The Scam Economy:

The True Cost of Online Scams and Crimes in America

A **Consumer Federation of America** Report

MARCH 2026

Consumer Federation of America

TABLE OF CONTENTS

FOREWORD

Federal agencies, third parties, and other groups report on scam losses each year, but these numbers are only the tip of the iceberg in measuring the size and devastation experienced by those who are targeted. Behind these reports and big spreadsheets describing reported losses are shattered families, rent money lost, and grandmothers exploited.

Newer technology is leading to a *rise* in these scams – in both severity and number: AI is supercharging these scams, social media platforms are enabling the spread, and data brokers facilitate targeting of victims, allowing criminals to reach consumers at massive scales while exploiting highly precise profiling to victimize vulnerable people.

One of the biggest problems in fully understanding the scope of these scams is underreporting. Due to reporting fragmentation and communication, as well as the understandable devastation, embarrassment, and confusion that victims often feel, estimates on how many people report their losses to scams put it extremely low – often in the single digit percent of the actual number, according to conservative key government estimations.

CFA is proud to publish this report that takes the most conservative estimate of underreporting and uses it to estimate *The True Cost of Scams*. While this issue is complicated to solve completely, there are significant unrealized opportunities for legislators, enforcement agencies, and industry to step up to address it.

We hope this data will bring this ugly underbelly of truth to light and inspire action. CFA will continue to work with policymakers, regulators, and other partners to improve prevention, reporting, and remedy of scams today to bring down these numbers and save Americans money, embarrassment, and anguish tomorrow.

Ben Winters
Director of AI and Privacy
Consumer Federation of America

A COMPREHENSIVE ANALYSIS OF NATIONAL AND STATE-LEVEL INTERNET BASED CRIME AND SCAM LOSSES

The amount of money Americans report losing each year to scammers is staggering. However, due to underreporting, those numbers don't come close to reflecting the actual cost. This report takes on the task of calculating the real damage inflicted by scammers and cybercriminals on Americans.

In 2024, Americans reported losing $16.6 billion to internet based scams and crimes according to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), which tracks a broad range of cybercrime incidents.[1] They note that this is a 33% increase from the 2023 total. Additionally, the Federal Trade Commission (FTC) documented a huge $12.5 billion in fraud losses across all channels that year, including both online and offline consumer fraud incidents.[2]

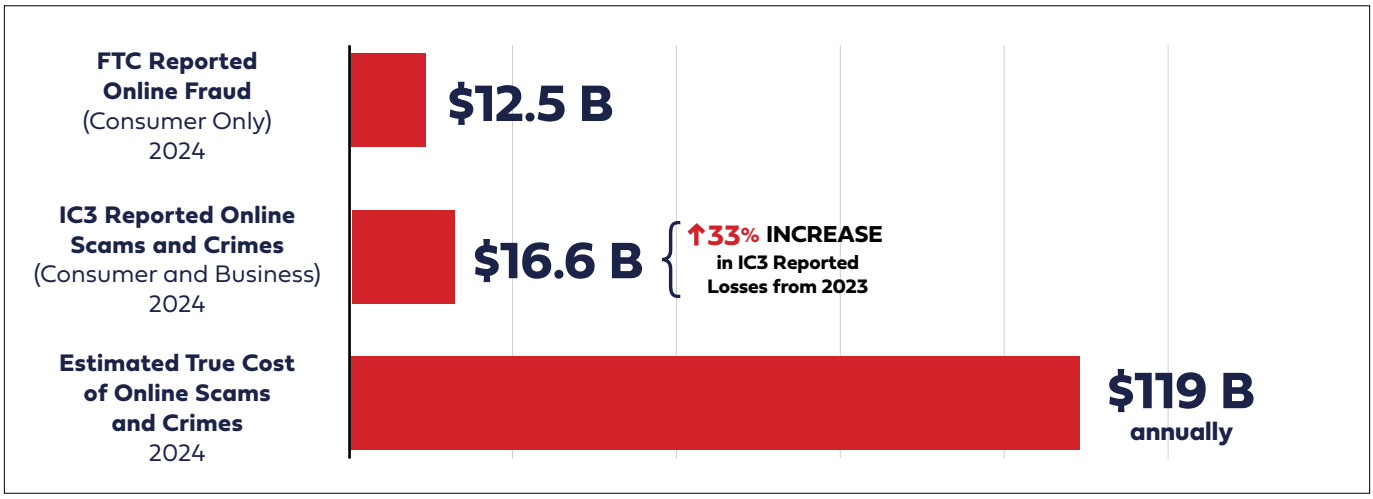
But those are just the official numbers. As the former Philadelphia police deputy commissioner Nola Joyce aptly described the challenge: **"It's the old iceberg metaphor. What we know about is above the surface. But in terms of value, and in terms of harm, a lot of that crime is below the surface."**[3]

What's more, the problem is poised to get worse as scammers become more sophisticated, consolidating their power and reach and operating from international scam havens. A recent interview in *The Economist* featured Martin Purbrick, an expert in Chinese organized crime, talking about how online scams may now rival illegal drugs in scale and societal harm and how scam networks are using technology in ways that allow them to target and deceive people more and more effectively, reducing the ability of victims to detect fraud before losses occur.[4]

This report's top findings:

- Using an analysis of underreporting patterns documented by the Bureau of Justice Statistics (BJS) and other researchers, and the FBI ITC 2024 data, we estimate in this report that the true cost of scams in America is in fact **at least $119 billion annually**. And this is a conservative estimate; other third party research (that we highlight in the "measuring underreporting" section of the

Figure 1. Reported Versus Estimated True Cost of Scams and Crimes



Sources: *FBI Internet Crime Complaint Center (IC3), Federal Trade Commission 2024.*

1 Federal Bureau of Investigation, "2024 Internet Crime Report," Internet Crime Complaint Center, 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

2 Federal Trade Commission, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024," March 10, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

3 "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported," The New York Times, February 5, 2018, https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html.

4 "Online Scams May Already Be as Big a Scourge as Illegal Drugs," *The Economist*, February 6, 2025. https://www.economist.com/briefing/2025/02/06/online-scams-may-already-be-as-big-a-scourge-as-illegal-drugs.

report) suggests that the direct loss may be even greater." This report's finding also does not account for indirect losses in legal and administrative costs to scams and crimes. As we describe in our methodology section, we build our analysis using conservative assumptions based on multiple studies, including peer reviewed research.. By conservative, we mean assumptions that anchor on the **lower end of credible research, ensuring our findings are best understood as a floor rather than a ceiling**.

The data show that:

- **For every reported case of online crime or scams, six go unreported to law enforcement authorities**, creating a major blind spot in our understanding of the real impact — nationally as well as for each US state and territory.

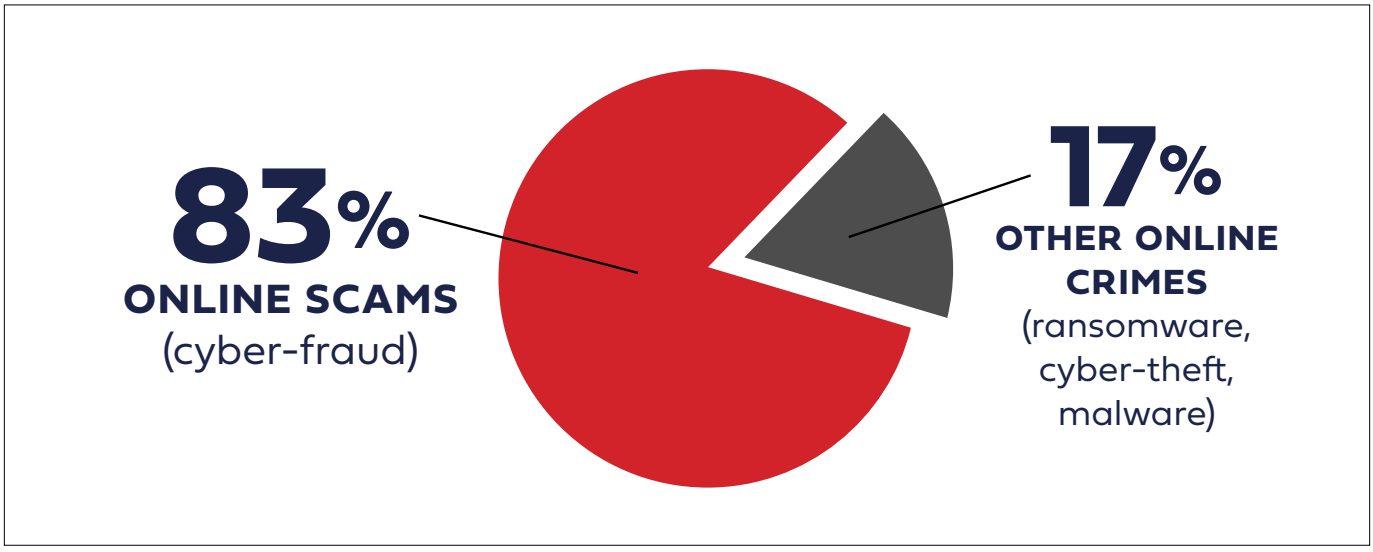
- **Online scams - or "cyber-fraud" as the IC3 report uses the term - make up the lion's share (approximately 83%) of all online scams and crimes in this report.** The other 17 percent are online crimes such as ransomware, cyber-theft, malware and related other online crimes.

- **Impact on States:** Our analysis demonstrates not just the national scope of this crisis, but provides a broad estimate of how it devastates individual states. California, for example, officially reported $2.54 billion in online-scam-related losses in 2024 — but our analysis shows that the estimated true cost to the people of California was **at least $18.1 billion**. We also estimate the projected actual losses in every other state, and highlight those hardest hit.

