship and Trust
Mean	\$40	11	4	6	~	210	514
Total sum	\$6,872,634	1,105,319	1,086,219	5,889,461	~	418,067,888	88,014,589

~ Not applicable. Based on a single case.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2017.

**Table A-21: Standard Error for Table 2-16: Percentage of Fraud Victims Experiencing Out-of-Pocket Financial Losses, by Type of Fraud, 2017**

Financial Losses	Types of Fraud						
	Prize or Grant	Phantom Debt	Charity	Employment	Investment	Product and Services	Relationship and Trust
Less than \$100	7.8%	3.8%	5.4%	7.7%	16.8%	3.1%	10.3%
\$100–\$499	6.6	6.2	4.5	10.6	~	3.0	3.7
\$500–\$999	4.0	6.0	2.7	8.0	~	1.9	7.4
\$1,000 or more	4.2	7.2	~	9.7	19.0	1.9	8.6
Unknown	4.7	2.5	0.6	4.0	13.0	0.5	4.8
Got any money back	0.8	3.5	2.9	~	~	1.5	5.9

~ Not applicable.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2017.

**Table A-22: Standard Errors for Table 2-17: Demographic Characteristics of Fraud Victims, 2017**

Characteristics	Percent							
	Fraud 1		Fraud 2		Fraud 4		Fraud 5	
	Experiencing Fraud	Fraud Victims	Experiencing Fraud	Fraud Victims	Experiencing Fraud	Fraud Victims	Experiencing Fraud	Fraud Victims
Total	0.07%	~	0.06%	~	0.05%	~	0.06%	~
Sex								
Male	0.10	1.94%	0.09	2.27%	0.07	2.84%	0.08	2.76%
Female	0.09	1.94	0.08	2.27	0.07	2.84	0.07	2.76
Race/Hispanic origin								
White	0.08	2.05	0.07	2.40	0.06	3.09	0.06	2.86
Black	0.27	1.84	0.26	2.18	0.20	2.67	0.23	2.52
Hispanic	0.17	1.66	0.16	1.97	0.13	2.37	0.14	2.25
Other	0.27	1.07	0.20	0.98	0.56	1.88	0.66	1.77
Age								
18–19	0.46	0.99	0.30	0.84	0.25	1.12	0.29	1.07
20–24	0.27	1.39	0.26	1.68	0.20	2.08	0.22	1.88
25–34	0.18	1.70	0.17	2.10	0.14	2.74	0.17	2.55
35–49	0.11	1.42	0.10	1.76	0.09	2.22	0.09	2.05
50–64	0.13	1.81	0.12	2.03	0.09	2.80	0.09	2.25
65+	0.13	1.61	0.11	1.75	0.09	2.19	0.09	1.88
Household income								
Less than \$25,000	0.17	1.75	0.17	2.17	0.15	2.90	0.16	2.54
\$25,000–\$49,999	0.14	2.02	0.12	2.23	0.10	2.75	0.11	2.60
\$50,000–\$74,999	0.13	1.48	0.12	1.72	0.09	2.18	0.11	2.05
\$75,000–\$99,999	0.16	1.50	0.14	1.64	0.12	2.15	0.12	1.81
\$100,000–\$149,999	0.22	1.39	0.18	1.52	0.15	1.83	0.17	1.84
\$150,000+	0.22	1.26	0.20	1.48	0.18	2.11	0.14	1.44

~ Not applicable.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2017.

**Table A-23: Standard Errors for Table A-1: Prevalence of Product and Services Fraud, by Type of Product or Service Purchased, 2017**

Type of Fraud	Number	Prevalence Rate	Percentage of Fraud Victims
Product and services fraud	114,939	0.05%	2.37%
Type of product purchased			
Clothing or accessories	47,308	0.02	1.52
Electronics or software	36,032	0.01	1.14
Weight loss or health supplements	28,428	0.01	0.95
Auto parts	20,844	0.01	0.67
Collectibles or memorabilia	21,373	0.01	0.70
Other products	63,382	0.03	1.96
Type of service purchased			
Home or auto repairs	26,751	0.01	0.86
Computer repair services	20,606	0.01	0.68
Vacation rental services	28,004	0.01	0.91
Internet or phone services	10,562	0.00	0.35
Business growth services	13,223	0.01	0.43
Online gaming services	9,925	0.00	0.32
Identity theft protection services	9,137	0.00	0.30
Credit report repair services	11,852	0.00	0.39
Insurance	9,338	0.00	0.31
Adoption services	/	/	/
Other services	36,121	0.01	1.12

/Less than 0.0005.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-24: Standard Errors for Table A-2: Prevalence of Charity Fraud, by Type of Fraud Scheme, 2017**

Type of fraud	Number	Prevalence Rate	Percent of Fraud Victims
Charity fraud	47,037	0.02%	1.4%
Bogus charitable organization scam	41,318	0.02	1.2
Crowdfunding under false pretenses	18,507	0.01	0.1

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-25: Standard Errors for Table A-3: Prevalence of Phantom Debt Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Prevalence Rate	Percentage of Fraud Victims
Phantom debt fraud	47,792	0.02%	1.50%
Unpaid taxes fraud	24,100	0.01	0.76
Loan debt scam	19,049	0.01	0.62
Unpaid credit card charges fraud	16,139	0.01	0.53
Medical billing fraud	12,533	0.01	0.41
Unpaid fine fraud	8,296	0.00	0.27
Other phantom debt fraud	22,685	0.01	0.74

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-26: Standard Errors for Table A-4: Prevalence of Prize and Grant Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Prevalence Rate	Percentage of Fraud Victims
Prize and grant fraud	47,870	0.02%	1.45%
Sweepstakes scam	22,389	0.01	0.73
Government loan or grant scam	19,752	0.01	0.64
Lottery scam	11,590	0.00	0.37
Inheritance scam	/	/	/
Other prize and grant fraud	30,704	0.01	0.99

/Less than 0.0005 or 0.0005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-27: Standard Errors for Table A-5: Prevalence of Relationship and Trust Fraud, by Nature of the Falsified Relationship and Mode of Contact, 2017**

Type of Fraud	Number	Prevalence Rate	Percentage of Fraud Victims
Relationship and trust fraud	30,532	0.01%	0.97%
Type of falsified relationship			
Romantic	16,603	0.01	0.55
Family member	16,392	0.01	0.53
Mode of contact			
Text or phone call	12,300	0.01	0.40
Mutual friend	17,062	0.01	0.56
Social media site	12,417	0.01	0.41
Another website or email	7,865	0.00	0.26
Dating app/website	5,588	0.00	0.18
Chat room	/	/	/
Other	15,956	0.01	0.51

/Less than 0.0005 or 0.0005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-28: Standard Errors for Table A-6: Prevalence of Employment Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Prevalence Rate	Percentage of Fraud Victims
Employment fraud	32,191	0.01%	1.03%
Business opportunities fraud	23,236	0.01	0.77
Work-at-home scam	18,941	0.01	0.63
Government job placement scam	/	/	/

/Less than 0.0005 or 0.0005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-29: Standard Errors for Table A-7: Prevalence of Investment Fraud, by Type of Fraud Scheme, 2017**

Type of Fraud	Number	Prevalence Rate	Percentage of Fraud Victims
Investment fraud	14,219	0.01%	0.46%
Penny stock fraud	/	/	/
Pre-initial public offering company scam	/	/	/
Real estate investment fraud	/	/	/
Oil and gas exploration scam	/	/	/
Alternative energy company scam	/	/	/
Government bond fraud	/	/	/
Foreign currency exchange fraud	/	/	/
Precious metals fraud	/	/	/
Other investment scam	14,219	0.01	0.46

/Less than 0.0005 or 0.0005%.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

**Table A-30: Standard Errors for Table A-8 and Table A-9: Percentage of Victims Who Experienced Distress and Other Problems as a Result of Fraud, by Type of Fraud, 2017**

Type of Fraud	Distressing				Impact On		Difficulty with Bills			
	Not at All	Mildly	Moderately	Severely	Job or School	Family or Friends	None	A little	Some	A lot
Prize and grant	9.48%	6.28%	6.66%	7.31%	4.86%	4.33%	7.82%	6.74%	4.94%	5.13%
Phantom debt	4.91	5.51	5.96	6.96	2.43	5.43	7.42	5.86	5.44	5.17
Charity	6.29	6.79	5.58	2.10	/	2.82	3.81	3.77	/	/
Employment	5.82	9.85	9.03	10.57	7.98	9.73	10.33	9.60	6.51	9.39
Investment	/	16.84	19.26	19.21	17.75	15.01	18.54	13.03	15.01	19.21
Product and services	2.05	2.88	2.33	2.28	1.09	1.05	2.67	2.27	0.99	1.41
Relationship and trust	7.27	10.22	8.28	8.13	5.60	6.25	9.23	6.80	3.53	6.58

/Less than 0.0005.

Source: Bureau of Justice Statistics, Supplemental Fraud Survey, 2017.

## Appendix B

### Summary of Existing Fraud Surveys/ Data Collections Examined and Summarized

<b>Name</b>	<b>Sponsor</b>
Better Business Bureau ScamTracker Risk Report (2017)	Better Business Bureau
Consumer Sentinel	Federal Trade Commission
Federal Trade Commission—Consumer Fraud in U.S. Survey (2011)	Federal Trade Commission
Internet Crime Complaint Center (IC3)	Federal Bureau of Investigation
AARP Fraud Watch Network Survey	AARP
Financial Fraud and Fraud Susceptibility in the United States: Research Report from a 2012 National Survey	FINRA Foundation
National Public Survey on White Collar Crime (2010)	National White Collar Crime Center
Crime Survey of England and Wales	Office for National Statistics (U.K.)
AARP Investment Fraud Vulnerability Study	AARP
Consumer Financial Exploitation of the Elderly in Arizona and Florida, 2010-2011	Holtfreter and colleagues
Fraud.org Top Scams of 2018	National Consumers League
Ipsos Public Affairs / Microsoft Tech Support Scam Survey	IPSOS Public Affairs
2019 Identity Fraud Study	Javelin Research
National Incident-Based Reporting System (NIBRS)	Federal Bureau of Investigation

## Better Business Bureau ScamTracker Risk Report (2017)

Source Location: <http://bbbfoundation.images.worldnow.com/library/a3949f5c-93cc-4e31-803b-bb77bf2e2c86.pdf>

### Background

The BBB ScamTracker Report (2017) was published by the Better Business Bureau Institute for Marketplace Trust (BBB Institute)—the education and research arm of the BBB. The 2017 report is the second annual report of its kind. The BBB developed ScamTracker in 2015 to address needs identified by local BBBs: to allow consumers to report scams in real time.

