FINANCIAL SECURITY PROGRAM
aspen institute

A Pervasive Threat

Analyzing Recent Survey Data on Fraud and Scams

December 2025

AUTHORS AND CONTRIBUTORS

Laila Bera authored this report with research contributions from Shehryar Nabi.

We are grateful to our Aspen FSP colleagues Steven Brown, Sheida Elmi, Erin Borġ, and Kate Griffin for their assistance, comments, and insights in the development of this brief.

We are also grateful to Hector Ortiz of the Consumer Financial Protection Bureau for his insight and advice on the data.

ACKNOWLEDGEMENTS

This report is a product of Aspen FSP. We thank JPMorganChase, Zelle, Target, Block, Flourish Ventures, Amazon, CLEAR, and Plaid for their generous support of the Task Force and this report, as well as our impact partners AARP and Stop Scams Alliance. The findings, interpretations, and conclusions expressed in this report—as well as any errors—are Aspen FSP's alone and do not necessarily represent the views of its funders or other Task Force participants.

REFERENCE

The project described in this paper relies on data from a survey administered by the Understanding America Study, which is maintained by the Center for Economic and Social Research (CESR) at the University of Southern California. The content of this paper is solely the responsibility of the authors and does not necessarily represent the official views of USC or UAS.

ABOUT THE ASPEN INSTITUTE FINANCIAL SECURITY PROGRAM

The Aspen Institute Financial Security Program's (Aspen FSP) mission is to illuminate and solve the most critical financial challenges facing American households and to make financial security for all a top national priority. We aim for nothing less than a more inclusive economy with reduced wealth inequality and shared prosperity. We believe that transformational change requires innovation, trust, leadership, and entrepreneurial thinking. Aspen FSP galvanizes a diverse set of leaders across the public, private, and nonprofit sectors to solve the most critical financial challenges. We do this through deep, deliberate private and public dialogues and by elevating evidence-based research and solutions that will strengthen the financial health and security of financially vulnerable Americans. To learn more, visit **AspenFSP.org**, join our mailing list at **http://bit.ly/fspnewsletter,** and follow **The Aspen Institute Financial Security Program** on LinkedIn.

Introduction

Fraud and scams pose a significant threat to U.S. households and are an urgent national security crisis.[1] Estimates show that one in five Americans (about 50 million) have lost money to an online scam or attack. The total financial loss of scams and fraud is devastating; according to the Federal Bureau of Investigation and Financial Trade Commission (FTC), about $16 billion and $12 billion in annual losses have been reported to them, respectively, and the FTC estimates that, accounting for under-reporting, total fraud and scam-related losses to U.S. consumers are $196 billion per year.[2]

The financial cost of scams varies wildly, from losing $25 after ordering from a fake retailer whose product will never arrive, to losing over $1 million in retirement savings to a romance investment scam.[3] Scam losses have negative consequences on the overall financial well-being of U.S. households. In the short term, scams threaten household financial stability, making it difficult to meet day-to-day financial needs and build savings. In the medium term and long term, losing money to a scam compromises households' financial resilience and their ability to invest and plan for the future.

Scams affect all households, but the impact of scams varies by income and age. Older Americans experience higher dollar losses. It can be particularly devastating for older adults who don't have additional years of earned income to rebuild a retirement fund after losing it to a scam. For younger Americans, who often have fewer assets to begin with, losing money to a scam can impact their ability to pay for day-to-day expenses and delay their ability to start building their own nest eggs. Regardless of the loss amount, the data paints a clear compelling picture: Scams are impacting people of all ages, genders, and income levels, as well as those across various geographies and educational backgrounds.

This brief highlights new findings on the prevalence of fraud and scams in the United States, based on an analysis of data from the Understanding America Survey (UAS). The survey, conducted between December 2024 and January 2025, asked respondents about their experiences with fraud and scams, whether and how often they had lost money, and their experiences of being made to feel blamed when reporting fraud and scam losses to their institutions.