- **Social Media Platform involvement:** We look to the most recent reports from the Global Anti-Scam Alliance (GASA) US Survey and the Better Business Bureau (BBB) to show the role of social media platforms in online scams losses. Both the BBB and the GASA US Survey show social media as the leading scam vector.[5] The GASA 2025 report notes that: "Gmail, Facebook, and Instagram were most frequently associated with scams, X (Twitter), Snapchat, and Telegram were cited as the slowest to respond to scam reports," and they note that over half (57%) of people reporting scams say they saw no discernible action taken by the platform in response.[6]

The methodology employed here relies on verified government sources, widely trusted industry researchers, and peer-reviewed sources to paint the most accurate picture possible of the real impact of scams and cybercrime on American society.

Figure 2. Breakdown of Online Scams vs. Other Online Crimes



Sources: *FBI Internet Crime Complaint Center (IC3) 2024; Author calculations.*

5 "2024 BBB Scam Tracker Risk Report." https://bbbmarketplacetrust.org/riskreport2024/.
6 Global Anti-Scam Alliance, "State of Scams in the U.S." https://www.gasa.org/_files/ugd/2594f1_3d99d0490aa74d49bab2f-8d4af327928.pdf.

BUILDING A NATIONAL ESTIMATE

THE FOUNDATION: WHAT WE KNOW FOR CERTAIN

According to the FBI's IC3, the total monetary losses reported by Americans to law enforcement from online scams and crimes totaled $16.6 billion in 2024, marking a 33% increase from the previous year.[7] The FTC's Consumer Sentinel Network, operating independently, documented $12.5 billion in fraud losses, representing a 25% increase.[8]

While some victims likely reported to both agencies, we use the higher IC3 figure as our baseline. It represents the more comprehensive dataset, because: (1) it specifically focuses on internet-enabled crimes most relevant to our analysis, and (2) its value points to a more comprehensive capture of online fraud and crime incidents, whereas FTC's lower figure reflects its more narrow mandate focusing largely on consumer fraud in particular. We detail this choice in our methodology section of this report.

The critical next question becomes: ***what percentage of actual fraud gets reported to authorities?***

MEASURING UNDERREPORTING

The challenge of measuring unreported crime has long plagued researchers, but the Bureau of Justice Statistics provides crucial insights into fraud reporting behavior through its comprehensive 2017 Supplemental Fraud Survey, which examined fraud experiences across a nationally representative sample of 51,200 adults aged 18 or older. The most significant finding from this nationally representative study points to a dramatic underreporting problem: **only 14% of financial fraud victims reported the incident to authorities**.[9]

This finding aligns with common sense: most fraud victims don't report their experiences to law enforcement, whether due to embarrassment, belief that nothing can be done, or uncertainty about where to report.

This also aligns with other research findings on this question:

The Stanford Center on Longevity, a research institution concerned with thriving in old age, is focused on this issue because older Americans are particularly vulnerable to fraud. They reviewed multiple surveys, and found that **reporting rates for fraud generally fall between 20% and 50%, which would mean that 50% to 80% of fraud remains unreported**. Stanford researchers also noted methodological challenges in fraud research, finding "compelling evidence that many survey participants under-report their experience as victims" and they state **"There is also compelling evidence that many survey participants under-report their experience as victims, with some error rates as high as 78%."**[10]

Additional supporting evidence comes from a 2024 survey by IPX1031, a financial services company specializing in real estate exchanges. The survey found that when Americans encounter scam attempts, **57% do not report these incidents to relevant authorities**—meaning only **43% do take some form of reporting action**. Among the 30% of Americans who were victimized in the past year, the average monetary loss per incident was $1,600. While this 43% reporting rate is higher than the BJS law enforcement reporting rate, it likely reflects initial contacts with **various authorities** (including customer service, banks, or consumer agencies) **rather than formal police reports specifically**.[11]

7 Federal Bureau of Investigation, "2024 Internet Crime Report," Internet Crime Complaint Center, 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
8 Federal Trade Commission, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024," March 10, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.
9 Bureau of Justice Statistics, "Financial Fraud in the United States, 2017," U.S. Department of Justice, 2019, https://bjs.ojp.gov/library/publications/financial-fraud-united-states-2017.
10 Stanford Center on Longevity, "Prevalence," 2016, https://longevity.stanford.edu/prevalence/.
11 "Fraud and Identity Theft in America 2024 Statistics," IPX1031, 2024, https://www.ipx1031.com/fraud-and-identity-theft-in-america/.

Another more recent study shows very similar under-reporting:

From a 2023 FTC report to Congress on fraud targeting the elderly: "'Because the vast majority of frauds are not reported, these numbers include only a fraction of older adults harmed by fraud.' **Based on their underreporting research, the FTC estimated that 2022's actual fraud losses reached $137.4 billion compared to just $9 billion in reported losses—indicating that official statistics capture less than 7% of true fraud costs.**[12]

Additionally, the 2025 GASA survey of US consumers examined both online and offline scams in the United States. In a nationally representative survey of 2,500 adults, the group found that while 82 percent of victims said they reported incidents to a payment provider and 74 percent reported to the platform where the scam took place, **only about one in 10 said they notified law enforcement** such as local or national police.[13]

Lastly, the FBI IC3 director Donna Gregory has estimated that IC3 complaints **represent only 10 to 12 percent of victims**, an 8.3× to 10× multiplier. And some academic and survey analyses have observed reporting rates as low as 4 to 5 percent, which would imply multipliers in the 20–25× range.[14]

Taken together, all of these sources tell a similar story:

Table 1. Comparison of Underreporting Estimates

Source	Study Year	What Was Measured	Reporting Rate	Underreporting Rate (1 - Reporting Rate)	Key Notes
Bureau of Justice Statistics	2017	Incidents reported to law enforcement authorities	**14%**	**86%**	Large national survey (51,200 adults); one of the most rigorous government studies
IPX1031 Survey	2024	Incidents reported to "relevant authorities"	**43%**	**57%**	Nationally representative survey of 2,500 adults; broader definition includes banks, customer service; 30% victimization rate
FTC Survey Research	Ongoing (data for estimate from 2017, published 2020)	Incidents reported to government agencies	**2.6%**	**97.4%**	Specifically government agencies; includes mass market scam and cybercrime victims
FTC Loss Analysis	2022	Captured in official statistics	**~7%**	**~93%**	Based on $9B reported vs $137.4B estimated actual losses
GASA 2025	2025	Survey of US consumers	**~10%**	**~90%**	Reporting rate to law enforcement by consumer scam victims
IC3 Director	2018	All online scams and crimes	**~10%**	**~90%**	Quoted Estimate

12 Federal Trade Commission, "Protecting Older Consumers 2022-2023: A Report of the Federal Trade Commission," October 18, 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf.

13 Global Anti-Scam Alliance, "State of Scams in the U.S.," 2025, https://www.gasa.org/_files/ugd/2594f1_3d99d0490aa74d49bab2f-8d4af327928.pdf.

14 "An 'Iceberg' of Unseen Crimes," The New York Times. https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html.

While specific reporting rates vary depending on the type of authority and methodology used, all research consistently shows that the vast majority of scam and crime incidents go unreported to official channels, with law enforcement reporting rates appearing to be particularly low.

WHY WE CHOSE THE BJS 14% REPORTING RATE FOR OUR WORK

As listed above, multiple authoritative sources indicate that online crime reporting rates may be far lower than the BJS's 14% figure. However, despite this evidence from more recent research, we deliberately chose the BJS 14% rate for several methodological reasons.

The BJS study remains one of the most comprehensive, nationally representative surveys specifically measuring reporting to law enforcement, and its methodology most closely aligns with our application to **law enforcement reporting** databases like IC3. This is in contrast to other studies that examine reporting to various government agencies (i.e., FTC Survey Research), such as consumer protection services, or that deal exclusively with specific populations like the elderly (i.e., Stanford Center on Longevity). Importantly, the BJS findings align with more recent under-reporting rates from later studies (i.e., GASA 2025).

As we referenced above, we stick with this earlier, lower underreporting estimate to ensure that our analysis and methodologies consistently errs on the side of caution.

CALCULATING THE TRUE NATIONAL COST OF ONLINE SCAMS AND CRIMES

As we calculate the cost of scams, we have to move from counting **how often** scams are reported to estimating **how much money** is actually lost—including unreported cases.

The studies outlined in **Table 1** provide evidence for how frequently fraud and scam incidents go unreported. It is important to keep in mind that this is distinct from the dollar losses that go unreported, as different types of scams and crimes have different reporting rates and large-dollar scams may be more likely to be reported. Nevertheless, we apply the same 14 percent overall reporting rate (a 7.1× under-reporting multiplier) **to dollar losses**. This assumes that the incident reporting rate is the same as the dollar-loss reporting rate, an assumption we want to make transparent. We argue why this is a justifiable assumption in Appendix A.

So, applying the BJS 14% reporting rate to the IC3's $16.6 billion in 2024 losses yields an estimated **$119 billion** as the true annual cost of online scams and crimes. This is about **7.1 times higher than official estimates, and costs each American an average of about $349 per year (using the 2024 Census estimate of approximately 340 million residents).**

Our $119 billion estimate reflects only ***direct* losses by people in the United States to online scams and crimes**. Even if this were the actual amount of losses (rather than the low end of the range) these figures, dramatic as they may seem, likely still understate the cost of online fraud and crime due to other factors that are much more difficult to quantify and are **not accounted for** in this estimate, including:

- **Indirect costs:** administrative and legal fees, lost productivity, mental health treatment
- **Business losses:** Reputational losses from businesses reporting fraud (or not reporting for fear of a hit to their reputation)
- **International victims:** Cross-border frauds affecting Americans abroad (not included in our estimate which is limited to crimes where the victims are in the US)

These indirect costs are beyond the scope of this analysis, but evidence suggests they are substantial. **The LexisNexis Risk Solutions True Cost of Fraud Study 2025: North America report** found that for financial institutions, every dollar of direct fraud loss produced more than **five dollars in indirect losses**, including legal fees, underwriting costs and other expenses.[15]

15 LexisNexis Risk Solutions, "True Cost of Fraud Study 2025: North America," September 10, 2025, https://risk.lexisnexis.com/about-us/press-room/press-release/20250910-fraud-multiplier.