### Methodology

Data are collected from consumers who reported scams proactively to the ScamTracker, which collects the following information:

- About the scammer
  - Scammer contact information (e.g., business name used, address used, phone number, email address used)
- About the scam
  - Initial means of contact with the scammer (email, fax, in person, internet messaging [e.g., WhatsApp], online classifieds [e.g., Craigslist], phone, postal mail, social media [e.g., Facebook], text message, website, other, not applicable)
  - Type of scam:

• Advance Fee Loan	• Investment
• Business Email Compromise	• Moving
• Charity	• Nigerian/Foreign Money Exchange
• Counterfeit Product	• Online Purchase
• Credit Cards	• Phishing
• Credit Repair/Debt Relief	• Rental
• Cryptocurrency	• Romance
• Debt Collections	• Scholarship
• Employment	• Sweepstakes/Lottery/Prizes
• Fake Check/Money Order	• Tax Collection
• Fake Invoice	• Tech Support
• Family/Friend Emergency	• Travel/Vacations
• Government Grant	• Utility
• Health Care/Medicaid/Medicare	• Yellow Pages/Directories
• Home Improvement	• Other
• Identity Theft	

- The story
- Screenshots, documents, etc.
- Whether the victim lost money
- Whether the scam targeted an individual or a business
- About the person scammed
  - Demographics (e.g., age, gender, military status, student status, location)
- About the person reporting
  - Whether the person reporting is the victim or not
  - Contact information for the reporting party

Approximately 47,000 scam reports were submitted in 2017; of those, approximately 31,000 fell into categories measured in the SFS (i.e., fraud against business and ID theft are excluded).

### Fraud Covered

ScamTracker collects information on the following types of fraud, categorized into the fraud taxonomy. BBB's definitions are included below.

- Prize and grant fraud
  - **Fake Check/Money Order Scams.** In this con, the victim deposits a phony check and then returns a portion by wire transfer to the scammer. The stories vary, but the victim is often told they are refunding an “accidental” overpayment. Scammers count on the fact that banks make funds available within days of a deposit but can take weeks to detect a fake check.
  - **Foreign Money Exchange Scams.** In this scam, the target receives an email from a government official, a member of royalty, or a business owner offering a huge sum for help getting money out of their country. The victim fronts the costs for the transfer, believing that they will be repaid.
  - **Government Grant Scams.** In this con, individuals are enticed by promises of free, guaranteed government grants. The only catch is a “processing fee.” Other fees follow, but the promised grant never materializes.
  - **Scholarship Scams.** This con hooks victims—often students struggling with tuition costs—with the promise of government scholarship money, but the up-front “fees” never produce those much-needed funds. Sometimes a fake check does arrive, and the student is asked to wire back a portion for taxes or other charges.
  - **Sweepstakes, Lottery and Prize Scams.** This con tricks/deceives victims into thinking they have won a prize or lottery jackpot but need to pay up-front fees to receive the winnings, which never materialize. Sometimes this con involves a fake check and a request to return a portion of the funds to cover fees.

- Phantom debt fraud
  - **Debt Collection Scams.** In this con, phony debt collectors harass their targets, trying to get them to pay debts they do not owe.
  - **Tax Collection Scams.** In this con, imposters pose as Internal Revenue Service representatives in the United States or Canada Revenue Agency representatives in Canada to coerce the target into either paying up or sharing personal information.
  - **Utility Scams.** In this con, scammers impersonate water, electric and gas company representatives to take money or personal information. They frequently threaten residents and business owners with deactivation of service unless they pay immediately. In another form, a “representative” may come to the door to perform “repairs” or an “energy audit” with the intent of stealing valuables.
- Charity fraud
  - **Charity Scams.** Charity scams use deception to get money from individuals believing they are making donations to legitimate charities. This is particularly common in the wake of a natural disaster or other tragedy.
- Employment fraud
  - **Employment Scams.** Victims of employment scams are led to believe they are applying or have just been hired for a promising new career while they have, in fact, given personal information or money to scammers for “training” or “equipment.” In another variation, the victim may be “overpaid” with a fake check and asked to wire back the difference.
- Investment fraud
  - **Investment Scams.** These scams take many forms, but all prey on the desire to make money without much risk or initial funding. “Investors” are lured with false information and promises of large returns with little or no risk.
- Products and services fraud
  - **Advance Fee Loan Scams.** In this scam, a loan is guaranteed, but once the victim pays up-front charges such as taxes or a “processing fee,” the loan never materializes.
  - **Counterfeit Product Scams.** Counterfeit goods mimic original merchandise, right down to the trademarked logo, but are typically of inferior quality. This can result in a life-threatening health or safety hazard when the counterfeit item is medication or an auto part.
  - **Credit Card Scams.** This con typically involves impersonation of a bank or other credit card issuer. By verifying account information, con artists try to fool their targets into sharing credit card or banking information.
  - **Credit Repair/Debt Relief Scams.** Scammers posing as legitimate service providers collect payment in advance with promises of debt relief and repaired credit but provide little or nothing in return.
  - **Home Improvement Scams.** In this con, door-to-door solicitors offer quick, low-cost repairs and then either take payments without returning, do shoddy work or “find” issues that dramatically raise the price.

- **Moving Scams.** These schemes involve rogue moving services offering discounted pricing to move household items. They may steal the items or hold them hostage, demanding additional funds to deliver them to the new location.
- **Online Purchase Scams.** These cons often involve purchases and sales, often on eBay, Craigslist, Kijiji, or other direct seller-to-buyer sites. Scammers may pretend to purchase an item only to send a bogus check and ask for a refund of the “accidental” overpayment. In other cases, the scammer will simply never deliver the goods.
- **Rental Scams.** Phony ads are placed for rental properties that ask for up-front payments. Victims later discover the property does not exist or is owned by someone else.
- **Tech Support Scams.** Tech support scams start with a call or pop-up warning that alerts the target to a computer bug or other problem. Scammers pose as tech support employees of well-known computer companies and hassle victims into paying for “support.” If the victim allows remote access, malware may be installed.
- **Travel and Vacation Scams.** Con artists post listings for properties that either are not for rent, do not exist or are significantly different than pictured. In another variation, scammers claim to specialize in timeshare resales and promise they have buyers ready to purchase.
- Relationship and trust fraud
  - **Family/Friend Emergency Scams.** This scheme involves the impersonation of a friend or family member in a fabricated urgent or dire situation. The “loved one” invariably pleads for money to be sent immediately. Aided by personal details they have found on social media; imposters can offer very plausible stories to convince their targets.
  - **Romance Scams.** An individual believing they are in a romantic relationship is tricked into sending money, personal and financial information, or items of value to the perpetrator.
- Other.
  - This category is not defined, it is a catchall category.
- Identity theft
  - **Health Care, Medicaid, and Medicare Scams.** These schemes run the gamut, with many attempting to defraud private or government health care programs. The con artist is often after the insured’s health insurance, Medicaid, or Medicare information to submit fraudulent medical charges or for purposes of identity theft.
  - **Identity Theft Scams.** Identity thieves use personal information (e.g., Social Security Number, bank account information, and credit card numbers) to pose as another individual for their own gain. This may include opening a credit account, draining an existing account, filing tax returns, or obtaining medical coverage.
  - **Phishing Scams.** These schemes employ communication impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the recipient into providing personal information or passwords.

- Fraud against an organization
  - **Business Email Compromise Scams.** This financial fraud targets businesses engaged in international commerce. Scammers gain access to company email and trick employees into sending money to a “supplier” or “business partner” overseas.
  - **Fake Invoice Scams.** This scam targets businesses. Scammers attempt to fool employees into paying for products that the business did not order and that may not even exist. Fake invoices are often for office supplies, website or domain hosting services, and directory listings.
  - **Yellow Pages/Directory Scams.** This con targets businesses, attempting to fool them into paying for a listing or ad space in a nonexistent directory or “Yellow Pages.” In some cases, the directory will technically exist, but will not be widely distributed and a listing will be of little or no value—these directories are essentially props in the scammer’s ploy.

### Key Estimates

47,827 reports were made in 2017, resulting in a median loss of \$288 per report (total loss not available). Of the total reports received, 30,076 were not identity theft or fraud against a business.

BBB created a scam risk index for each type of fraud

---


$$\text{Exposure} * \text{Susceptibility} * \text{Monetary Loss} = \text{BBB Scam Risk Index}$$


---

where:

- Exposure is a measure of the prevalence of a scam type, calculated as the percentage of all scams reported, represented by that scam type. This calculation includes scam reports by those who suffered monetary losses and by those who were exposed to scams but avoided losses;
- Susceptibility is a measure of the likelihood of losing money when exposed to a scam type, calculated as the percentage of all reports of the scam type that involved a monetary loss; and
- Monetary Loss is calculated as the median dollar amount of losses reported for a particular scam type, excluding reports where no loss occurred.