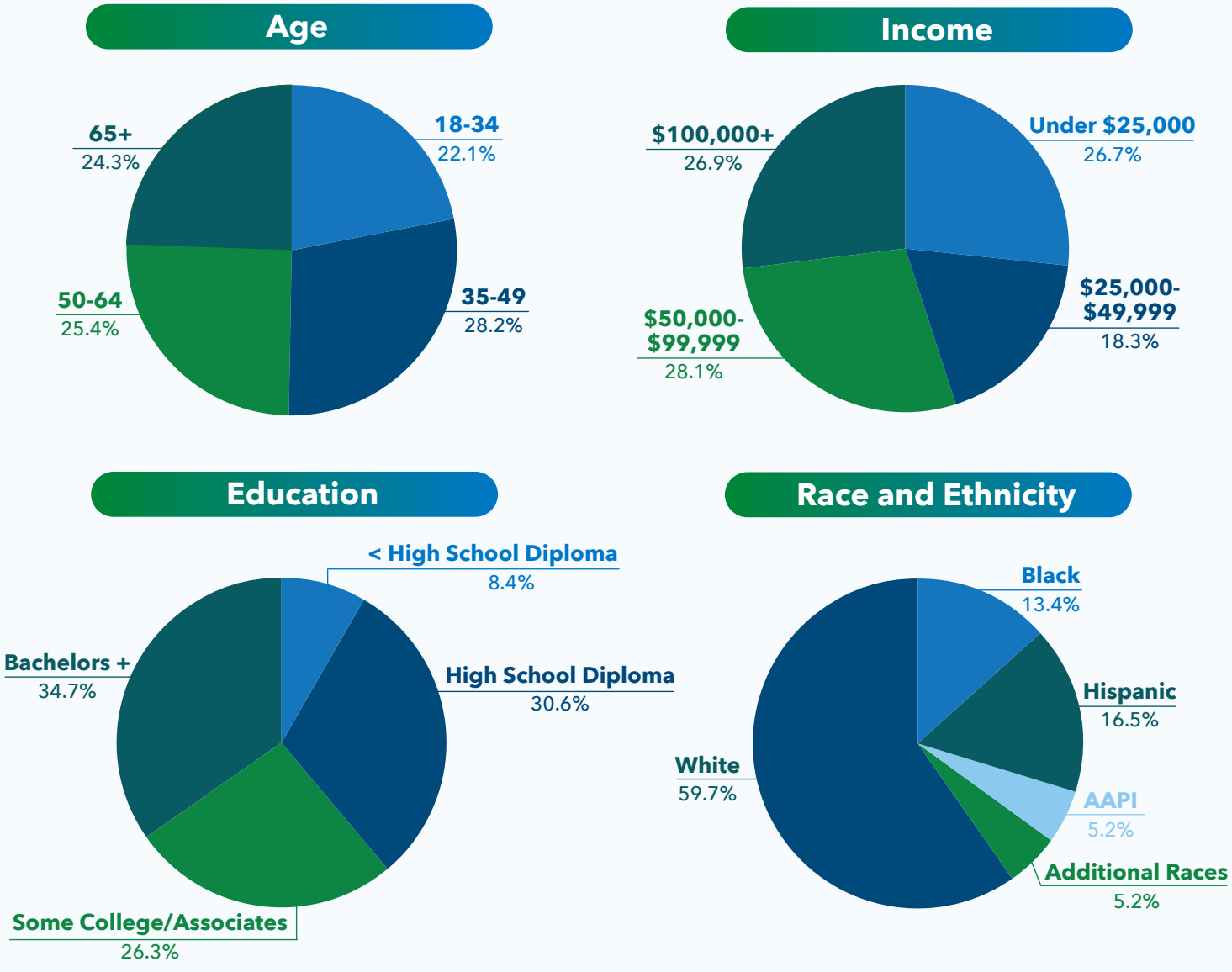
Key Insights

Fraud and Scams Impact Wide Swaths of Americans

While fraud and scams are often perceived as targeting older Americans, UAS data show people of all ages, incomes, and backgrounds are affected. This challenges stereotypes and emphasizes the pervasive nature of the scam threat. Figure 1 shows different age groups experience fraud and scams at similar rates in 2024. Adults earning less than $25,000 are just as likely to be scammed as those earning over $100,000, yet at least 30 percent in both groups reported losses in 2024.[4] Overall, over 87.5 million people, or 33 percent of American adults, reported experiencing a scam in the prior year.[5] Those scams resulted in at least $42.7 billion in total unrefunded losses, with an average loss of nearly $2,400.

Figure 1. Broad Swaths of Adults Report Experiencing Frauds and Scams

Distributions of U.S. adults who experienced a fraud or scam in the prior 12 months by age, income, education, and race/ethnicity