A recent nationally representative survey by the Pew Research Center provides further confirmation of the persistent gap between scam victimization and law enforcement reporting. According to an April 2025 Pew Research Center poll of U.S. adults who lost money to an online scam or attack, only 26 percent said they contacted law enforcement about the incident, while 74 percent did not report it.[16] Although this reporting rate is higher than other sources discussed, the findings reinforce the same pattern of underreporting.

CALCULATING "SCAMS ONLY" FROM IC3 DATA

For this report we purposefully track "scams and crimes" because **this matches the exact scope of the IC3 report coverage**. IC3 treats online scams and online fraud as the same underlying criminal activity—**deceptive schemes to steal money or property**. For readers interested in isolating only scam-based harms from other cybercrimes, the closest analog is what the IC3 report categorizes as "Cyber-Enabled Fraud." This is not precise, but is broadly illustrative of this category.

The IC3's "Cyber-Enabled Fraud" category encompasses 333,981 complaints totaling **$13.7 billion** in losses, representing what the general public would consider "online scams."[17] This category includes traditional fraud schemes facilitated by internet technology, such as investment fraud, business email compromise, tech support scams, romance fraud, and government impersonation schemes.

Applying the BJS 14% reporting rate to IC3's $13.7 billion in cyber-enabled fraud losses yields an estimated **$97.9 billion in annual online scam costs**—still approximately 7.1 times higher than reported, or **$288 per American per year**.

Under this accounting, online **scams** represent **83% of all reported IC3 "scams and crimes" losses**, with the remaining 17% attributed to cyber threats like ransomware, data breaches, and malware attacks.

The rest of this report looks at the full scope of all "online scams and crimes" the IC3 tracks.

SOME STATES ARE HIT HARDER THAN OTHERS

GEOGRAPHIC CONCENTRATION OF LOSSES

While online scams and crimes affect every corner of America, their impact is far from evenly distributed. **The top ten states by IC3 reported losses account for 50.37% of all reported fraud nationwide in 2024**.

This 1.35× overconcentration likely reflects several factors: these states include major financial centers (New York), technology hubs (California, Washington), large elderly populations (Florida, Arizona), and generally higher wealth levels that become magnets for scammers.

The IC3's state-by-state data shows a clear hierarchy of online fraud and crime impact, with California bearing the heaviest burden at $2.54 billion in reported losses, or 15.3% of the national total. Texas follows with $1.35 billion (8.1%), then Florida with $1.07 billion (6.5%). But these reported figures, sobering as they are, dramatically understate the harm inflicted in each state.

CALCULATING TRUE STATE-LEVEL LOSSES

Applying our methodology to individual states exposes the scope of unreported online fraud and crime. In doing so we assume that the dynamics that drive underreporting nationally—embarrassment, confusion about where to report, lack of faith in recovery—do not vary significantly by state.

California is the state with the highest reported losses at $2.5 billion. But, when adjusting for underreporting, California's actual estimated losses for 2024 stand at $18.1 billion. This means California alone actually suffers online fraud and crime losses more than the entire reported national total.

16 Pew Research Center, "Online Scams and Attacks in America Today," July 31, 2025, https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/.

17 Federal Bureau of Investigation, "2024 Internet Crime Report," Internet Crime Complaint Center, 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

The human impact becomes clearer when expressed per capita: every California resident, from newborns to centenarians, loses about $460 on average annually, based on the Census Bureau's Vintage 2024 population estimate of 39.4 million. This is money that could otherwise support local businesses, fund retirements, or provide for families.

While California, Texas, and Florida lead in total losses, smaller states often bear a heavier burden relative to population. In 2024, Nevada ($588 per resident), Wyoming ($530), and the District of Columbia ($2,965) experienced the highest per-capita scam and cybercrime losses, far exceeding the national average of roughly $288 per American per year.

THE TOP 10 STATES: A DETAILED ANALYSIS

Here are the top ten states identified by the IC3 reported losses, and the calculation of their actual losses to cybercrime and online fraud, and per capita estimates:

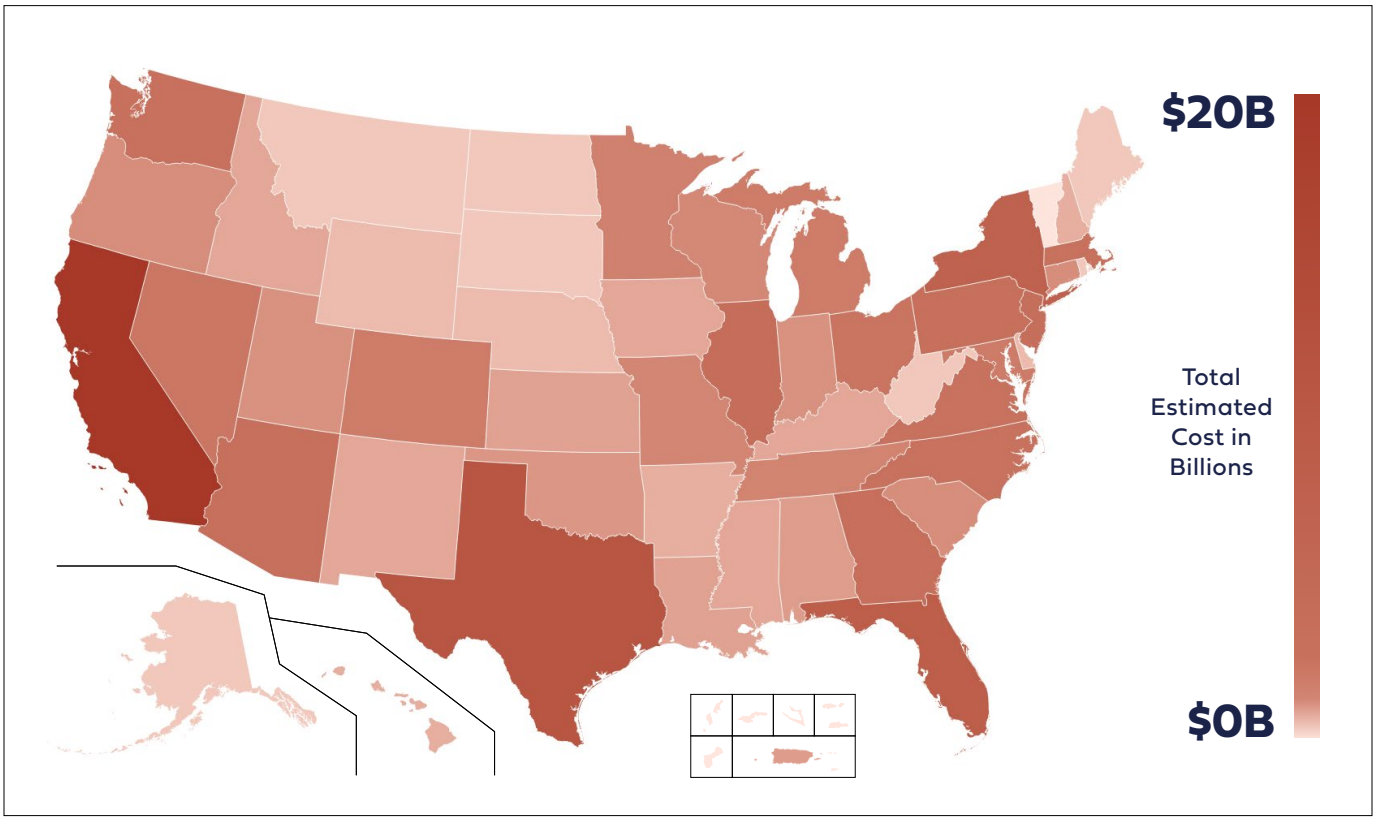
Table 2. Top 10 States by Losses to Online Scams and Crimes

Rank	State	IC3 Reported 2024 Losses	% of National Losses	Estimated True Losses	Estimated True Losses Per Capita
1	California	$2,539,041,635	15.30%	$18.1 billion	$460
2	Texas	$1,351,598,183	8.14%	$9.7 billion	$309
3	Florida	$1,071,909,632	6.46%	$7.7 billion	$328
4	New York	$903,975,003	5.45%	$6.5 billion	$325
5	Illinois	$479,054,271	2.89%	$3.4 billion	$269
6	New Jersey	$434,856,424	2.62%	$3.1 billion	$327
7	Georgia	$420,454,472	2.53%	$3.0 billion	$269
8	Pennsylvania	$400,082,312	2.41%	$2.9 billion	$220
9	Arizona	$392,441,717	2.36%	$2.8 billion	$370
10	Washington	$368,203,209	2.22%	$2.6 billion	$330
	Total of Top 10 States Combined	**$8,361,616,858**	**50.37%**	**$59.8 billion**	

Sources: *FBI Internet Crime Complaint Center (IC3); US Census Bureau; Author calculations.*