Scam Types	No. of Reports	Percentage		Median \$ Loss	Risk Index
		Exposure	Susceptibility		
<b>Prize and grant fraud</b>	<b>6,041</b>				
Fake Check/Money Order	1,097	2.3	14.2	1,488	21.3
Foreign Money Exchange	128	0.3	18.8	965	2.1
Government Grant	1,981	4.1	10.3	500	9.4
Scholarship	15	0.03	13.3	1,594	0.3
Sweepstakes, Lottery and Prize	2,820	5.9	6.4	500	8.2
<b>Phantom debt fraud</b>	<b>5,894</b>				
Debt Collection	2,304	4.8	7.2	404	6.1
Tax Collection	3,090	6.5	1.2	999	3.3
Utility	500	1.0	9.6	500	2.2

Scam Types	No. of Reports	Percentage		Median \$ Loss	Risk Index
		Exposure	Susceptibility		
<b>Charity fraud</b>	<b>419</b>				
Charity	419	0.9	11.0	105	0.4
<b>Employment fraud</b>	<b>2,429</b>				
Employment	2,429	5.1	13.8	800	24.6
<b>Investment fraud</b>	<b>238</b>				
Investment	238	0.5	50.8	2,310	25.6
<b>Products and services fraud</b>	<b>13,988</b>				
Advance Fee Loan	1,061	2.2	38.9	600	22.7
Counterfeit Product	886	1.9	46.5	150	5.7
Credit Card Scams	1,244	2.6	14.1	150	2.4
Credit Repair/Debt Relief	572	1.2	17.3	599	5.4
Home Improvement	374	0.8	44.9	1,225	18.9
Moving	64	0.1	53.1	486	1.5
Online Purchase	4,655	9.7	72.5	100	30.9
Rental	295	0.6	34.2	570	5.3
Tech Support	2,277	4.8	26.4	300	16.5
Travel and Vacation	2,560	5.4	3.7	1,184	10.2
<b>Relationship and trust fraud</b>	<b>485</b>				
Family/Friend Emergency	341	0.7	10.3	3,000	9.6
Romance	144	0.3	45.1	1,500	8.9
<b>Other</b>	<b>1,826</b>				
Other	1,826	3.8	15.5	550	14.3
<b>Uncategorized</b>	<b>500</b>				

## Consumer Sentinel

Source Location: <https://www.ftc.gov/site-information/open-government/data-sets#csn>

### Background

Hosted by the Federal Trade Commission, Consumer Sentinel is a repository for consumer reports of complaints for a wide variety of fraud. Consumer Sentinel is based on the premise that sharing information can make law enforcement more effective. To that end, the Consumer Sentinel Network provides law enforcement members with access to complaints provided directly to the Federal Trade Commission by consumers and provides members with access to complaints shared by Data Contributors.<sup>24</sup>

<sup>24</sup> Consumer Sentinel Data Contributors include the following: AARP Fraud Watch Network, Alaska Attorney General, Canada Competition Bureau, Colorado Attorney General, Consumer Financial Protection Bureau, Green Dot Corporation, Hawaii Office of Consumer Protection, Homeowners Preservation Foundation, Idaho Attorney General, Indiana Attorney General, International Association of Better Business Bureaus, Iowa Attorney General, Los Angeles County Department of Consumer and Business Affairs, Louisiana Attorney General, Maine Attorney General, Massachusetts Attorney General, Michigan Attorney General, Microsoft Corporation Cyber Crime Center, Mississippi Attorney General, MoneyGram International, Montana Department of Justice, National Consumers League, Nebraska Attorney General, Nevada Attorney General, Nevada Department of Business and Industry, New York State Attorney General, North Carolina Department of Justice, Ohio Attorney General, Oregon Department of Justice, Pennsylvania Attorney General, PrivacyStar, Publishers Clearing House, South Carolina Department of Consumer Affairs, Tennessee Division of Consumer Affairs, U.S. Department of Defense, U.S. Department of Education, U.S. Department of Veterans Affairs, U.S. Postal Inspection Service, Utilities United Against Scams, Washington State Attorney General, Western Union Company, Wisconsin Department of Agriculture, Trade and

It provides law enforcement (who have been approved as members of the Consumer Sentinel Network) with access to millions of consumer complaints. Complaint types include identity theft; do-not-call registry violations; computers, the internet, and online auctions; telemarketing scams; advance fee loans and credit scams; immigration services; sweepstakes, lotteries, and prizes; business opportunities and work-at-home schemes; health and weight loss products; debt collection, credit reports, and financial matters.

## Methodology

Complaints of fraud are input from consumers via forms available online. Data contributors may also share fraud complaints. Complaints need not be substantiated, include incidents of both actual and suspected fraud, and are not limited to actual loss. Reports can include juveniles and adults as well as businesses or individuals.

## Fraud Covered

Consumer Sentinel covers a variety of fraud that consumers feel the need to report, including many items (such as identity theft) that are beyond the scope of SFS. The items that align with SFS include the following:

- **Advance Payments for Credit Services:** The promise of a loan or credit card that requires you to pay a fee first; worthless credit card loss protection and insurance programs; the promise that accurate negative information can be removed from your credit file for a fee; services offering to recover government refunds or unclaimed funds; etc.
- **Books and Magazines:** Pitches for "free," "pre-paid," or "special" magazine or book subscription deals; etc.
- **Business and Job Opportunities:** Franchise or business opportunities (e.g., offers to start a new business); work-at-home plans, (e.g., stuffing envelopes or processing medical claims); multi-level marketing schemes, employment agencies or job counseling, overseas work, inventions, or idea promotions.
- **Charitable Solicitations:** Misleading pitches for donations to benefit a charity; solicitations for bogus charity or relief organizations; etc.
- **Foreign Money Offers and Counterfeit Check Scams:** Letters or emails promising a percentage of millions of dollars that from a foreign country in return for money, bank account numbers or other identifying information from the victim; fraudulent schemes involving foreign lotteries, mystery shoppers or internet purchases\classified ads in which someone is overpaid with a counterfeit check and asked to wire back the difference immediately after check deposit, leaving the victim responsible for the funds

---

Consumer Protection, Xerox Corporation. In addition, the following entities refer complaints to the FTC: Ayuda, Catholic Charities USA, Connecticut Department of Consumer Affairs, Iowa, Clinton County Sheriff's Office Ohio, Cuyahoga County Department of Consumer Affairs, PeopleClaim, Petscams.com, Scam Detector, U.S. Customs and Border Protection, U.S. Department of Health and Human Services, Office of Inspector General, U.S. Department of Justice, Disaster Fraud Task Force, U.S. Department of Justice, Executive Office for Immigration Review, U.S. Department of Justice, Task Force on Market Integrity and Consumer Fraud, U.S. Department of the Treasury, Internal Revenue Service, & U.S. Senate Special Committee on Aging.

withdrawn; etc.

- **Grants:** Businesses or individuals marketing either government grant opportunities or financial aid assistance services; problems with student loan processors, debt collectors collecting on defaulted student loans, diploma mills and other unaccredited educational institutions; etc.
- **Health Care:** Fraudulent, misleading or deceptive claims for vision correction procedures; dietary supplements; weight loss products or services; impotency treatments; health spas and equipment; infertility services; sunscreens; HIV test kits; medical discount plans; as well as complaints about over-the-counter or prescription drugs; other medical products, supplies or treatments; fitness monitors and devices that can connect to the internet and use a processor or sensors to collect consumer information; etc.
- **Imposter Scams:** Someone pretends to be a trusted person to get consumers to send money or give personal information. Examples include scammers claiming to work for or be affiliated with a government agency; scammers posing as a friend or relative with an emergency need for money; scammers posing as a romantic interest; scammers claiming to be a computer technician offering technical support; and scammers claiming to be affiliated with a private entity (e.g., a charity or company).
- **Internet Auction:** Nondelivery or late delivery of goods; delivery of goods that are less valuable than advertised; failure to disclose all the relevant information about the product or terms of the sale; etc.
- **Internet Services:** Problems with websites that offer content for a fee or advertise products and services; difficulty canceling an ISP or online account; malware and computer exploits; issues with online payment services, social networking services, internet gaming, and virtual reality; undisclosed charges; website design and promotion services; and problems with broadband internet services and content, including the truthfulness of cost, access, and speed disclosures.
- **Investment Related:** Investment opportunities in day trading; gold and gems; art; rare coins; other investment products; reports about companies that offer advice or seminars on investments; etc.
- **Mortgage Foreclosure Relief and Debt Management:** Mortgage lenders, brokers, and other entities making false promises to save consumers' homes from foreclosure; mortgage refinancing, mortgage term modifications, and debt management issues; credit organizations charging excessive fees, making false promises to provide free services, pay creditors, or reduce interest rates.
- **Office Supplies and Services:** Fraudulent or deceptive offers for toner, copier paper, maintenance supplies, equipment maintenance contracts; classified advertising and Yellow Pages invoice scams; website cramming schemes; etc.
- **Prizes, Sweepstakes, and Lotteries:** Promotions for "free" prizes for a fee; foreign lotteries and sweepstakes offered through the phone, fax, email or mail; etc.
- **Shop-at-Home and Catalog Sales:** Undisclosed costs, failure to deliver on time, nondelivery and refusal to honor a guarantee, purchases made online (not including auction sales), telephone or mail.
- **Tax Preparers:** Companies that engage in "skimming" consumer tax refunds or charging

inflated fees while promising substantial refunds; companies aiding consumers in willfully and intentionally falsifying information on a tax return to limit the amount of tax liability; entities pretending to be tax preparers or the IRS to obtain funds or information from consumers.

- **Telephone and Mobile Services:** Advertising related to mobile plans, rates or coverage areas; unsolicited mobile text messages; problems with mobile applications or downloads; other mobile device problems; charges for calls to "toll-free" numbers; unauthorized charges, such as charges for calls consumers did not make; unauthorized switching of consumers' phone service provider; misleading pre-paid phone card offers; VoIP service problems; unsolicited faxes; electronic consumer products such as smartwatches and connected-home devices that can connect to the internet and use a processor or sensors to collect consumer information; etc.
- **Travel, Vacations and Timeshare Plans:** Deceptive offers for "free" or low-cost vacations; cut-rate student travel packages; misleading time share offers; etc.

## Key Estimates

Total estimated fraud loss for 2017 is calculated to be \$1.538 billion, with 1.94 million complaints.