Scam Victims Are Often Revictimized

Being scammed once is harmful enough, but unfortunately, for many people it happens multiple times. More than one in 10 U.S. adults (10.6 percent) had experienced multiple scams in the past year and as Figure 2 shows, the adults who experience multiple scams are similar in many ways to those who report only one prior fraud or scam in the past year. Across all age groups, income levels, and educational backgrounds, only adults earning less than $50,000 reported higher rates of multiple scam or fraud attempts. Notably, there are minimal differences in age across the number of attempts reported and no differences in education, suggesting that these are not primary drivers of revictimization.

Figure 2. Adults with Lower Incomes Report More Revictimization, Much Smaller Differences in Age and Education

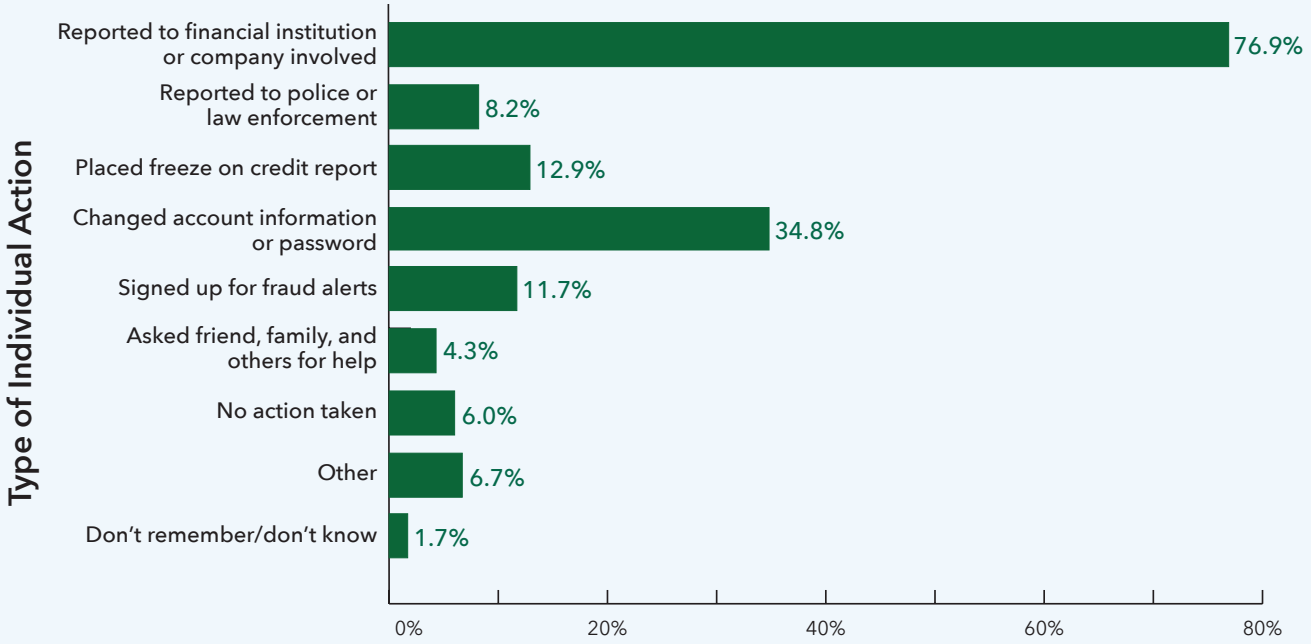
Demographics by number of times adults report experiencing a fraud or scam within the prior 12 months