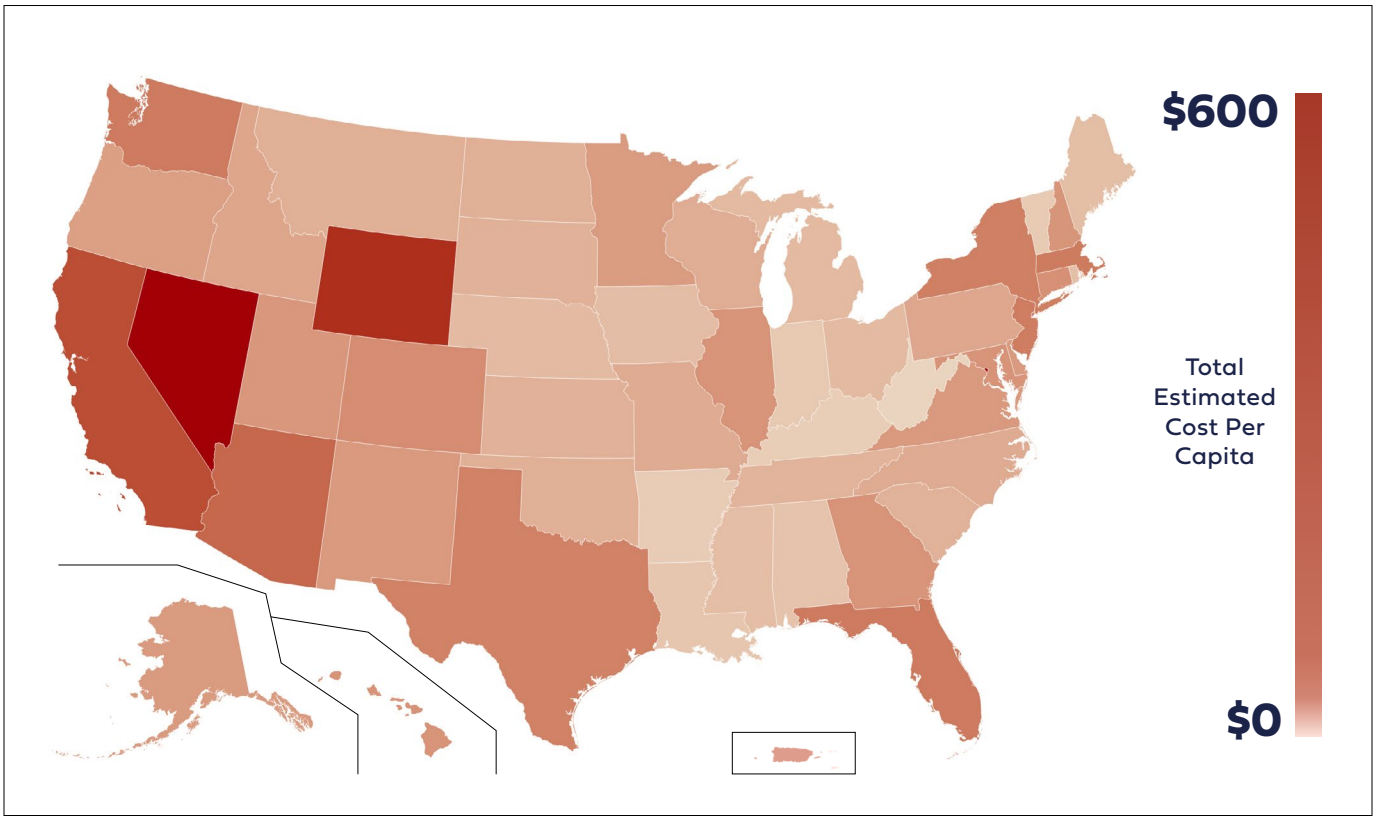
Note: *IC3's published state-by-state tables do not allocate every reported loss to an individual state. A portion of total losses appears in IC3's national data under aggregated, cross-jurisdictional, or unassigned categories. Because of this, the sum of state-level losses is smaller than the national total, and the two numbers should not be expected to match exactly.*

Figure 3. Estimated Total of Online Scam and Crime Losses for All States and Territories



Sources: *FBI Internet Crime Complaint Center (IC3) 2024; Author calculations.*

Figure 4. Estimated Total of Online Scam and Crime Losses for All States and Territories Per Capita



Sources: *FBI Internet Crime Complaint Center (IC3) 2024; U.S. Census Bureau; Author calculations.*

KEY STATE HIGHLIGHTS

Below we describe the losses in these key states in more-depth, and speculate on some of the reasons why these states are among the most affected.

California: With true losses of $18.1 billion, California bore the heaviest burden in absolute as well as per-capita terms (among the top 10 states) in 2024. The state's unique combination of factors—a massive population, high wealth concentration in the San Francisco Bay area and Southern California, large immigrant communities sometimes targeted by specialized scams, and a sizable elderly population—creates a perfect storm for online fraud and crime victimization. The $459 per capita loss represents not just individual tragedies but a massive drain on the state's economy.

Texas: Texas experienced an estimated $9.7 billion in true online fraud and crime losses in 2024, equating to per-capita losses of roughly $309. The state's rapid population growth, thriving business sector, growing elderly population, and large rural areas where victims may be isolated from support services all contributed to its second-place ranking. The contrast between the reported $1.35 billion and the real $9.7 billion losses highlights how severely official statistics undercount the impact of online fraud and crime.

Florida: Florida's $7.7 billion in true losses (≈$328 per capita) reflects its large elderly population, who are disproportionately targeted by scammers and criminals. The state's status as a retirement destination means that sophisticated online fraud and crime rings specifically target Florida residents with tech support scams, romance frauds, and government imposter schemes designed to exploit older adults' propensity for trusting authority figures, discomfort with technology, and sometimes diminished capacity to detect deception.

New York: New York suffered $6.5 billion in true online fraud and crime losses (equalling about $325 per capita). The concentration of wealth in Manhattan, combined with a diverse population that scammers target with culturally-specific schemes, drives these losses. The state's historical status as the country's center of banking and finance paradoxically makes it both more aware of the machinations of online fraud and crime and more attractive to fraudsters seeking high-value targets.

The Remaining States: Illinois ($3.4 billion), New Jersey ($3.1 billion), Georgia ($3.0 billion), Pennsylvania ($2.9 billion), Arizona ($2.8 billion), and Washington ($2.6 billion) round out the top 10, each suffering billions in losses–dwarfing their reported figures.

We list all US states and territories in **Appendix C** of this report.

ADDITIONAL STATE IMPACTS BEYOND THE TOP 10

Michigan: Michigan, with reported losses of $241.7 million, faced true losses estimated at $1.73 billion. Michigan's manufacturing base and its high population of auto industry retirees create unique vulnerabilities to employment scams and pension-related online fraud. The state's roughly $170 per capita loss impacts Detroit's urban communities and rural Upper Peninsula residents alike.

Colorado: Colorado's reported $243.5 million in losses translates to approximately $1.74 billion in true online fraud and crime costs. With a per-capita loss of **roughly $291**, the state's thriving tech sector based in the Denver and Boulder areas attracts elaborate investment scams, while its outdoor recreation culture sees targeted frauds around outdoor equipment sales and travel bookings. The state's relatively affluent, educated population paradoxically makes residents confident they won't fall for scams, potentially reducing reporting rates.

South Carolina: South Carolina experienced true losses of approximately $1.05 billion, based on reported losses of $146.5 million. The state's ~$191 per capita impact hits retirement communities along the coast particularly hard. Charleston's historic charm and Hilton Head's resort culture attract scammers targeting both tourists and retirees who have migrated from northern states.

Nebraska: Nebraska's reported losses of $46.7 million indicate true losses approaching $334 million. With an approximately $166 per capita impact, the state's agricultural communities face unique scams around farm equipment, crop insurance, and agricultural subsidies. Omaha's

insurance industry concentration also attracts financial fraudsters, specifically going after both companies and individuals in the sector.

REGIONAL PATTERNS AND INSIGHTS

The geographic distribution of online fraud and crime losses reveals important patterns. The top 10 states collectively experienced $59.8 billion (50.37% of the national total) in true losses, with the same share of reported losses. The remaining states and territories experienced an estimated $59.2 billion in true losses. While their individual burdens may be smaller in absolute terms, the per-capita impact in some smaller states can be dramatic. States with predominantly rural populations often face unique challenges: fewer resources for fraud prevention, less awareness of sophisticated scams, and a greater pride in independence that fraudsters can exploit (and that contribute to underreporting of scams).

The concentration of losses in wealthy states like California isn't merely a function of population. The 1.26× overconcentration (50.37% of losses from 40% of population) reflects these states being deliberately targeted by fraudsters who follow Willie Sutton's famous logic about robbing banks: "go where the money is." Tech entrepreneurs and investors in California and Texas, retirees in Florida and Arizona, and the financial sector in New York all represent rich hunting grounds for online fraud and crime operations.

TOP ONLINE SCAMS TYPES WITH REPORTED AND TRUE COST ESTIMATES

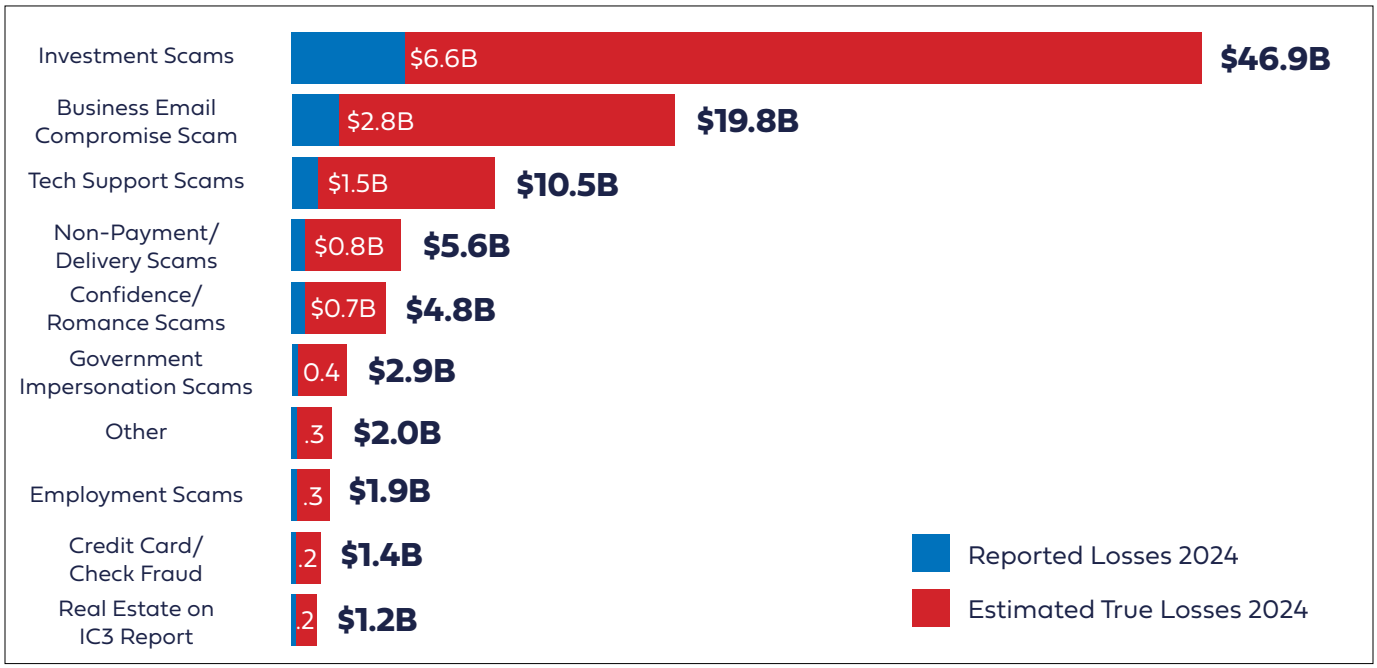
In **Table 3** we isolate the top scam/fraud types, as shown by IC3 reporting, with estimates of the true costs nationally. In estimating the actual costs, we assume that each online scam type has an underreporting rate equal to the overall underreporting rate of 14% from the Bureau of Justice Statistics used throughout this report. Future research should better measure underreporting rates by category so we can further refine our estimates of losses by scam and crime type.