Fraud Category	Total \$ Loss	No. of Reports
<b>Prize/Grant</b>	<b>\$904,689,044</b>	<b>1,138,306</b>
Prizes, Sweepstakes and Lotteries	95,052,359	142,870
Foreign Money Offers & Counterfeit Check Scams	34,343,296	31,980
Grants	6,256,020	5,786
<b>Charity</b>	<b>2,536,033</b>	<b>3,703</b>
Charitable Solicitations	2,536,033	3,703
<b>Employment</b>	<b>141,032,946</b>	<b>145,089</b>
Business and Job Opportunities	46,914,979	18,702
Shop-at-Home and Catalog Sales	94,117,967	126,387
<b>Investment</b>	<b>47,697,104</b>	<b>15,079</b>
Investment Related	47,697,104	15,079
<b>Products and Services</b>	<b>113,351,638</b>	<b>290,104</b>
Tax Preparers	484,437	3,360
Telephone and Mobile Services	16,920,319	149,578
Travel, Vacations and Timeshare Plans	38,454,908	22,264
Advance Payments for Credit Services	14,904,565	17,762
Health Care	1,410,104	10,321
Internet Services	19,397,434	45,093
Internet Auction	3,575,719	2,267
Mortgage Foreclosure Relief and Debt Mgmt.	17,179,967	8,973
Office Supplies and Services	621,483	7,083
Magazines and Books	373,093	5,099
Buyers' Clubs	29,609	542
<b>Relationship and Trust</b>	<b>328,423,263</b>	<b>347,829</b>
Imposter Scams	328,423,263	347,829

## Federal Trade Commission—Consumer Fraud in U.S. Survey (2011)

Source Location: [https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey\\_0.pdf](https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf)

## Background

The FTC has previously overseen two surveys about consumers' experiences with consumer fraud. The results of the first survey, conducted in May and June 2003, were reported in an FTC staff report, "Consumer Fraud in the United States: An FTC Survey" (<https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-ftc-survey/040805confraudrpt.pdf>), which was released in August 2004. The second survey was conducted in November and December 2005. The results of this second survey were reported in another FTC staff report, "Consumer Fraud in the United States: The Second FTC Survey" (<http://www.ftc.gov/opa/2007/10/fraud.pdf>), which was published in October 2007. Both surveys asked consumers about their experiences with particular types of fraud during the preceding year. The reports examined the extent of consumer fraud and the degree to which certain groups of consumers are more or less likely to become victims. The reports also noted the means by which fraud victims first learned about a fraudulent offer or product—such as print advertising, telemarketing, internet/email, and television/radio advertising.

The 2011 survey was similar to the earlier ones, again asking consumers about their experiences with particular types of fraud during the preceding year. The survey was conducted through telephone interviews using a random digit dialing sampling methodology. The sampling scheme was designed to obtain a random sample of U.S. adults age 18 or older. Between November 28, 2011, and February 5, 2012, 3,638 interviews were completed.

## Methodology

Interviews for the 2011 FTC Consumer Fraud Survey were conducted between November 28, 2011, and February 5, 2012. The survey was conducted via telephone by a commercial survey research firm. Interviews were conducted in both English and Spanish using computer-assisted telephone interviewing and random digit dialing. A total of 3,638 interviews were completed with U.S. adults who were at least 18 years old. Both cell and landline phone numbers were included in the sample. Interviews were conducted with consumers in all 50 states and the District of Columbia. Results did not include attempted fraud, except with Prize Fraud (which includes people who attended a seminar with \$0 in losses). Weights were applied to the survey data to ensure that the overall results are as representative as possible of the national population.

## Fraud Covered

Consumers were asked if they had particular experiences rather than asking more generally whether the consumer had been a victim of a consumer fraud. The 2011 FTC fraud survey asked questions designed to learn whether consumers had been the victim of 17 types of fraud.

- **Weight Loss Products:** Purchased a weight loss product that was promoted as making it easy to lose weight or to lose weight without diet or exercise. Only lost a little of the weight anticipated or lost no weight.
- **Prize Promotions:** Paid money, made a purchase, or attended a sales presentation to receive a promised prize or lottery winnings. Did not receive the prize or winnings or the prize was not as promised.
- **Unauthorized Billing—Buyers' Clubs:** Billed for a buyers' club membership consumer had not agreed to purchase.

- **Unauthorized Billing–Internet Services:** Billed for Internet services consumer had not agreed to purchase.
- **Work-at-Home Programs:** Purchased a work-at-home program. Did not earn at least one-half of the promised level of earnings.
- **Credit Repair:** Paid someone who promised to remove negative but accurate information from credit report or promised to provide information on how to establish a new credit record that would not contain negative information in current credit report.
- **Debt Relief:** Paid someone who promised to arrange to pay off credit card debts for less than the amount owed or to arrange a lower interest rate on current credit card debt and then failed to provide the promised services or obtain the promised results.
- **Credit Card Insurance:** Purchased insurance against the misuse of a lost or stolen credit card.
- **Business Opportunities:** Purchased a business opportunity. Did not earn at least half as much as promised or did not receive promised assistance.
- **Mortgage Relief:** Made an advance payment to someone other than the company that holds or services the mortgage to obtain a mortgage modification. The modification was either not received or the terms offered were significantly worse than what had been promised.
- **Advance Fee Loans:** Paid an advance fee to obtain a promised or guaranteed loan or credit card. Promised credit was not received.
- **Pyramid Schemes:** Purchased a membership in a pyramid scheme. Did not earn at least half of the amount the promoter promised would be earned.
- **Government Job Offers:** Made a payment to someone who falsely represented that the purchaser would receive a government job.
- **Counterfeit Checks:** Received a check and sent some of the money back to the sender or to someone else. Later learned that the check was counterfeit.
- **Grants:** Paid someone who promised to obtain a grant either from the government or from someone else. No grant was received.

## Key Estimates

An estimated 10.8 % (25.6 million) of U.S. adults—those at least 18 years old—were victims of one or more of the frauds covered by this survey (“Any Surveyed Fraud”) during 2011.

**Specific Surveyed Frauds.** Note that totals listed below do not account for victims with more than one specific fraud in each category.

Fraud Type	Victims in Millions (%)
<b>Prize &amp; Grant Fraud</b>	<b>3.0 (1.3%)</b>
Prize Promotions	2.4 (1.0%)
Counterfeit Check Scams	0.4 (0.2%)
Grant Scams	0.2 (0.1%)
<b>Employment</b>	<b>4.1 (1.7%)</b>
Work-at-Home Programs	1.8 (1.7%)
Business Opportunities	1.1 (0.5%)
Pyramid Schemes	0.7 (0.3%)

Fraud Type	Victims in Millions (%)
Government Job Offers	0.5 (0.2%)
<b>Products and Services</b>	<b>15.6 (6.5%)</b>
Weight Loss Products	5.1 (2.1%)
Paid, Never Received Product	4.5 (1.9%)
Credit Repair	1.7 (0.7%)
Credit Card Insurance	1.3 (0.6%)
Debt Relief	1.5 (0.6%)
Mortgage Relief	0.8 (0.3%)
Advance Fee Loans	0.7 (0.3%)
<b>Other – Unauthorized Billing</b>	<b>7.4 (3.1%)</b>
Billing—Buyers Clubs	1.9 (0.8%)
Billing—Internet Services	1.9 (0.8%)
Billing- Other products	3.6 (1.5%)

## Internet Crime Complaint Center (IC3)

Source Location: [https://www.ic3.gov/Media/PDF/AnnualReport/2017\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2017_IC3Report.pdf)

### Background

Hosted by the FBI, IC3 initially began in 2000 as the Internet Fraud Complaint Center. It was renamed in 2003 to better reflect its broader purpose as a repository for internet-related complaints and investigative leads for law enforcement.

### Methodology

The source of all IC3's information is victim complaints that were reported to IC3. Victims of cyber or internet-related crime are encouraged or directed by law enforcement to file a complaint online at [www.ic3.gov](http://www.ic3.gov). Complainants are asked to document accurate and complete information related to the internet crime and any other relevant information necessary to support the complaint. Although this list is not verified by law enforcement, sworn law enforcement is able to use the list of complaints for investigative leads.

Crimes may be filed at IC3 if *either* the victim or the alleged subject of the internet crime is located within the United States. U.S. citizenship is not a requirement for submissions. Complaints may be referred to local, federal, or international law enforcement. Victim age is requested, but cyber victims in this report are not limited to adults (e.g., age 18 or older). Complaints may derive from individuals or companies.

Approximately 300,000 victim complaints are reported annually.

### Fraud Covered

IC3 collects information any variety of fraud or suspicious behavior with a nexus to the internet. The victim complaints are not independently verified by law enforcement. Internet crime includes any illegal activity involving one or more components of the internet, such as websites, chat rooms, or email. Internet crime involves the use of the internet to communicate false or fraudulent representations to consumers.

- **Advanced Fee:** In advance fee schemes, the perpetrator informs a victim that the victim has qualified for a large financial loan or has won a large financial award but must first pay the perpetrator taxes or fees to access the loan or award. The victim pays the

advance fee but never receives the promised money.

- **Charity:** Perpetrators set up false charities, usually following natural disasters, and profit from individuals who believe they are making donations to legitimate charitable organizations.
- **Confidence/Romance Fraud:** A perpetrator deceives a victim into believing the perpetrator and the victim have a trusting relationship, whether family, friendly or romantic. As a result of that belief, the victim is persuaded to send money, personal and financial information, or items of value to the perpetrator or to launder money on behalf of the perpetrator. Some variations of this scheme are romance/dating scams or the grandparent's scam.
- **Employment:** An individual believes they are legitimately employed and loses money or launders money/items during their employment.
- **Health Care Related:** A scheme attempting to defraud private or government health care programs, usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, stolen health information, or may involve medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums or social media, and fraudulent websites.
- **Investment:** Deceptive practice that induces investors to make purchases based on false information. These scams usually offer the victims large returns with minimal risk. Variations of this scam include retirement schemes, Ponzi schemes and pyramid schemes.
- **Lottery/Sweepstakes:** An individual is contacted about winning a lottery or sweepstakes they never entered and are asked to pay a tax or fee to receive their winnings.
- **Misrepresentation:** Merchandise or services were purchased or contracted by individuals online for which the purchasers provided payment. The goods or services received were of measurably lesser quality or quantity than was described by the seller.
- **No Lead Value:** Incomplete complaints that do not allow a crime type to be determined.
- **Nonpayment/Nondelivery:** In nonpayment situations, goods and services are shipped, but payment is never rendered. In nondelivery situations, payment is sent, but goods and services are never received.
- **Other:** Other types of fraud not listed.
- **Real Estate/Rental:** Fraud involving real estate, rental, or timeshare property.