	Number of Recent Frauds or Scams	
	One	Multiple
Age (mean)	51.3	50.6
Income Distribution		
Under $50,000	37.7%	44.7%
$50,000-$99,999	32.1%	27.6%
$100,000+	30.1%	27.7%
Educational Distribution		
Up to Associate's	63.1%	63.1%
Bachelor's or More	36.9%	36.9%

These findings are in line with what we hear from victim support service experts: Scamming is a crime that has a high rate of revictimization compared to other crimes. This pattern of repeat victimization highlights the persistent threat of scams and the vulnerability it creates for individuals and families. Each new incident compounds the financial and emotional toll, making it even more difficult for people to recover and feel trust in a digital world.

3 in 4 Adults Reported the Most Recent Fraud or Scam to Their Financial Institution

Figure 3. Individuals' Responses After Having Money Taken From Their Account Due to a Fraud or Scam



Note: Answers sum to more than 100% because respondents were allowed to select multiple actions.

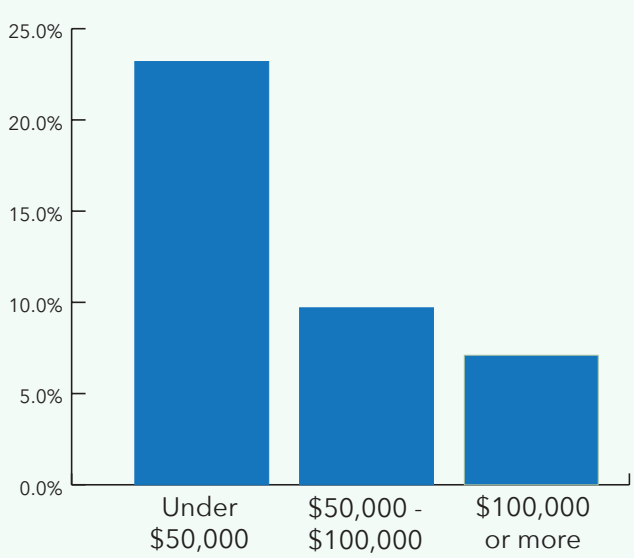
Most victims reported their fraud or scam to their financial institution after they had money taken from their account, but few reported it to law enforcement or asked others for help.[6] Figure 3 shows that when Americans experience financial loss from a fraud or scam, the overwhelming majority (about 77 percent) report the incident to their financial institution or the company involved. Far fewer turn to law enforcement, with only about 8 percent reporting to the police. After a fraud or scam, many individuals take proactive steps to protect themselves from further harm; over a third change their account information or passwords, and about 13 percent place a freeze on their credit report. Smaller shares sign up for fraud alerts or seek help from friends and family. Notably, 6 percent of respondents report taking no action. These findings tell us that more consumer-reported data on fraud and scam losses are found at financial institutions than at law enforcement agencies.[7]

Although 13 federal agencies, such as the Internet Crime Complaint Center (IC3), the FTC, and the FBI, provide a way for consumers to report their losses, 3 out of 4 U.S. adults report fraud or scams directly to their primary financial institution, while about one in 12 U.S. adults report to the police or law enforcement.[8] This consumer preference for reporting to financial institutions indicates that relying on federal reporting alone is insufficient for understanding the national landscape of fraud and scams.[9]