Table 3. Top 10 Online Scam and Crime Types by Losses

Rank	Type	Description	Reported Losses 2024	Estimated True Losses 2024
1	Investment Scams	Fake investment/crypto schemes inducing victims to send funds	$6.6B	$46.6B
2	Business Email Compromise Scam	Spoofed/compromised business or personal email accounts to redirect payments	$2.8B	$19.7B
3	Tech Support Scams	Scammers posing as tech/security support to gain remote access or extract money	$1.5B	$10.4B
4	Non-Payment/ Delivery Scams	Victim pays for goods/services never delivered (fake sellers/marketplace scams)	$0.8B	$5.6B
5	Confidence/ Romance Scams	Trust/relationship scams (romance, family, friends) used to solicit money	$0.7B	$4.7B
6	Government Impersonation Scams	Fraudsters impersonate IRS/SSA/other officials to coerce payments or personal information	$0.4B	$2.9B
7	Other	Miscellaneous cyber-enabled scams and crimes not elsewhere categorized	$0.3B	$2.0B
8	Employment Scams	Fake job offers/scams requiring upfront payments or money-moving schemes	$0.3B	$1.9B
9	Credit Card Fraud and Scams	Unauthorized use of credit/debit cards or card numbers to obtain goods/funds	$0.3B	$1.9B
10	Real Estate/Rental Scams	Fraudulent listings, title/escrow scams, or fake landlords/sellers	$0.2B	$1.5B

Sources: *FBI Internet Crime Complaint Center (IC3); Author calculations.*

Figure 5. Top 10 Online Scam and Crime Types by Losses



Sources: *FBI Internet Crime Complaint Center (IC3); Author calculations.*

KEY OBSERVATIONS ON TOP SCAMS

A handful of cyber-enabled crime and scam categories dominate the scam economy. **Investment fraud and business email compromise (BEC)** together account for more than half of all reported financial losses. When adjusted for underreporting using the 7.1× multiplier, these two alone likely represent more than $66 billion in actual losses in just 2024 alone.

Investment scams, driven primarily by cryptocurrency schemes, exploit the promise of quick wealth to siphon away vast sums. BEC attacks, by contrast, often target businesses directly, rerouting wire transfers or invoices and draining millions of dollars in a single incident.

Other leading fraud categories reveal how scammers exploit both **trust in institutions** and **emotional vulnerabilities**. Tech support scams and government impersonation schemes prey on victims' belief in the authority of the IRS, or other trusted entities. Employment scams dangle the hope of opportunity while turning victims into unwitting money mules. Romance and confidence scams, meanwhile, wreak their own kind of havoc. They rely not on technical sophistication per se, but on deeply personal emotional manipulation, often leaving victims ashamed and less likely to report their losses.[18]

The IC3 data also highlights the split between **high-dollar-low-volume scams** and **low-dollar-high-volume scams**. Investment, BEC, and real estate scams pull in enormous sums per incident, while non-delivery and employment fraud accumulate losses across tens of thousands of smaller complaints.

Together, they show that the scam economy thrives at both ends of the spectrum — by targeting businesses with high-stakes transfers and by exploiting individuals in everyday digital transactions.

Again, the scale of underreporting cannot be ignored. Reported losses for the top fraud categories total around $13 billion, but actual losses are likely closer to $95 billion when applying the underreporting multiplier. This gap

18 AARP, "7 Tactics Criminals Use To Perpetuate Scams Against You," Nov. 11, 2022, https://www.aarp.org/money/scams-fraud/seven-criminal-tactics/.

underscores how embarrassment, fear, and lack of awareness keep many victims silent — particularly in romance fraud and other emotionally manipulative schemes. The result is that the scam economy is both far larger and more complex than illustrated by official statistics alone.

PLATFORM-SPECIFIC SOURCES OF ONLINE SCAMS

While the FBI's Internet Crime Complaint Center (IC3) is invaluable for assessing the scale and typology of cyber-enabled frauds, it has limitations in identifying which specific online platforms or channels—such as social media, marketplaces, or apps—are used by scammers. The IC3 reporting format is organized by crime category (investment scams, business-email compromise, tech-support scams, etc.), not by platform. Complainants rarely—and often cannot—specify which website, app, or service was used in the scheme. As a result, IC3's published data do not systematically break out fraud by "Platform X vs. Platform Y."

We also are not aware of any systematic research quantifying the full scope of online scams that **directly generate revenue for major platforms**, whether through paid advertising, revenue-sharing programs, or monetized scam content.

However, major news outlets have begun to expose this dynamic. The *New York Times* reported on October 1st, 2025, that political advertising scams involving deepfakes and misleading paid content were circulating on Facebook and Instagram.[19] The *Wall Street Journal* also documented similar scam activity across Meta-owned platforms on May 15th, 2025: "One late 2024 document reviewed by the Journal shows that the company will allow advertisers to accrue between eight and 32 automated "strikes" for financial fraud before it bans their accounts. In instances where Meta employees personally escalate the problem, the limit can drop to between four and 16 strikes."[20]

Internal company documents reviewed by Reuters and published on November 6 show that Meta Platforms projected roughly 10 percent of its 2024 revenue — about $16 billion — would come from ads promoting scams and banned goods. Meta disputes this figure, stating that the true number is lower, but has not provided its own figure. The documents estimate Meta's platforms serve about 15 billion "higher-risk" scam advertisements every day. And enforcement appeared to be very limited: only when automated systems were at least 95 percent certain an advertiser was fraudulent would the account be banned. In other cases, Meta allowed offenders to keep running ads, sometimes charging them a premium "penalty bid" fee. Internal assessments indicated Meta's sites were involved in about one-third of successful scams in the United States, while U.K. regulators found Meta products linked to 54 percent of all payments-related scam losses, more than all other social platforms combined. One internal memo also showed Meta's ad-vetting team was directed not to take actions that would cost the company more than 0.15 percent of revenue — about $135 million — even though scam-related ads were generating many billions in income.[21]

Beyond this reporting, what we do know from the Federal Trade Commission, Federal Bureau of Investigation, and Better Business Bureau relating to online advertising and online scams and crime is this:

In the FTC's Consumer Sentinel Network Data Book 2023, among fraud reports where a contact method was identified, **13%** began with an **online ad or pop-up** (median reported loss **$168**), while **15%** began on **social media** (median reported loss **$341**).[22]

Similarly, in the **BBB's 2024 Scam Tracker Risk Report, *online ad* was cited by roughly 12 to 15 percent of respondents as their first point of contact**. The BBB found that scams initiated through ads carried higher trust and conversion rates, as consumers were more likely to click

19 "Facebook's Political Ads: Deepfakes and Scams," The New York Times, October 1, 2025, https://www.nytimes.com/2025/10/01/technology/facebooks-political-ads-deepfakes-scams.html.

20 "Meta Fraud on Facebook and Instagram," The Wall Street Journal, May 15, 2025, https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8.

21 "Meta is Earning Fortune from a Deluge of Fraudulent Ads, Documents Show," Reuters, November 6, 2025, https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

22 Federal Trade Commission, *Consumer Sentinel Network Data Book 2023* (Washington, DC: Federal Trade Commission, February 2024), "Fraud Reports by Contact Method," https://www.districtcreditunion.com/wp-content/uploads/2024/08/CSN-Annual-Data-Book-2023.pdf.

ads appearing to come from known brands or local businesses.

The FTC's 2024–2025 annual report to Congress shows a sharp rise in high dollar fraud against older adults, driven by investment scams, romance fraud, and impersonation schemes. Older adults reported that investment scammers often targeted them on social media, and the FTC **notes that consumers of all ages report social media as the most common method of contact for investment scams**. Given that investment scams now generate more losses for older adults than any other fraud category, the prominence of social media as a contact channel underscores the growing role that social platforms play in high dollar fraud against seniors.

The FTC also found that scams initiated on social media produced both the highest number of loss reports and the highest aggregate losses among older adults in 2024, surpassing phone calls, email, websites, and all other contact methods.

Older adults reported losing nearly $561 million to scams that began on social media, a figure that has increased nearly ninefold since 2020. This marks the first time the FTC has identified social media as the leading contact method for fraud affecting adults 60 and older, both in volume and in total dollars lost.[23]

Neither the FTC, IC3, nor BBB quantify how much platform revenue—through paid advertising, revenue-share programs, or monetized views—stems from scam content. Further, none estimate the financial gain to platforms versus the losses to victims.

However, the BBB's 2024 *Scam Tracker Risk Report* did ask victims to indicate **which online platforms were involved in their scam experience**.[24] Because respondents could select multiple platforms, the percentages exceed 100 percent in aggregate. These figures do not represent dollar losses per platform, but instead reflect how often each platform was flagged by victims in their reports.