### Key Estimates

In 2017, 301,580 complaints were filed resulting in \$1.42 billion total loss.

There were 231,125 fraud victims in 2017 (excluding other crime types) with nearly \$729 million in losses related to fraud.

Fraud Type	Reported	
	Complaints	Loss (\$)
<b>Prize and Grant</b>	<b>26,147</b>	<b>\$70,285,831</b>
Lottery/Sweepstakes	3,012	16,835,001
Overpayment	23,135	53,450,830
<b>Phantom Debt</b>	<b>9,149</b>	<b>12,467</b>
Government Impersonation	9,149	12,467
<b>Charity</b>	<b>436</b>	<b>1,405,460</b>
Charity	436	1,405,460
<b>Employment</b>	<b>15,784</b>	<b>38,883,616</b>
Employment	15,784	38,883,616
<b>Investment</b>	<b>3,089</b>	<b>96,844,144</b>
Investment	3,089	96,844,144
<b>Products and Services</b>	<b>126,884</b>	<b>285,519,934</b>
Advanced Fee	16,368	57,861,324
Misrepresentation	5,437	14,580,907
Nonpayment/Nondelivery	84,079	141,110,441
Real Estate/Rental	9,645	56,231,333
Health Care Related	406	925,849
Tech Support	10,949	14,810,080
<b>Relationship and Trust</b>	<b>15,372</b>	<b>211,382,989</b>
Confidence Fraud/Romance	15,372	211,382,989
<b>Other</b>	<b>34,264</b>	<b>23,853,704</b>
Other	14,023	23,853,704
No Lead Value	20,241	0

## AARP Fraud Watch Network Survey

Source Location:

[https://www.aarp.org/content/dam/aarp/research/surveys\\_statistics/econ/2014/Caught-Scammer-Net-Risk-Factors-Internet-Fraud-Victims.doi.10.26419%252Fres.00076.001.pdf](https://www.aarp.org/content/dam/aarp/research/surveys_statistics/econ/2014/Caught-Scammer-Net-Risk-Factors-Internet-Fraud-Victims.doi.10.26419%252Fres.00076.001.pdf)

## Background

*Caught in the Scammer's Net: Risk Factors That May Lead to Becoming an Internet Fraud Victim: AARP Survey of American Adults Age 18 or Older, 2014* was published through the FraudWatch Network, part of AARP. The study sought to answer the following research questions:

- Are there behaviors and life experiences that may increase a person's risk of becoming a victim of online fraud?
- What proportion of individuals nationally, and in particular target states, may be at risk of being victimized by online fraud?
- How concerned are Americans about online fraud and what, if any, steps are they taking to protect themselves?

## Methodology

The GfK Group conducted the survey at AARP's behest to examine internet use and experiences with internet-related fraud. The survey was conducted online, using a sample from GfK's KnowledgePanel; a supplement was used to create some state-specific statistics for Arkansas, Arizona, Florida, Georgia, Idaho, Indiana, New Hampshire, New York, Ohio, South Dakota, Texas, and Washington state. Per the report, 11,741 state surveys were completed from November 13, 2013, through December 30, 2013.

The GfK KnowledgePanel had 8,150 respondents whereas 3,591 came from an off-panel sample to supplement the state oversamples thus ensuring a minimum of 800 completions per state except in South Dakota. Moreover, the KnowledgePanel completed 1,539 national sample surveys. The national survey had a completion rate of 51.3% and a margin of error of 3.1.

The questionnaire asked respondents about the following:

- Internet use, access, and familiarity
- Frequency of internet use
- Online statements of privacy and terms of agreements
- Online shopping
- Facebook
- Smartphone/internet applications
- Knowledge about internet safety
- Life events/personal/psychological measures, including
  - What stressful life events the respondent experienced in the past 2 years
  - A risk index scale (e.g., “I enjoy making risky financial investments now and then”)
  - A feelings index scale (“How often do you feel... isolated from others? Left out?”)
  - Feelings about debt the respondent holds
- Experience with online fraud, including
  - Description of a scam
  - Whether respondent received an email about the scam, and whether they responded to it
  - Whether the respondent lost money, and how much
  - Whether the respondent reported the scam to police, state attorney general, or the FTC
  - Demographics

#### Fraud Covered

Fraud Covered included the following (categorized according to the taxonomy):

- Prize and grant fraud
  - 419 scams
  - Foreign lottery
  - Sweepstakes offer
- Employment fraud
  - Advance fees for jobs
  - Secret shoppers
- Products and services fraud

- Advance fees for credit cards
- Fake check scams
- Travel scams
- Something wrong with your computer scam (tech support)
- Miracle cures
- Debt relief scams
- Timeshare condo resale
- Prescription drug scams
- Relationship and trust fraud
  - Relative in distress
  - Romance scams
- Identity theft
  - Phishing emails

### Key Estimates

Risk factors for becoming a victim of online fraud include the following:

- Behaviors
  - Clicking on pop-ups
  - Opening emails from unknown sources
  - Being impulsive
- Life experiences
  - Loss of a job
  - Feeling isolated or lonely
  - Being concerned about debt
- Knowledge
  - Being unaware that banks do not send emails to their customers asking them to click on a link to verify personal information

Nearly 1 in 5 (19%) Americans who use the internet (approximately 34.1 million people) engage in at least 7 of the 15 behaviors or experience life events that may put them at an increased risk of being victimized by online fraud.

Nearly two-thirds (65%) of Americans who use the internet (approximately 116 million people) received at least one online scam offer in 2013.

Nearly 8 in 10 (79%) Americans who use the internet are concerned about being scammed on the internet.

Respondents were grouped into four key groups:

- Those who lost money (“victims”), n=233
- Those who responded to a fraud offer but did not lose money (“at-risk users”), n=762
- Those who did not respond to a fraud offer (“non-victims”), n=6,581
- Those who never received a fraud offer (“non-receivers”), n=3,695

The table below shows the distribution of the 7,576 respondents who received an email scam.

Fraud Type	Received?	Responded?	Lost Money?	Amount of Loss						
				<\$10	\$10–\$49	\$50–\$99	\$100–\$499	\$500–\$999	\$1,000–\$4,999	>\$5,000
Prize and Grant Fraud										
419 scams	4,037	103	16	4	0	5	6	1	0	0
Foreign lottery <sup>a</sup>	2,812	47	10	0	0	2	2	2	3	0
Sweepstakes offer <sup>a</sup>	2,689	233	15	0	9	2	1	0	0	0
Employment Fraud										
Advance fees for jobs	936	57	29	5	12	10	2	1	0	0
Secret shoppers	3,001	187	25	1	5	4	9	0	5	0
Products and Services Fraud										
Advance fees for credit cards	1,802	62	26	0	12	1	3	9	1	0
Fake check scams	834	147	27	1	11	10	3	1	2	0
Travel scams	2,200	99	32	0	3	11	7	8	2	1
Something wrong with your computer scam (tech support)	2,607	210	45	0	2	3	23	16	0	0
Miracle cures	1,180	60	36	1	1	24	9	2	0	0
Debt relief scams	1,813	47	15	7	0	1	4	2	0	0
Timeshare condo resale	1,009	67	30	8	0	0	4	16	2	0
Prescription drug scams	1,535	43	8	7	1	0	0	0	0	0
Relationship and Trust Fraud										
Relative in distress	1,175	71	5	0	0	2	1	2	0	0
Romance scams	1,006	71	29	2	6	7	1	2	10	0
Identity Theft										
Phishing emails	2,896	62	10	1	1	0	7	1	0	0

<sup>a</sup> Numbers do not sum due to respondents who lost money refused to report the amount of loss.

## Financial Fraud and Fraud Susceptibility in the United States: Research Report from a 2012 National Survey

Source Location: <https://www.finrafoundation.org/sites/finrafoundation/files/financial-fraud-and-fraud-susceptibility.pdf>

### Background

The Financial Fraud Research Center—a collaboration of the FINRA Investor Education Foundation (FINRA Foundation) and the Stanford Center on Longevity—estimated that fraud cost Americans over \$50 billion a year.<sup>25</sup> In 2007, the FINRA Foundation, working alongside AARP, commissioned a telephone survey of investors between the ages of 55 and 64, including a supplemental sample of respondents pre-identified as prior victims of investment fraud.<sup>26</sup> Findings indicated that high levels of fraud susceptibility were linked to specific behaviors and attitudes toward investing. More recent research commissioned

<sup>25</sup> Financial Fraud Research Center. Scams Schemes & Swindles: A Research Review of Consumer Financial Fraud, 2011.

<sup>26</sup> FINRA Foundation. Senior Fraud Risk Survey, August 2007.

for the British Columbia Securities Commission<sup>27</sup> found that a lack of understanding of risk and return was also a driver of fraud susceptibility.

The current study contributes to a deeper understanding of the problem of financial fraud by gauging exposure and response to traditional and internet-based scams, and the relationships between susceptibility to fraud and personality, demographics, and financial capability.

## Methodology

The survey was funded by the FINRA Investor Education Foundation and conducted by Applied Research and Consulting between September 28 and October 4, 2012. A core sample of 2,000 respondents age 40 or older was recruited to reflect 2010 Census distribution for Census region, age, and ethnicity. To have an adequate sample for analysis of specific ethnicities, African American and Hispanic individuals (age 40 or older) were oversampled, bringing the total sample size to 2,364. For analysis purposes, the total sample was weighted to match 2010 Census distributions for ethnicity and gender. Respondents were surveyed online and were drawn using non-probability quota sampling from two established online panels (Survey Sampling International and EMI) consisting of millions of individuals who have been recruited to join the panel, and who are offered incentives in exchange for participating in the surveys.

A pure probability sample of this size would have an estimated margin of error of  $\pm 2$  percentage points calculated at a 95% confidence level, and the margin of error would increase somewhat for subgroupings of the sample.

The authors note limitations in the form of possible sources of error (e.g., coverage, nonresponse, and measurement error) that could affect the results. The authors also note that nearly 2,000 respondents in the current study had previously participated in FINRA Foundation's 2012 National Financial Capability Study, meaning the dataset from the current study can be combined with the dataset from National Financial Capability Study.