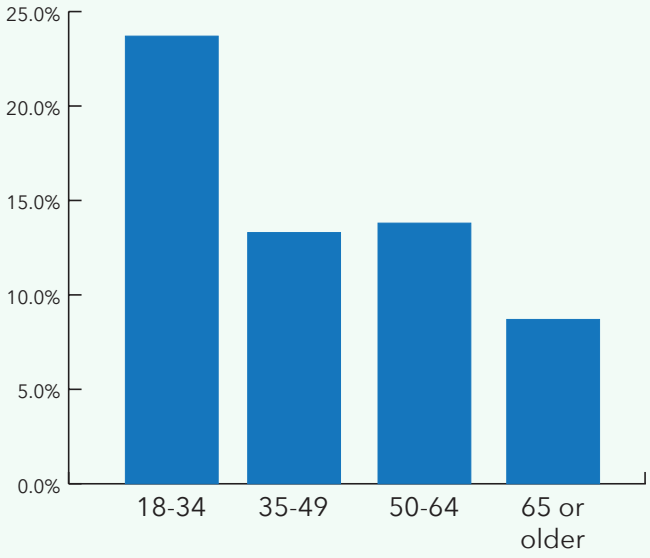
Disparities in Blame Experienced After Reporting Fraud or Scams

Figure 4. Percentage of Victims Who Felt Blamed After Reporting Losses

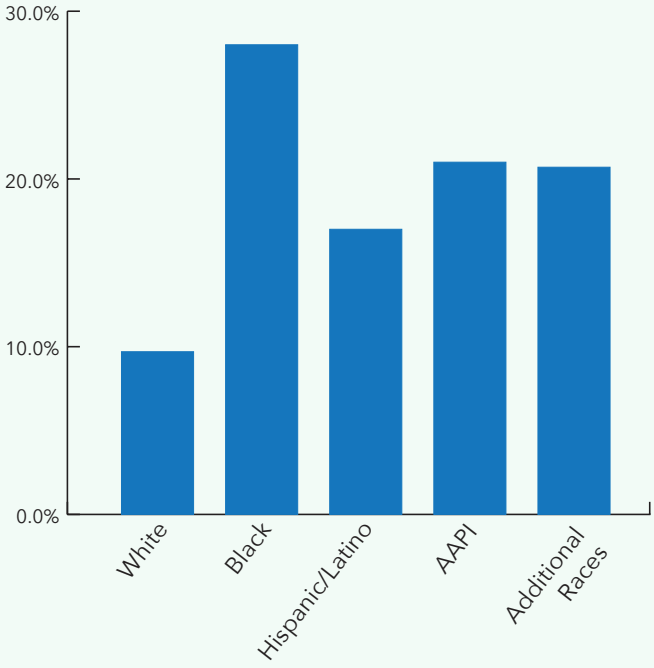
Distributions of U.S. adults who felt blamed by their institutions by income, age, and race/ethnicity



Household Income



Age



Race and Ethnicity

Note: These data only represent people who reported their loss to the institution.

Although fraud and scams impact all Americans, some populations are more likely to feel blamed when they seek help than others. This is particularly true for young adults, low-income households, and Black non-Hispanic people who experience higher rates of blame than older adults, high-income households, and White non-Hispanic people. Among those who reported to an institution,14 percent reported that they were made to feel blamed or made to feel personally responsible. When broken down by household income, age, and race and ethnicity, blame is unevenly distributed across groups as shown in Figure 4, including:

- Households with incomes less than $50,000 are over three times more likely to feel blamed after reporting fraud compared to households with incomes $100,000 or more (23.2 percent vs. 7.1 percent).
- Among adults under 35, about one in four report feeling blamed after reporting, compared to one in 13 seniors aged 75 and above (23.7 percent vs. 8.7 percent).
- Racial and ethnic disparities are substantial. About one in four Black, non-Hispanic individuals (28.7 percent), one in five Asian non-Hispanic individuals (21.3 percent), one in five Hispanic or Latino (17 percent), and one in five other, multiracial non-Hispanic (20.4 percent) victims felt blamed after reporting. In contrast, only one in 10 White, non-Hispanic respondents had the same experience (9.7 percent).