GASA's State of Scams USA 2025 further shows that 81% of scam attempts in the U.S. occurred on platforms with a Direct Message function, and social media was identified as a contact channel in 32% of scam attempts.

Figure 6. All Scams Compared to Scams With a Reported Monetary Loss by Means of Contact

Percentage of all scams and scams with a monetary loss do not add up to 100% because the "other" category was not included.

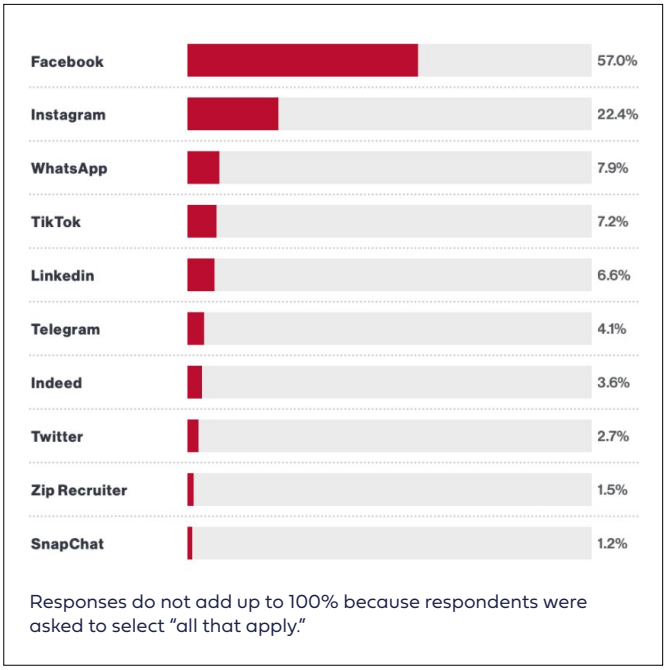
Source: *Better Business Bureau Scam Tracker Risk Report (2024).*

23 Federal Trade Commission, "Protecting Older Consumers, 2024–2025: A Report of the Federal Trade Commission," December 2025, https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.

24 Better Business Bureau. 2024 BBB scam tracker risk report. BBB Institute for Marketplace Trust. https://bbbmarketplacetrust.org/riskreport2024/.

The GASA 2025 report notes that: "Gmail, Facebook, and Instagram were most frequently associated with scams, X (Twitter), Snapchat, and Telegram were cited as the slowest to respond to scam reports," and they note that: "over half (57%) say they saw no discernible action taken by the platform in response."[25] The BBB report concurs that Facebook and Instagram are two of the platforms most frequently associated with scams. In fact, according to the BBB, the top three reported online platforms are all Meta-owned products: Facebook (57.0%), Instagram (22.4%), and WhatsApp (7.9%).[26] For more details on the top reported platforms, see **Figure 7**.

Figure 7. Top Reported Online Platforms



Source: *Better Business Bureau Scam Tracker Risk Report (2024).*

POLICY RECOMMENDATIONS: ADDRESSING THE TRUE COST OF SCAMS AND PLATFORM ACCOUNTABILITY

As discussed in the report, the true cost of scams is far greater than what is currently reported. Current data also indicate that social media is the leading scam vector, but existing research from the FTC and FBI has limitations in identifying which specific online platforms are used for scams. Exposing the true scope of these losses underscores an urgent need for greater transparency and clear accountability across the digital ecosystem The following recommendations outline steps to ensure platforms strengthen fraud detection and reporting systems, and ultimately take responsibility for preventing scams before they reach consumers.

STRENGTHENING REPORTING AND TRANSPARENCY REQUIREMENTS

The lack of transparency across platforms makes it difficult to see the full picture of scam activity or hold bad actors accountable for their role in consumer harm. Platforms often know how scams spread and how much revenue they generate (as revealed by the Reuters reporting on internal Meta documents discussed above), but these data points are not systematically disclosed publicly or to regulators. The following recommendations outline steps to ensure greater reporting and transparency:

1. **Mandatory Scam Loss and Incident Reporting By Platforms:** Online platforms (social media, messaging / texting apps, online marketplaces) should publish to all interested researchers, quarterly reports disclosing:

25 Global Anti-Scam Alliance, "State of Scams in the U.S.," 2025. https://www.gasa.org/research/.
26 "2024 BBB Scam Tracker Risk Report," Better Business Bureau Institute for Marketplace Trust, February 2025, https://bbbmarketplacetrust.org/riskreport2024/.

- Total number of scams and type of scam incidents reported by users
- Number of fraudulent ads or accounts removed including those proactively taken down by the platform and average response times
- Repeat offenders or known scam networks identified

2. **Centralized Reporting to Regulators:** Online platforms should submit scam and fraud data to regulators including the FTC, FBI, and state attorneys general. Data should include:
   - Number and type of scam facilitated
   - Platform response actions (ad or account removals, policy changes, etc.)

3. **Transparent Ad Verification and Due Diligence:** Online platforms should verify the identity, business registration, and payment information of all advertisers before approving ads similar to Know Your Customer rules in the financial sector.

CREATING SAFER DESIGN FEATURES ON PLATFORMS

Online platforms provide few default protections for users and make little effort to detect and prevent fraudulent activity. In many cases, platforms are designed in a way that allow criminals to target vulnerable users with fraudulent activity. The recommendations below would create safeguards that mitigate design features bad actors exploit online to spread scams:

1. **Stronger Privacy and Security Settings for Users:** Platforms should provide users with stronger default privacy settings and implement data minimization practices that limit exposure to unsolicited messages, financial solicitations, or unknown advertisers.

2. **Detect and Prevent Fraudulent Activity:** Platforms should detect and prevent the creation of fraudulent profiles and pages through stronger identity verification and pattern detection tools. Accounts that will be used for commercial purposes should go through enhanced verification.

3. **Empowering Users to Report Fraud:** Users often lack the ability to report fraudulent content, and even when they do, platforms frequently fail to respond. To empower users to report fraud, platforms should establish a fraud reporting system including a clearly visible 'Report Scam' button on all content that could contain advertisements, commercial, or promotional material. Platforms should also acknowledge receipt of user-submitted scam reports and provide updates on actions taken within a reasonable timeframe.

MORE DATA FROM FTC AND FBI IC3 REPORTS

The **FTC's Consumer Sentinel Data Book** and the **FBI's Internet Crime Complaint Center (IC3) Report** are foundational to understanding the scope and scale of online scams and cyber-enabled crime in the United States.

(We also applaud the work done by non-governmental organizations like the Better Business Bureau and Global Anti-Scam Alliance, all of which we cite in this report.)

While the FTC has estimated the degree of under-reporting of scam losses in special reports to Congress, calculating, for instance, that 2022's reported $9 billion represented only about 7% of actual losses,[27] neither the FTC's standard annual Consumer Sentinel report nor the FBI's IC3 report adjusts its published figures for under-reporting.

Both continue to rely on raw, self-reported incidents and losses without consistent cross-agency definitions.

To strengthen national visibility into the real scale and economics of digital fraud, we recommend that future FTC and FBI IC3 reporting include the following:

27 Federal Trade Commission, "Protecting Older Consumers, 2023–2024: A Report of the Federal Trade Commission," October 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf.

1. **Adjusted Estimates of Under-Reporting**
   - **Develop and publish methodologically sound estimates of under-reporting for both:**
     - **Incidence rates of scams and cyber-enabled crimes**
     - **Dollar losses associated with those crimes**
   - Break down under-reporting estimates by scam type, U.S. state, and key **demographic groups (age, gender, income, education, and other relevant characteristics).**

2. **Standardized Definition of "Cyberfraud"**
   - Establish a **shared, detailed definition** of *cyberfraud* or *"cyber-enabled fraud"* across both FTC and FBI IC3 reporting.
   - Ensure consistent categorization of online scam types, including investment, romance, business-email compromise, tech-support, and social-media scams.

3. **Robust State-Level and Demographic Loss Data**
   - Continue publishing **state-level loss data**, but move beyond reported totals to include **statistically adjusted estimates** that reflect likely true losses, including both incident rate under-reporting and dollar loss under-reporting for each category and for the whole.
   - Include **demographic cross-tabs** showing how different age and income groups are affected by specific scam types.

4. **Analysis of Platform-Linked Harms and Revenues**
   - Include detailed information on both the digital platforms that were used in the inception of a crime or scam, but also any digital platform that played any secondary role in executing the crime or scam.
   - Include estimates or case studies of **digital platform revenues** linked to scams or frauds, such as:
     - Ad-share, referral fees, or traffic revenue from scam-related activity
     - Monetization pathways on social platforms, ad networks, and AI-driven services that indirectly profit from scam exposure
   - The FTC in particular should publicly release findings from its inquiry into scam ads and fraudulent activity on major platforms. This would help quantify how **online platform design and incentives** intersect with national scam losses.

CONCLUSION: THE HIDDEN AMERICAN CRISIS

Online scams and crimes in America represent more than a criminal justice issue, they represent a hidden economic crisis — draining an estimated $119 billion annually from citizens and communities and putting it in the pockets of perpetrators of these crimes. Official statistics capture only one-seventh or ***less*** of the true impact of online fraud and crime.

Research consistently shows that social media platforms are the biggest source of attacks. For some scams and crimes, social media platforms directly profit via advertising revenue, revenue splits and monetized content.

California's $18.1 billion in estimated annual losses exceeds the entire budget of many federal agencies. Texas's $9.7 billion annually is money that is leaving the state economy and going into the black market. Florida's $7.7 billion annual loss represents thousands of retirees' life savings evaporating into the hands of criminals. Other smaller states and territories see per capita losses that are grievously harmful. Across all 50 states, the pattern repeats: high levels of unreporting masking economic devastation.