## Fraud Covered

Respondents were asked about 11 specific scam scenarios, here sorted into the taxonomy framework:

- Investment Fraud
  - **Oil & gas scam:** Have you ever been asked to participate in an investment that involved oil or gas exploration?
  - **Promissory note scam:** Have you ever been asked to participate in an investment that involved a promissory note?
  - **Penny stock/pump & dump scam:** Have you ever received a recommendation to purchase a penny stock?
  - **Pre-IPO scam:** Have you ever been asked to invest in exclusive shares of a company before that company's initial public offering (IPO)?
  - **High-yield investment program scam:** Have you ever been asked to participate in an investment that guaranteed a daily rate of return of over 10%?

---

<sup>27</sup> British Columbia Securities Commission. National Investment Fraud Vulnerability Report, March 2012.

- **Cold call scam:** Have you ever been called on the phone by someone you did not know who offered you an investment opportunity?
- **Free lunch seminar:** Have you ever been invited to a meeting that offered a free meal and “educational” information for some sort of investment (such as a vacation timeshare or an annuity product) that turned out to be a sales pitch?
- **Digital currency scam:** Have you ever been asked to participate in an investment that required you to pay using a digital or e-currency such as Bitcoin or e-Gold?
- Prize and Grant Fraud
  - **Email scam:** Have you ever received an email from a stranger in another country offering you a large amount of money but first requesting that you send them a deposit or fee?
  - **Foreign lottery scam:** Have you ever received a letter in the mail stating that you had won a lottery or sweepstakes in another country and included a cashier’s check advance payment on those winnings?
- Employment Fraud
  - **Multilevel marketing (MLM) scam:** Have you ever been asked to participate in an investment that offered a commission if you referred other people to participate in the investment?

#### Key Estimates

- More than 8 in 10 (84%) respondents were solicited to participate in potentially fraudulent offers:
  - 67% reported receiving an email from another country offering a large sum in exchange for an initial fee
  - 64% reported being invited to an educational investment meeting that was a sales pitch
  - 36% reported having received a letter stating that they had won a foreign lottery, including a cashier’s check
  - 30% reported having received recommendations to purchase penny stock
  - 24% reported having been cold called by a stranger offering an investment opportunity
  - 18% reported having been asked to participate in an investment that offered commission for additional investor referrals
- More than 1 in 10 (11%) of all respondents lost a significant amount of money after engaging with an offer.
  - At least 16% of respondents reported investing money in response to at least one of the potentially fraudulent offers; 11% acknowledged that making an investment in response to one of these offers turned out to be worth much less than they had been led to believe—or resulted in them losing all or more of the money they had invested.

- The range 11%–16% (arrived at through indirect questioning) is likely a more realistic indication of fraud victim prevalence than self-report. The authors caution that even 11%–16% may understate the problem, because it relies on 11 specific fraud scenarios and relies on respondent memory/recollection.
- Although 11% of respondents lost money in potentially fraudulent offers, only 4% admitted to being a victim of fraud when asked directly—which suggests an under-reporting rate of more than 60%.

Fraud-specific experiences are reported below, indicating whether respondents (n=2,364) were solicited for each type of scam, whether they engaged with the scam, and whether they lost money by engaging.

Scam Type	Percentage		
	Solicited	Engaged	Lost Money
Email scam	67%	3%	<1%
Free lunch	64	32	4
Foreign lottery	36	2	1
Penny stock	30	5	3
Cold call	24	1	1
MLM	18	2	1
Oil & gas	14	3	2
Pre-IPO	9	3	1
High-yield investment Program (HYIP)	6	1	1
Promissory note	4	1	1
Digital Currency	3	1	1
<b>At least one potentially fraudulent offer</b>	<b>84%</b>	<b>39%</b>	<b>11%</b>

IPO = initial public offering.

Percentage of respondents (n=2,364) who reported engaging and investing money in a potentially fraudulent opportunity:

Form of Engagement	Percentage
Engaged	39
Invested	16

Percentage of respondents (n=2,364) who were solicited, invested in, or lost money in a potentially fraudulent opportunity, by demographics:

Form of Engagement	Percentage					
	Total (n=2,364)	Gender		Age		
		Male (n=1,164)	Female (n=1,200)	40–49 (n=643)	50–64 (n=1,130)	65+ (n=591)
Solicited	84	87	81	78	83	93
Invested	39	42	36	31	39	49
Lost money	11	14	8	10	10	16

Self-reported fraud (when asked directly):

Form of Engagement	Percentage		
	Yes	No	Unsure
Asked to invest in a fraudulent investment	14	78	9
Invested in a fraudulent investment	4	95	2

## National Public Survey on White Collar Crime (2010)

Source Location: <https://www.nw3c.org/docs/research/2010-national-public-survey-on-white-collar-crime.pdf>

### Background

The 2010 National Public Survey on White Collar Crime was designed by the National White Collar Crime Center to measure the public's experience with white-collar crime in the following areas: victimization, reporting behaviors, and perceptions of crime seriousness. It was funded by the Bureau of Justice Assistance.

### Methodology

The National Public Survey on White Collar Crime, sponsored by the National White Collar Crime Center, obtained telephone interviews with a representative sample of 2,503 adults in the United States. Telephone interviews were conducted via landline (n=1,667) and cell phone (n=836, including 360 respondents without a landline phone). Interviews were done in English and Spanish between June 30 and August 8, 2010. Respondents were asked about fraud that occurred within the last 12 months. This survey only includes fraud that occurred against individuals. It is unclear whether fraud incidents capture only actual fraud (with loss) or also attempted fraud (no loss).

Statistical results were weighted to correct for known demographic discrepancies. The margin of error is  $\pm 2.2$  percentage points. Overall response rates were 13.0% for landline phones and 18.3% for cell phones.

### Fraud Covered

- Investment
  - **Fraudulent business venture**— “Has anyone succeeded in getting someone in your household to invest money or time in a business venture such as a work-at-home plan, a franchise, or stock purchase that turned out to be fake or fraudulent?”
  - **False stockbroker information**— “Has anyone in your household been given misleading stock or financial information that resulted in a financial loss?”
- Product and Services
  - **Price misrepresentation**— “Has anyone MISREPRESENTED to ANYONE in your household the price of a product or service by charging more than the originally stated cost?”
  - **Unnecessary repairs**— “Has someone in your household paid for repairs to a vehicle, appliance, or a machine in your home that were later discovered unperformed OR that were later discovered to be completely unnecessary?”

- **Mortgage fraud**— “Has someone in your household taken on a mortgage in which you were misled about the terms of repayment or interest rates?”
- **Fraudulent transaction**— “Has someone in your household lost money due to a fraudulent transaction conducted on the internet?”
- Other
  - **Credit card misuse**— “Has someone in your household discovered that someone else has used their existing credit or debit card accounts to make charges without permission?”
  - **Other ID theft**— “Has someone in your household discovered that their personal information had been used by someone else to obtain new credit cards or accounts without permission?”

## Key Estimates

Overall, 24% of households and 17% of individual respondents reported experiencing some form of fraud victimization in the past year (including identity theft). The table below shows the distributions of the types of fraud experienced.

Fraud Type	Individual % (Household %)
<b>Investment</b>	
False Stockbroker Information	7.7% (7.6%)
Fraudulent Business Venture	8.0% (9.7%)
<b>Product and Services</b>	
Price Misrepresentation	28.8% (28.1%)
Unnecessary Repairs	22.8% (22.3%)
Mortgage Fraud	4.4% (4.3%)
Fraudulent transaction	14.3% (15.8%)
<b>Other</b>	
Credit Card Misuse	38.7% (39.6%)
Other identity theft	9.9% (12.2%)

## Crime Survey of England and Wales

Source Location:

<https://beta.ukdataservice.ac.uk/datacatalogue/studies/study?id=7280#!/documentation>

## Background

The Crime Survey for England and Wales (CSEW), previously known as the British Crime Survey, has been in existence since 1981. The survey traditionally asks a sole randomly selected adult, in a random sample of households, details pertaining to any instances where they, or the household, were a victim of a crime in the previous 12 months. Results are disseminated via the Office for National Statistics (UK). Fraud questions were added to the survey in October 2015 and have been asked of the full survey sample since October 2017.

## Methodology

The population for CSEW is adults age 16 or over in private households in England and Wales. For year ending December 2017, the unweighted sample size was 20,974 adults. Survey questions are asked face-

to-face (some non-fraud questions are asked in a self-administered questionnaire). CSEW is a cross-sectional study; the unit of measurement is individuals. Rate estimates are provided.

## Fraud Covered

Fraud types covered, including CSEW definitions, are included below.

- Consumer products and services fraud
  - **Consumer and retail fraud:** Comprises cases where the respondent has generally engaged with the fraudster in some way, usually to make a purchase that is subsequently found to be fraudulent, for example, online shopping, bogus callers, ticketing fraud, phone scams and computer software service fraud.
- Identity theft
  - **Bank and credit account fraud:** Comprises fraudulent access to bank, building society or credit card accounts or fraudulent use of plastic card details.
- Other fraud
  - Comprises all other types of fraud against individuals not recorded elsewhere, for example, investment fraud or charity fraud.

**NOTE:** The survey also measures advance fee fraud, defined as “compris[ing] incidents where the respondent has received a communication soliciting money, mainly for a variety of emotive reasons, for example, lottery scams, romance fraud and inheritance fraud.” Because this category includes prize and grant fraud and romance and trust fraud, it cannot be mapped onto the taxonomy used.