These findings urge institutions to modify their current practices to ensure all victims are treated with dignity when reporting a fraud and scam loss. Victim support experts, including AARP and the Financial Industry Regulatory Authority Foundation, have identified shame as one of the contributing factors that deters victims from reporting.[10] This is an opportunity for institutions to better respond to consumer needs and further underscores that scams cause significant emotional distress.[11]

A Need for a Unified Measurement Framework

The UAS data provides some directional insights into the true scale, scope, and complexity of fraud and scam trends, as well as victims' experiences of being made to feel blamed when reporting. We know, however, that further information is needed to support private and public sector leaders to drive resources toward prevention efforts. Below are recommendations to advance the field of measurement and aid future research.

Limitations of Current Fraud and Scam Research

Current research often combines scams and fraud, and sometimes cyber attacks, into a single category, making it difficult to fully understand the unique challenges each issue presents. Yet scams and fraud are fundamentally different, and each requires distinct solutions and policy responses. In the financial services field, fraud typically means unauthorized transactions that occur without a consumer's consent. Scams, on the other hand, involve authorized transactions where a person has been manipulated or deceived, often through sophisticated social engineering tactics. While often conflated with fraud and scams, cyber attacks refer to malicious activity that

attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.[12] For example, ransomware prevents victims and businesses from accessing computer files, systems, or networks and demands a fee to be paid for access to be granted. These attacks often target critical infrastructure and enterprise defenses, rather than consumers.

Recognizing these differences is crucial, as each has its own risk patterns, prevention tools, and regulatory considerations. For example, in the case of fraud, companies attempt to detect anomalies that indicate account takeovers, such as new device sign-ons from unusual locations. Scam transactions, on the other hand, are conducted by users who can bypass verification and answer any security question in a multi-factor authentication request and are often more challenging to detect.

By keeping these categories distinct in data collection and analysis, researchers and policymakers can gain a clearer picture of the scale, scope, and trends driving harm. This clarity is essential for directing resources where they will have the greatest impact and for designing prevention efforts that address the specific tactics used by criminals. While some studies opt for broad classifications like "scam attacks," such approaches can blur important distinctions that matter for both consumers, policymakers, law enforcement, and industry leaders.

The lack of a unified measurement framework also creates challenges for comparing data sets and findings. For example, the Understanding America Survey, Making Ends Meet surveys, and the U.S. Census, although they are nationally representative studies, are not designed to be directly comparable and ask slightly different questions. Similar inconsistencies appear across research from government agencies and private organizations. The U.S. Government Accountability Office 2025 report maps the landscape of varying definitions of scams across government agencies, including the Federal Reserve's Scam Classifier Model, which defines scams as "the use of deception or manipulation intended to achieve financial gain."

The FTC and FBI (along with other agencies) have also developed their own fraud taxonomy framework.[13] The FTC's Sentinel data, for instance, depends on consumer-reported cases, yet evidence shows that many victims and financial institutions do not report incidents to federal authorities. When victims report incidents, it is unclear whether they contact multiple agencies and, if so, to what extent these overlaps affect the duplication of results in reports by the FTC or FBI. Without standard definitions and consistent reporting, efforts to synthesize findings or benchmark progress are undermined, leaving policymakers and practitioners with an incomplete understanding of the landscape.[14]

Recommendations

In 2025, the Aspen Institute Financial Security Program developed a comprehensive set of recommendations for a national strategy to prevent fraud and scams with input from more than 300 experts across 80-plus organizations for an all-of-ecosystem approach.[15] Within that report, the Scams Prevention Framework outlines the key strategies for corporate leaders, policymakers, and all stakeholders to act against scams and empower scam prevention efforts.[16]

The report also offers a proposed metrics framework as a starting point for researchers with a focus on scale, trends, and efficacy, including efforts to:[17]