The path forward requires acknowledging the real scope and scale of online scams and crimes. The $16.6 billion in reported losses for 2024 from the FBI that triggered headlines represents merely the visible portion of a much larger crisis. By understanding that losses approach or likely exceed $119 billion—that every American effectively pays a $348 annual "online scam tax"—we can begin marshaling resources proportionate to the threat.

The criminals perpetrating these scams and crimes count on our collective silence—on victims being too embarrassed to report, on authorities being too overwhelmed to investigate, and on society being too distracted to notice $119 billion disappearing each year. Breaking that silence, armed with evidence-based estimates of what the real cost is, represents our best hope for protecting all Americans.

As long as the true cost of the scam economy goes unreported, fraudsters are empowered to claim more victims. Statistics are underestimated, which leads to under-resourced responses. However, every accurate assessment of online fraud and crime's scope—like the $119 billion calculated here—builds momentum toward the comprehensive response this crisis demands.

APPENDIX A: METHODOLOGY

Because empirical research on the true economic costs of online scams remains relatively new, our approach draws from other emerging domains where direct measurement is limited and under-reporting or definitional gaps require modeled extrapolation.

Similar assumption-based frameworks are standard in fields such as cybercrime economics,[28] technology-impact forecasting,[29] and artificial-intelligence labor-market modeling.[30] In each case, researchers transparently identify key assumptions, anchor estimates to peer-reviewed baselines, and interpret results as lower-bound estimates rather than precise point predictions. Our methodology adheres to those same principles.

STEP 1: BASELINE DATA COLLECTION

We begin with one of the most comprehensive official datasets available: the FBI's Internet Crime Complaint Center (IC3) 2024 annual report. This database represents the primary federal repository for cybercrime and fraud complaints from American victims.
The IC3 received 859,532 total complaints in 2024, of which 256,256 reported actual financial losses totaling **$16.6 billion, a 33% increase from the previous year**. The FBI report itself cites an average loss of **$19,312 per complaint** across all complaints, including those with no reported dollar loss. If we calculate only among the 256,256 complaints that included a documented dollar amount, **the average rises to $64,782 per case with losses**. Both measures are accurate and differ because they use different denominators.

These figures serve as our foundation because they represent verified complaints with specific loss amounts, providing the most reliable baseline for extrapolation.

Per-capita figures throughout this report are calculated using the U.S. Census Bureau's Vintage 2024 state population estimates (July 1, 2024), ensuring consistency across all states and territories.

This report presents estimates based on available data and acknowledged methodological limitations. Figures should be considered approximations for policy discussion purposes.

DATA SOURCE SELECTION: IC3 VS. FTC

While both the FBI's Internet Crime Complaint Center (IC3) and the Federal Trade Commission (FTC) collect fraud loss data, we use IC3's $16.6 billion figure as our baseline rather than the FTC's $12.5 billion for several methodological reasons consistent with our approach:

First, the Bureau of Justice Statistics (BJS) reporting rate that forms the foundation of our methodology was derived from surveys about crime reporting to law enforcement agencies. The IC3, as an FBI-operated system, more closely aligns with the law enforcement reporting context of the original BJS study than the FTC's consumer protection database.

Second, we use the IC3 figure ($16.6B) because it captures a broader set of internet-enabled crimes, including business-targeted losses, whereas the FTC's $12.5B is limited to consumer fraud. This yields a larger baseline number, but our approach is still conservative in the sense that we deliberately adopt the higher BJS reporting rate (14%), which produces the smallest multiplier. In this report, "conservative" means anchoring assumptions on the lower bound of credible research to avoid inflating results.

STEP 2: REPORTING RATE APPLICATION

The Bureau of Justice Statistics 2017 Supplemental Fraud Survey, based on a nationally representative sample of 51,200

28 Sasha Romanosky, "Examining the Costs and Causes of Cybercrime," Journal of Cybersecurity 2, no. 1 (2016): 121–135; Ross Anderson et al., "Measuring the Changing Cost of Cybercrime," The Journal of Cybersecurity 5, no. 1 (2019): tyz002.
29 Erik Brynjolfsson and Andrew McAfee, Machine, Platform, Crowd: Harnessing Our Digital Future (New York: W. W. Norton & Company, 2017).
30 Daron Acemoglu and Pascual Restrepo, "The Wrong Kind of AI? Artificial Intelligence and the Future of Labor Demand," Cambridge Journal of Regions, Economy and Society 13, no. 1 (2020): 25–35.

adults aged 18 and older, found that only 14% of financial fraud victims reported incidents to police.[31] This represents the most comprehensive government study of fraud reporting behavior available.

We applied this reporting rate directly to the IC3 baseline using the following formula:

Estimated True Losses = Reported Losses ÷ Reporting Rate

Estimated True Losses = $16.6 billion ÷ 14% = $119 billion

Multiplier = 7.1×

To illustrate sensitivity: if only 10% (10× multiplier) of victims reported, total losses would reach about $166 billion; if 20% (5× multiplier) reported, the figure would be about $83 billion. Our choice of 14%—drawn from the Bureau of Justice Statistics survey most analogous to IC3 data—falls within this credible range.

Our $119 billion estimate should be understood as a floor—not the absolute minimum possible, but the lowest estimate supported by credible reporting-rate data and deliberately cautious assumptions. The true cost is likely much higher.

NOTE: INCIDENT-BASED VS. DOLLAR-BASED UNDERREPORTING ESTIMATES

The 14 percent reporting rate we apply throughout the report is based on incidents of fraud reported to law enforcement, not the share of total dollar losses reported. In practice, larger-loss victims may be more likely to report, which means the real dollar-based reporting rate could differ. **However, there is no established national estimate that reliably quantifies that difference.** Because the incident-based figure from the Bureau of Justice Statistics is the most rigorous and directly aligned with IC3 reporting practices, we also use it to estimate true dollar losses. For more information, including how **external studies support this decision** see **Appendix B**.

STEP 3: STATE-LEVEL APPLICATION

The Bureau of Justice Statistics reporting data reflect national averages but does not provide state-level breakdowns. Due to this limitation, we apply the national reporting rate (14%) uniformly across all states as a **necessary methodological simplification**. Regional variations in fraud awareness, law enforcement resources, or reporting culture may affect actual multipliers. **Therefore, these estimates should be considered reasonable approximations grounded in evidence rather than precise calculations. Future research should examine reporting rates by geography, so that we can further refine our estimates of losses.**

31 Bureau of Justice Statistics, "Financial Fraud in the United States, 2017."

APPENDIX B: VALIDATION AGAINST OTHER STUDIES AND DATA

Several independent data points help validate our estimates and support the conclusion that annual online fraud and crime losses are well above officially reported figures. We do not add these to our $119B estimate. Instead, they provide external validation that our floor estimate is reasonable and aligns with other independent methods. These include:

UNITED STATES SOURCES

AARP's 2023 report:

AARP found that older Americans lose an estimated $28.3 billion annually to financial exploitation, a figure cited by the National Council on Aging and other government sources.[32] Importantly, this estimate covers all elder financial exploitation, much of it offline, but it underscores the plausibility of tens of billions lost each year among older adults alone.

FBI IC3 data:

FBI IC3 data consistently shows that victims aged 60+ account for about 30% of reported fraud dollar losses.[33] While we do not directly scale AARP's offline-inclusive figure to the national total, the fact that both sources independently point to older Americans absorbing tens of billions annually reinforces our conclusion that overall losses, at all ages, easily exceed $100 billion.

IPX1031 Survey:

A 2024 national consumer survey by IPX1031 asked adults to self-report scam victimization. It found 30% of adults were scam victims and losses averaged $1,600 per adult.[34]

When we use the U.S. Census Bureau's Vintage 2024 Population estimate of approximately 267 million adults, applying a 30% victimization rate and an average loss of $1,600, this implies roughly $128.2 billion in annual scam losses. This is comparable with our findings.

While this survey-based approach is not peer-reviewed, its different methodology provides independent validation of our $119 billion estimate. This convergence across very different methods underscores the robustness of our findings.

Pew Research Survey:

Additional evidence from Pew Research Center underscores the continued low rate of reporting to law enforcement. In a nationally representative April 2025 survey, Pew found that only 26 percent of adults who lost money to an online scam said they contacted the police, while 74 percent did not.[35] Because this statistic reflects only individuals who experienced a direct financial loss, it may overstate reporting relative to the full universe of fraud victims. Nonetheless, the result remains directionally consistent with other law enforcement based reporting measures, including the BJS's 14 percent rate and similar estimates from GASA, FTC analyses, and IC3 leadership, and strengthens the conclusion that the actual law enforcement reporting rate is far below 50 percent and that our use of the 14 percent BJS figure remains a conservative baseline.

Federal Trade Commission:

In 2022, the FTC estimated that it captured only about 7% of consumer fraud victims, implying that actual consumer losses that year were on the order of $137.4 billion.[36] This figure largely reflects consumer fraud only, it excludes the business-targeted crimes that IC3 captures, but it uses a similar extrapolation logic to ours, reinforcing the conclusion that reported figures represent only a fraction of the actual national cost, consistent in scale with our findings.

The FTC's new estimate that older adults reported $2.4 billion in fraud losses in 2024, including

32 "AARP Report: $28.3 Billion a Year Stolen from Adults 60+," AARP, June 15, 2023, https://states.aarp.org/colorado/aarp-report-28-3-billion-a-year-stolen-from-adults-60.
33 Federal Bureau of Investigation, "2024 Internet Crime Report."
34 "Fraud and Identity Theft in America 2024 Statistics," IPX1031.
35 Pew Research Center, "Online Scams and Attacks in America Today."
36 Federal Trade Commission, "Protecting Older Consumers 2022-2023," 40.

$561 million from scams that began on social media, fits cleanly within our national loss model. Older adults account for roughly one-fifth of all reported fraud losses, so scaling their $2.4 billion to reflect the 14 percent reporting rate used in this report implies true losses of about $17 billion among Americans aged 60 and older, a figure that falls well within the FTC's own underreporting range of $10.1 billion to $81.5 billion. We expect this number to be less than the IC3 figure as the FTC only focuses on consumer fraud, while the IC3 includes all online scams and crimes.