## Key Estimates

Estimates for year ending December 2017 via

<https://www.ons.gov.uk/file?uri=%2fpeoplepopulationandcommunity%2fcrimeandjustice%2fdatasets%2fcrimeinenglandandwalesexperimentaltables%2fyearendingdecember2017/additionalfraudandcybercrimetablesyearendingdec2017.xls>

**Fraud and computer misuse by loss (of money or property)—number and rate of incidents and number and percentage of victims, year ending December 2017 CSEW<sup>1,2</sup>**

Offence Group <sup>3</sup>	England and Wales Adults Aged 16 and Over			
	Number of Incidents (thousands)	Rate per 1,000 Adults	Number of Victims (thousands) <sup>4</sup>	Percentage Victims Once or more <sup>4</sup>
<b>FRAUD<sup>5</sup></b>	<b>3,241</b>	<b>70</b>	<b>2,730</b>	<b>5.9%</b>
With loss, no or only partial reimbursement	511	11	446	1.0
With loss, fully reimbursed	1,842	40	1,587	3.4
Without loss	887	19	771	1.7
<b>Bank and credit account fraud</b>	<b>2,332</b>	<b>50</b>	<b>1,972</b>	<b>4.2</b>
With loss, no or only partial reimbursement	208	4	171	0.4
With loss, fully reimbursed	1,620	35	1,393	3.0
Without loss	504	11	447	1.0
<b>Consumer and retail fraud<sup>6</sup></b>	<b>813</b>	<b>17</b>	<b>727</b>	<b>1.6</b>
With loss, no or only partial reimbursement	262	6	250	0.5
With loss, fully reimbursed	219	5	195	0.4
Without loss	332	7	284	0.6
<b>All other fraud<sup>7,8</sup></b>	<b>96</b>	<b>2</b>	<b>74</b>	<b>0.2</b>
With loss, no or only partial reimbursement	41	1	26	0.1

Offence Group <sup>3</sup>	England and Wales Adults Aged 16 and Over			
	Number of Incidents (thousands)	Rate per 1,000 Adults	Number of Victims (thousands) <sup>4</sup>	Percentage Victims Once or more <sup>4</sup>
With loss, fully reimbursed	4	0	4	0.0
Without loss	52	1	45	0.1
<b>COMPUTER MISUSE</b>	<b>1,374</b>	<b>30</b>	<b>1,125</b>	<b>2.4</b>
<b>Computer virus<sup>9</sup></b>	<b>840</b>	<b>18</b>	<b>704</b>	<b>1.5</b>
With loss, no or only partial reimbursement	220	5	207	0.4
With loss, fully reimbursed	4	0	4	0.0
Without loss	617	13	497	1.1
<b>Unauthorized access to personal information (including hacking)</b>	<b>534</b>	<b>11</b>	<b>460</b>	<b>1.0</b>
Unweighted base – number of adults	20,974			

1. New victimization questions on fraud and computer misuse were incorporated into the CSEW from October 2015. Up to the year ending September 2017 the questions were asked of half the survey sample. From October 2017 onwards the questions are being asked of a full survey sample.

(continued)

2. In March 2018 the new CSEW estimates on fraud and computer misuse were accessed by the Office for Statistics Regulation against the Code of Practice for Statistics and were awarded National Statistics status.

3. See Section 5 of the [User Guide](#) for more information about the crime types included in this table.

4. Data for sub-categories will not sum to totals shown for headline categories because people can be victims of more than one crime.

5. The 'with loss' categories relating to fraud refer to financial loss, including money stolen and additional charges or costs incurred, as well as loss of property or goods.

6. Non-investment fraud has been renamed as 'Consumer and retail fraud' to reflect the corresponding name change to the Home Office Counting Rules from April 2017.

7. For the purposes of this analysis, 'All other fraud' refers to advance fee fraud and other fraud combined.

8. In the large majority of cases of loss relating to 'advance fee fraud' and 'other fraud', victims received no or only partial reimbursement, as the nature of such frauds makes full reimbursement less likely.

9. Loss through computer viruses is mainly associated with additional charges or costs incurred as a result of the virus (e.g. repair/replacement costs), which are less likely to be fully reimbursed.

Source: Crime Survey of England and Wales, Office for National Statistics

## AARP Investment Fraud Vulnerability Study

Source Location:

[https://www.aarp.org/content/dam/aarp/research/surveys\\_statistics/econ/2017/investment-fraud-vulnerability.doi.10.26419%252Fres.00150.001.pdf](https://www.aarp.org/content/dam/aarp/research/surveys_statistics/econ/2017/investment-fraud-vulnerability.doi.10.26419%252Fres.00150.001.pdf)

## Background

The study, commissioned by AARP, sought to identify the differences between known investment fraud victims and the general investor population in three domains:

- Psychological mindset
- Behavioral characteristics
- Demographics

## Methodology

The survey was administered by phone to 1,028 individuals (214 known fraud victims, 814 general investors) between August 23, 2016, and October 17, 2016.

**Known victims of fraud.** Fraud victims were provided by an AARP database of known victims of fraud (n=8,095). All 8,095 had been victims in 29 different investment scam cases filed by state or local officials against fraudulent companies that subsequently filed for bankruptcy. All cases (n=8,095) were

called until the survey status was considered “resolved” (e.g., until an interview was completed, until a phone number was found to be nonworking, until the respondent provided a hard refusal to participate, or until at least six contact attempts had been made). From this population, 214 phone interviews were completed.

**General investors.** General investors were targeted from random digit dialing lists of eligible landlines in the United States. Respondents were screened to have taxable, non-retirement assets. From this population, 814 phone interviews were completed.

## Fraud Covered

The study only covers investment fraud (i.e., commodity futures, gold coin, real estate, ATM leaseback, oil and gas, and life insurance death benefits scams).

## Key Estimates

- Psychological mindset. Compared with general investors (n=814), a larger proportion of the known victim sample (n=214) agreed with statements that expressed the following ideas:
  - Wealth as a success measure (60%, vs. 41% of general investors)
  - Open to sales pitches (40%, vs. 30% of general investors)
  - Risk-taking (48%, vs. 30% of general investors)
  - Prefer unregulated investments (48%, vs. 30% of general investors)
  - Self-reported conservative political ideology (64%, vs. 44% of general investors)
- Behavioral characteristics. Compared with general investors (n=814), a larger proportion of the known victim sample (n=214) reported the following:
  - Being targeted by phone calls and emails from brokers wanting to sell investments (58% received at least one call per month, vs. 32% of general investors)
  - Making five or more investment decisions annually (42%, vs. 11% of general investors)
  - Making remote investments involving responding to sales pitches over the phone (24%, vs. 6% of general investors), via email (9%, vs. 3% of general investors), or in response to a TV ad (5%, vs. 4% of general investors)
- Demographics. Compared with the general investors (n=814), a larger proportion of the known victim sample (n=214) had the following characteristics:
  - Over age 70 (50%, vs. 35% general investors)
  - Male (81%, vs. 42% general investors)
  - Married (66%, vs. 58% general investors)
  - Veterans (33%, vs. 18% general investors)

All respondents were asked whether they had ever been convinced to invest their money in something by promising high or guaranteed rates of return, but the investments turned out to be worthless. Approximately 18% of general investors reported having been a victim of an investment scam.

	Percentage	
	General Investors (n=814)	Victims (n=214)
<b>Ever a victim of fraud</b>		
Yes	18.3%	47.2%
No	80.7	51.9
Don't know/refused	1.0	0.9

Of those victimized, the following was true:

	Percentage	
	General Investors (n=149)	Victims (n=101)
<b>Frequency of victimization</b>		
Only once	18.6%	48.1%
2–3 times	8.1	14.5
4–5 times	7.4	21.0
5 or more times	1.4	7.0
Don't know/refused	1.1	3.7
<b>Time frame of victimization (most recent incident)</b>		
Less than 12 months ago	1.0	4.7
1–3 years ago	1.7	15.4
4–5 years ago	1.2	11.7
More than 5 years ago	13.6	15.0
Don't know/refused	1.0	1.4

## Consumer Financial Exploitation of the Elderly in Arizona and Florida, 2010-2011

Source Location: Data: <https://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/34925>;

Report: <https://www.ncjrs.gov/pdffiles1/nij/grants/245388.pdf>

### Background

This study was funded by the National Institute of Justice and conducted by Kristy Holtfreter and Michael Reisig from Arizona State University, Daniel Mears from Florida State University, and Scott Wolfe from the University of South Carolina. The goal of the study was to understand risk and protective factors for fraud victimization among the elderly and assess awareness of state programs related to fraud prevention.

### Methodology

The study was conducted in Arizona and Florida because of the high proportion of older adults in these two states. During a one-month period from June 27, 2011, to July 27, 2011, computer-assisted telephone interviews were conducted with 1,000 persons age 60 or older in each state (for a total of 2,000 respondents). Interviews were conducted in English and Spanish and took approximately 20 minutes to complete.

The sample was selected using random digit dialing of landline phone numbers from a White Pages database. The response rate was 48.4%, based on an initial n of 4,130 eligible interviewees (households that answered the phone and included a person age 60 or older, not suffering from cognitive impairment). The sample was predominately female (63%) and white (94%), with an average age of 72.

Victimization experiences were captured using a three-step approach in which survey respondents were asked if anyone had tried to defraud them, whether the incident took place 1, 2, or more than 2 years

before the incident, and whether the fraud attempt was successful in that the respondent provided money to the fraudster. Respondents were asked this set of questions about 10 specific fraud scams.

### Fraud Covered

The researchers divided the fraud scams into three types: shopping/purchasing fraud, financial fraud, and other fraud.

- Prize and grant
  - Has anyone ever tried to get you to pay a fee to claim a phony prize, like a sweepstakes or vacation? (other fraud)?
- Charity fraud
  - Has anyone ever tried to get you to contribute money to a phony charity or religious organization (other fraud)?
- Employment fraud:
  - Has anyone ever tried to get you to invest in a phony business opportunity such as work-at-home scams? (financial fraud)?
- Product/services fraud:
  - Has anyone ever tried to get you to pay for repairs to your home, an appliance or automobile for work that was never performed or was unnecessary (shopping fraud)?
  - Has anyone ever tried to sell you a health, beauty care, weight loss or other product or service that did not work as claimed (shopping fraud)?
  - Has anyone ever tried to sell you a phony subscription to magazines or something else (shopping fraud)?
  - Has anyone tried to trick you into giving them money to improve your financial situation, like repair credit or get equity out of your home (financial fraud)?
  - Has anyone tried to get you to pay money in advance to reduce your mortgage payment (other fraud)?
- Identity theft
  - Has anyone ever tried to steal your personal information so they could use it to get a credit card or a loan (other fraud)?