- **Disaggregate fraud and scams in nationally representative survey data collection methods** to ensure more robust data collection that allows for granular analysis of trends and harms.
- **Develop clear, distinct standard definitions of fraud and scams that can be adopted by federal agencies, nonprofit research institutions, and the private sector** to ensure greater harmonization of reports and support apple-to-apple comparisons. This could include using the Federal Reserve Board's Scam Classifier Model decision tree for payments as a sample framework to develop a more robust industry-agnostic model for fraud and scams.
- **Promote better, more systematic data collection on scam activity, reporting mechanisms, and interventions.** This may include a combination of nationally representative surveys, economic modeling, and funding for research studies.
- **Implement and replicate fraud and scam modules in nationally representative surveys** to ensure longitudinal data collection and to make use of existing data collection efforts. Surveys administered by federal agencies, such as the Survey of Household Economics and Decisionmaking and the Making Ends Meet Survey, have moved in this direction in recent years, but should expand to other data collectors and survey administrations with representative samples, such as Gallup, Pew Research, and the U.S. Census Bureau.
- **Leverage private sector data and transaction data**—specifically where the money was sent, what channel was used, and how much money was lost—to further fill information gaps and provide a more holistic view of the scale and scope.

Areas for Future Study

The field of fraud and scam measurement is emerging and expanding. There are many compelling questions that researchers, policymakers, and industry leaders can explore to move the field forward, including:

1. What is the current landscape regarding definitions of fraud and scams, and how does harmonizing these definitions impact our understanding of their scale and trends? Having a clear consensus of where these crimes fit within legal and regulatory frameworks could open new avenues for prevention, enforcement, and victim support.
2. How can we measure the effectiveness of real-time friction interventions across platforms? Evaluating interventions, such as warning prompts or transaction holds, in real time and across different platforms can help identify what actually deters fraud and scams before they cause harm.
3. How do institutional practices contribute to feelings of blame or personal responsibility among different demographic groups, and what training or practices can effectively reduce these disparities?

Conclusion

The Understanding America Survey deepens our knowledge of how fraud and scams impact the lives of Americans across all ages, incomes, and communities. The findings make it clear: No group is immune, and the financial harm caused by these crimes can derail households' stability and long-term financial security. High rates of repeat victimization underscore the urgent need for coordinated action.

Despite the scale of the problem, current systems for reporting and tracking fraud and scams leave policymakers with an incomplete picture. Most victims turn to their financial institutions rather than law enforcement, leaving much of the data siloed and untapped. When victims do report, some are made to feel blamed more than others. The lack of standard definitions and a unified measurement framework make it challenging to understand trends, target resources, and benchmark progress.

To address these challenges, it is essential to create a unified framework for measuring fraud and scams that enables consistent data collection and analysis across sectors. We call on policymakers, corporate leaders, and advocates to come together to further refine and implement this unified measurement framework. Only through coordinated action can we close data gaps, track progress, and target solutions that will protect households nationwide.

For more detailed recommendations on Aspen FSP's recommendations for a whole-of-society approach to prevent scams, read *United We Stand: A National Strategy to Prevent Scams*.

Data

The analyses presented here are based on data collected across multiple surveys/modules of the Understanding America Study, specifically 665, 670, and 681. Survey 665 was the module focused on experiences with fraud, including questions about losing and recovering funds, the financial products and institutions involved in the fraud or scam, and actions taken after experiencing the most recent fraud or scam.

UAS 665 was fielded between December 2024 and January 2025, with 3,812 respondents, weighted to be representative of U.S. adults ages 18 and older.

Endnotes

1 Jeffrey Gottfried, Eugenie Park, and Monica Anderson. "Online Scams and Attacks in America Today." Pew Research Center. July 31, 2025. https://www.pewresearch.org/internet/2025/07/31/online,;-scams-and-attacks-in-america-today/. A ratio of 1 in 5 adults equates to approximately 53 million adults, based on a total U.S. adult population of approximately 267 million. See: U.S.Census Bureau, "National Population by Characteristics: 2020-2024," June 2025. https://www.census.gov/data/tables/time-series/demo/popest/2020s-national-detail.html.

2 The 2024 Internet Crime Report combines information from complaints of suspected internet crime and details reported losses exceeding $16 billion—a 33 percent increase in losses from 2023. See: Federal Bureau of Investigation. "Internet Crime Report 2024." Internet Crime Complaint Center (IC3). April 24, 2025. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report. Of the 2.6 million fraud reports, 38 percent indicated money was lost. In 2024, people reported losing over $12 billion to fraud-an increase of over $2 billion over 2023. See: Federal Trade Commission. "Sentinel Network Data Book 2024." March 2025. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024. Federal Trade Commission. December 1, 2025. "Protecting Older Consumers 2024—2025." https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.

3 Fulford, Scott. "More Than a Quarter of Americans Lost Money to Financial Fraud." LinkedIn, August 2025. https://www.linkedin.com/pulse/more-than-quarter-americans-lost-money-financial-fraud-scott-fulford-2qije.

4 Figure 1 presents the percentage of respondents who experienced a fraud or scam of any kind, regardless of whether financial loss occurred. Of those who experience a fraud or scam, at least 30% of respondents who reported losing money were unable to recover it.

5 From the UAS survey: Experiences with fraud and scams (the survey does not distinguish between the two) refers to "situations where someone takes or tries to take your money, without your permission or through deception."

6 We refer here to people who had money taken from their account, which includes people who had all of the taken money returned to them and people who had some or none of the taken money returned to them.

7 Data reported are from the perceptions of UAS data respondents when responding to the question: When you experienced the most recent fraud or scam, what did you do?

8 For more information about the different federal agency reporting mechanisms see: U.S. Government Accountability Office. "Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams (GAO-25-107088)." April 2025. https://www.gao.gov/assets/gao-25-107088.pdf.

9 Ibid.

10 AARP Fraud Watch Network and FINRA Investor Education Foundation, in collaboration with Heart + Mind Strategies. "Blame and Shame in the Context of Financial Fraud: A Movement to Change Our Societal Response to a Rampant and Growing Crime." June 2022. https://finrafoundation.org/sites/finrafoundation/files/Blame-and-Shame-in-the-Context-of-Financial-Fraud.pdf.

11 The Identity Theft Resource Center's 2025 Consumer Report showed that 25 percent of victims have thought about suicide due to identity theft crime revictimization. See: Identity Theft Resource Center. "ITRC 2025 Consumer Impact Report." Identity Theft Resource Center, 2025. https://www.idtheftcenter.org/publication/itrc-2025-consumer-impact-report/.

12 National Institute of Standards and Technology (NIST). "Cyber Attack." Computer Security Resource Center Glossary. Last modified 2024. https://csrc.nist.gov/glossary/term/cyber_attack.

13 For more information on government wide scam and fraud definitions see pages 28-32 of the U.S. Government Accountability Office's "Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams (GAO-25-107088)." April 2025. https://www.gao.gov/assets/gao-25-107088.pdf.

14 The Scam Threat Abstract from the National Strategy provides an evidence base which combines multiple studies on scams and fraud: https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/68dc501beab5733960d4daaf/1759268891938/AspenFSP_TheScamThreat_Figure1.pdf.

15 Aspen Institute Financial Security Program. Nick Bourke, Erin Borġ, Laila Bera, Molly Rubenstein, and Kate Griffin. "United We Stand: A National Strategy to Prevent Scams." Aspen Institute Financial Security Program, 2025. https://fraudtaskforce.aspeninstitute.org/nationalstrategy.

16 Aspen Institute Financial Security Program. "Fraud and Scam Prevention Framework: Figure 2." Aspen Institute Financial Security Program, 2025. https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/68dc5029d5d8207a0b480e26/1759268905677/AspenFSP_FraudandScamPF_Figure2.pdf.

17 For an in-depth measurement framework sample and further recommendations on advancing measurement, see Figure 4 on page 43 of the National Strategy for Preventing Financial Fraud and Scams: Aspen Institute Financial Security Program. "United We Stand: A National Strategy to Prevent Scams".