### Key Estimates

Nearly 6 of 10 respondents were targeted for fraud, meaning they experienced attempted or completed fraud during a 1-year period. About 14% of the sample experienced fraud victimization during the prior year. The most common type of fraud victimization was product or services fraud, which was experienced by 3.5%.

Fraud Type	Prevalence, %	Median Loss (\$)
Prize and Grant	0.5%	\$219
Charity	2.6	20
Employment	0.5	6,248
Products and Services		
Unnecessary repairs	1.2	225

Nonworking product	3.5	67
Phony subscription	1.1	30
Mortgage debt relief scams	0.2	700
Credit services scam	0.4	580
Other (tricked into giving information)	0.8	38

## Fraud.org Top Scams of 2018

Source Location: [https://fraud.org/romance\\_scams\\_2018topten/](https://fraud.org/romance_scams_2018topten/)

### Background

The National Consumers League reports annually on the complaints received directly from consumers at Fraud.org. The National Consumers League does not attempt to verify the authenticity of complaints.

### Methodology

Data are collected from reports made to Fraud.org, which collects the following information:

- Consumer (reporter) information, including location and year of birth
- Scammer information, including company name, contact information, and location
- Scammer contact details, including date of first contact, method of first contact
- Loss information, including the amount of money requested by the scammer, amount of money paid (by the reporter), and method of payment
- The story (via text field)

The total number of reports received in 2018 from Fraud.org is not available.

### Fraud Covered

All of the fraud types covered are unknown; The National Consumers League only reports the “top” scams of each year. However, the following categories are included in the 2018 report, with their definitions below:

- Prize and grant fraud.
  - **Prizes/Sweepstakes/Free Gifts.** Requests for payment to claim fictitious prizes, lottery winnings, or gifts.
  - **Fake Check Scams.** Consumers paid with phony checks for work or for items they are trying to sell, instructed to wire money back to buyer.
  - **Scholarships/Grants.** For a fee, a “search company” offers to conduct customized search for scholarships or grants for students. Scammers take money and run or provide a worthless list.
- Phantom debt fraud.
  - **Recovery/Refund Companies.** Scammers contact victims and claim they owe money on a fictitious debt or offers to recover money lost in a previous scam.
- Products and services fraud.

- **Internet.** General Merchandise Sales (not auctions). Goods purchased are either never delivered or misrepresented.
- **Advance Fee Loans, Credit Arrangers.** False promises of business or personal loans, even if credit is bad, for an up-front fee.
- **Computers: Equipment and Software.** Scammers claim to offer “technical support” for computer problems and charge a fee to fix a nonexistent problem.
- Relationship and trust fraud.
  - **Friendship & Sweetheart Swindles.** Con artist nurtures an online relationship, builds trust, and convinces victim to send money.
  - **Family and Friend Imposters.** A scammer calls or emails, claiming that a friend or family member is in distress (e.g., in jail, in the hospital) and urgently needs funds to help.
- Identity theft.
  - **Phishing/Spoofing.** Emails pretending to be from a well-known source ask consumers to enter or confirm personal information.

## Key Estimates

Results are presented only as a percentage of the total number of reports, which is not known.

Scam Type	Percentage of Total
<b>Prize and grant fraud</b>	<b>31.69%</b>
Prizes/Sweepstakes/Free Gifts	16.97
Fake Check Scams	13.09
Scholarships/Grants	1.63
<b>Phantom debt fraud</b>	<b>7.63</b>
Recovery/Refund Companies	7.63
<b>Products and services fraud</b>	<b>40.85</b>
Internet: General Merchandise Sales (not auctions)	31.25
Advance Fee Loans, Credit Arrangers	7.37
Computers: Equipment and Software	2.23
<b>Relationship and trust fraud</b>	<b>4.22</b>
Friendship & Sweetheart Swindles	2.81
Family and Friend Imposters	1.41
<b>Identity theft</b>	<b>4.84</b>
Phishing/Spoofing	4.84

Data are also presented on method of first contact with the scammer:

Method of Contact	Percentage of Total
Websites	37.72%
Phone	32.80
Email	12.62
In person	7.58
Postal mail	6.99
Other (e.g., in person, <sup>a</sup> TV/radio, print, fax)	2.60

<sup>a</sup> "In person" is listed as a subcategory in the table and an example of an "other" method of contact. Because raw data are not available, the nature of discrepancy is unclear.

And consumer age:

Consumer Age	Percentage of Total
17 and younger	0.68%
18–25	10.67
26–35	16.65
36–45	17.02
46–55	15.80
56–65	18.87
66 and older	20.31

## Ipsos Public Affairs/Microsoft Tech Support Scam Survey

Source Location: <https://blogs.microsoft.com/on-the-issues/2016/10/17/tech-support-scams-growing-problem/#sm.0001el20x2191qf2dwnrwxckmqxzd>

Report: <https://blogs.microsoft.com/wp-content/uploads/sites/5/2016/10/Tech-Scams-Public-Report.pdf>

## Methodology

<https://blogs.microsoft.com/wp-content/uploads/sites/5/2016/10/10.17-Methodologypdf>

## Background

Ipsos Public Affairs conducted an international survey at Microsoft's behest in summer 2016 to learn more about technical support fraud in 12 countries (i.e., Australia, Brazil, Canada, China, Denmark, France, Germany, Great Britain, India, Singapore, South Africa, and the United States).

## Methodology

A sample of 1,000 adults (18+) is randomly selected from Ipsos's online panels in 12 countries, for a total of 12,000 adults. The total number of respondents is not known.

Respondents were interviewed about their experiences with technical support scams in the past year ("2015 and later") across four different types of interaction: unsolicited phone calls, unsolicited emails, website pop-ups/online ads, and being redirected to a website. Results are presented by victim action taken:

- No interaction [with the potential scammer]
- Interacted [with the potential scammer] but ignored the interaction
- Interacted [with the potential scammer], took [the scammer's] recommended action but

did not lose money

- Interacted [with the potential scammer], took [the scammer's] recommended action and lost money

## Fraud Covered

The study only covers technical support (a subcategory of Consumer Products and Services fraud).

## Key Estimates

Of the respondents in the United States:

- Experience with tech support scams:
  - 21% reported no interactions with would-be scammers in the past year
  - 46% reported interactions but ignored the interaction
  - 12% reported interacting with and taking the recommended action from would-be scammers but not losing any money
  - 21% reported interacting with and taking the recommended action from would-be scammers and losing money
- Belief that the interaction is authentic:
  - 22% believe an unsolicited phone call is authentic
  - 18% believe a pop-up/ad is authentic
  - 20% believe an unsolicited email is authentic
  - 25% believe a redirect to a website is authentic
- Among those who experienced the following interactions:
  - 34% associated Microsoft with an unsolicited phone call
  - 20% associated Microsoft with a pop-up/ad
  - 17% associated Microsoft with an unsolicited email
  - 18% associated Microsoft with a redirect to a website
- Likelihood of trusting unsolicited phone calls or emails:
  - 59% reported being “very unlikely,” 16% reported being “somewhat unlikely,” 11% reported being “somewhat likely,” and 15% reported being “very likely” to trust an unsolicited email or phone call
- Likelihood of Microsoft making initial contact with consumers:
  - 56% reported “very unlikely,” 17% reported “somewhat likely,” 13% reported “somewhat likely,” and 15% reported “very likely” that Microsoft would make initial contact with consumers

## 2019 Identity Fraud Study

Source Location: <https://www.javelinstrategy.com/press-release/consumers-increasingly-shoulder-burden-sophisticated-fraud-schemes-according-2019> (link is to press release only; complete survey results and methodology available for purchase)

### Background

The annual Identity Fraud Study is a comprehensive analysis of identity fraud trends, independently produced by Javelin Strategy & Research. The lead sponsor of this study is FIS, a global financial services technology provider. Other sponsors include marquee sponsor Experian, a global information services company, and educational partner GIACT, a payment fraud mitigation company. The study is in its 16th consecutive year and is the nation's longest-running study of identity fraud.

### Methodology

The Identity Fraud Survey is an online survey of 5,000 individuals in the U.S. general population. Respondents are adults, and fraud losses are actual rather than attempted. All results released are weighted to reflect the U.S. population.

### Fraud Covered

The Identity Fraud Survey measures "identity fraud," which is defined as "unauthorized use of some portion of another's personal information to achieve illicit financial gain." Among the types of fraud it covers are identity theft and card fraud.

### Key Estimates

Information on findings is limited by what is accessible publicly, without having to pay additional fees.

Identity Fraud Victims by Year	U.S. Population Affected (%)	Actual Loss (\$)
2017	16.7M (6.64%)	\$16.8B
2018	14.4M (5.66%)	14.7B

## National Incident-Based Reporting System (NIBRS)

Source Location: <https://www.fbi.gov/services/cjis/ucr/nibrs> (for basic description)

### Background

NIBRS is a national database of crime incidents that were reported to local, state, or federal law enforcement. Crime incident data are fed from local and state law enforcement agencies to state Uniform Crime Reporting programs, which in turn feed the data to the FBI. NIBRS data have been collected since 1989, although its collection is still quite limited.

### Methodology

Crime incident data are fed from participating law enforcement agencies to state Uniform Crime Reporting programs. These data represent all crime incidents reported to law enforcement and would include individuals and businesses and both adults and children. However, until recently, fewer than

20% of the U.S. law enforcement agencies submitted their crime incident data to NIBRS, so its results are not representative of the entire U.S. population.

### Fraud Covered

NIBRS's definition of "fraud" includes seven broad categories:

- Hacking/computer intrusion
- Credit card/ATM fraud
- Impersonation
- Identity Theft
- Welfare Fraud
- False Pretenses/Swindle/Confidence Game
- Wire Fraud

### Key Estimates

In 2016, there were 409,974 victims of fraud (as broadly defined in NIBRS) who reported the crime to law enforcement. However, numbers are much lower when subset for only fraud that fits the SFS definition.

Fraud Type	2016 NIBRS Results
False Pretenses/Swindle/Confidence Game	150,878
Wire Fraud	9,617
<b>TOTAL</b>	<b>160,495</b>