In short, the FTC's new numbers further support the conclusion that our $119 billion estimate represents a lower bound estimate of the true scale of harm.[37]

GASA (U.S. Findings):

The Global Anti-Scam Alliance's 2025 State of Scams in the U.S. report provides another important reference point on reporting behavior. They studied both online and offline scams in the U.S. Their nationally representative survey of 2,500 adults found that while 82 percent of victims said they reported scams to a payment service and 74 percent reported to the platform where the scam occurred, only about 10 percent reported to law enforcement. Another 9 to 12 percent said they told a consumer protection authority or national reporting site, but overall fewer than one in five victims reported to any kind of government authority.[38] This finding aligns closely with the Bureau of Justice Statistics' 2017 Supplemental Fraud Survey (14 percent reporting rate to law enforcement),[39] which we used in this report.

Their findings of total cost of scams-only in the U.S. also is in line with our findings. GASA's $64.8B and our $97.9B "scams-only" estimate both show that scam losses are vastly larger than the FBI's $13.7B official number. The difference between them reflects methodology, GASA's survey caps extreme losses, while ours incorporates the high-dollar categories visible in IC3 data. Taken together, they provide strong, independent validation of the true cost of online scams.

Academic Research (U.S. focused)

A 2020 analysis by economist Keith B. Anderson[40] drew on three nationally representative FTC-sponsored surveys (2005, 2011, 2017) and found that only 44.6% of victims complained to anyone beyond friends or family, and that fewer than 3% reported to a government agency, with only 2.3% contacting the Better Business Bureau.[41] These findings track our estimate that a low percentage of fraud victims report to authorities and reinforce the conservative nature of our approach (a 14% reporting rate vs. less than 5%).

FinCEN Statement (U.S. focused)

A December 2024 interagency statement from the U.S. Department of the Treasury, joined by the Federal Reserve, CFPB, FDIC, NCUA, and OCC, cited recent research estimating that older Americans lose about $28.3 billion annually to financial exploitation.[42] Separately, FinCEN reported that financial institutions filed 155,415 suspicious activity reports related to elder financial exploitation between June 2022 and June 2023, associated with more than $27 billion in flagged suspicious activity.[43] By comparison, IC3's 2024 data showed only $4.8 billion in reported losses among victims aged 60+ (albeit for a different timeframe). Since older adults typically account for about 30% of total fraud dollar losses, FinCEN's findings point to the likelihood that real national fraud losses are several times larger than IC3's $16.6 billion overall figure, consistent with our under-reporting projection and our $119 billion estimate.

37 Federal Trade Commission, "Protecting Older Consumers, 2024–2025."
38 Global Anti-Scam Alliance, "State of Scams in the U.S."
39 Bureau of Justice Statistics, "Financial Fraud in the United States, 2017."
40 Keith B. Anderson, "To Whom Do Victims of Mass-Market Consumer Fraud Complain?" SSRN, 2021, https://doi.org/10.2139/ssrn.3852323.
41 Keith B. Anderson, "To Whom Do Victims of Mass-Market Consumer Fraud Complain?" SSRN, 2021.
42 "AARP Report: $28.3 Billion a Year Stolen from Adults 60+."
43 Financial Crimes Enforcement Network, "Financial Trend Analysis: Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023," April 2024, https://www.fincen.gov/sites/default/files/shared/FTA_Elder_Financial_Exploitation_508Final.pdf.

IC3 Leadership Validation: (U.S. Focused)

Donna Gregory, long-time Unit Chief of the FBI's Internet Crime Complaint Center (IC3), told The New York Times in 2018 that the complaints received by IC3 represented only about 10–12% of all estimated cybercrime victims in the United States.[44] Applying Gregory's estimated reporting rates to 2024's $16.6 billion in IC3-reported losses would suggest annual losses of $138–166 billion, with a midpoint around $152 billion. This implies an 8.3× to 10× multiplier, pointing to potentially greater underreporting than our lower 7.1× estimate.

INTERNATIONAL SOURCES

CSEW: (UK Focused)

The UK Crime Survey for England and Wales (CSEW) provides additional validation for low fraud reporting rates. The CSEW found that about 15% of fraud incidents were reported to Action Fraud or the police, implying a reporting multiplier of about 6.7×.[45] This multiplier is broadly consistent with our multiple of 7.1× and if we had applied this UK multiplier to the U.S. baseline of $16.6 billion in reported losses, it would yield approximately $111 billion in total losses. However, the studies cited in this report are not all focused on the exact same data. The CSEW figure covers all fraud, including offline schemes, while our U.S. baseline is drawn from IC3 data, which is concerned strictly with internet-enabled fraud and crime.

ACCC / Scamwatch: (Australia Focused)

Australia shows a similarly severe underreporting gap. The Australian Competition and Consumer Commission's Scamwatch program has repeatedly found that it captures **less than 13 percent** of Australians' total scam losses. In its annual "Targeting Scams" reports, the ACCC compares Scamwatch data with losses reported by banks, payment platforms, and large-scale national surveys, and estimates that actual losses are roughly **eight times** higher than the official totals. **This 8× dollar-loss underreporting multiplier is fully consistent with the international pattern** and supports the plausibility of a high U.S. multiplier.[46]

CAFC: (Canada Focused)

Canada's national fraud statistics reflect a similar pattern. The Canadian Anti-Fraud Centre (CAFC) has found that officially reported losses capture **less than one-fifth** of the true national scam burden when compared with survey-based estimates produced by the Competition Bureau and the Canadian Bankers Association. **This implies a five-fold underreporting multiplier, which closely mirrors those observed in Australia and the United Kingdom and is coherent with the 7.1 multiplier we use.**[47]

CONCLUSION FOR DOLLAR-LOSS REPORTING RATE CHOICE

The convergence of evidence across multiple independent methodologies—internal cross-checks, institutional analyses, direct population surveys, and international comparisons—provides robust support for using the BJS 14% incident reporting rate as a baseline proxy for dollar-loss underreporting.

44 "An 'Iceberg' of Unseen Crimes," The New York Times.

45 Office for National Statistics, "Nature of Fraud and Computer Misuse in England and Wales: Year Ending March 2019," August 24, 2020, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019.

46 Australian Competition and Consumer Commission, "Targeting Scams: Report of the National Anti-Scam Centre on Scams Activity 2024," 2024, https://www.scamwatch.gov.au/system/files/targeting-scams-report-2024.pdf.

47 Canadian Anti-Fraud Centre, "2024 Annual Statistical Report," 2025, https://antifraudcentre-centreantifraude.ca/annual-reports-2024-rapports-annuels-eng.htm.

APPENDIX C: DATA ON ALL US STATES AND TERRITORIES

Important Note on State Totals: The IC3's state-level tables do not include all reported losses. Approximately 17 to 18 percent of the national IC3 total is categorized as multi-state, cross-jurisdictional, or unassigned, and therefore does not appear in state-specific records. As a result, the sum of state-level losses in Appendix C is smaller than the national loss total used elsewhere in this report. Because these unassigned losses cannot be allocated to states, the state-level estimates presented here should be interpreted as conservative figures.

Table A-1: Reported and Estimated Total of Online Scam and Crime Losses for All States and Territories

Rank	State/Territory	IC3 Reported 2024 Losses	% of National Losses	Estimated True Losses	Per Capita (approx)
1	California	$2,539,041,635	15.30%	$18.1B	$460
2	Texas	$1,351,598,183	8.14%	$9.7B	$309
3	Florida	$1,071,909,632	6.46%	$7.7B	$328
4	New York	$903,975,003	5.45%	$6.5B	$325
5	Illinois	$479,054,271	2.89%	$3.4B	$269
6	New Jersey	$434,856,424	2.62%	$3.1B	$327
7	Georgia	$420,454,472	2.53%	$3.0B	$269
8	Pennsylvania	$400,082,312	2.41%	$2.9B	$220
9	Arizona	$392,441,717	2.36%	$2.8B	$370
10	Washington	$368,203,209	2.22%	$2.6B	$330
11	Massachusetts	$338,872,378	2.04%	$2.4B	$339
12	North Carolina	$324,287,947	1.95%	$2.3B	$210
13	Virginia	$317,406,595	1.91%	$2.3B	$257
14	District of Columbia	$291,531,458	1.76%	$2.1B	$2,965
15	Ohio	$278,038,028	1.67%	$2.0B	$168
16	Nevada	$268,769,310	1.62%	$1.9B	$588

Rank	State/Territory	IC3 Reported 2024 Losses	% of National Losses	Estimated True Losses	Per Capita (approx)
17	Colorado	$243,517,403	1.47%	$1.7B	$291
18	Michigan	$241,737,979	1.46%	$1.7B	$170
19	Maryland	$238,976,904	1.44%	$1.7B	$273
20	Minnesota	$203,352,530	1.23%	$1.5B	$251
21	Tennessee	$190,271,310	1.15%	$1.4B	$187
22	Missouri	$183,751,987	1.11%	$1.3B	$210
23	Wisconsin	$169,942,495	1.02%	$1.2B	$204
24	South Carolina	$146,468,765	0.88%	$1.0B	$191
25	Oregon	$144,160,344	0.87%	$1.0B	$241
26	Connecticut	$143,884,002	0.87%	$1.0B	$280
27	Utah	$129,414,310	0.78%	$0.9B	$264
28	Indiana	$125,093,323	0.75%	$0.9B	$129
29	Oklahoma	$113,724,886	0.69%	$0.8B	$198
30	Alabama	$103,771,880	0.63%	$0.7B	$144
31	Puerto Rico	$91,363,707	0.55%	$0.7B	$204
32	Louisiana	$87,411,457	0.53%	$0.6B	$136
33	Kansas	$80,300,908	0.48%	$0.6B	$193
34	New Mexico	$76,621,670	0.46%	$0.5B	$257
35	Kentucky	$73,919,940	0.45%	$0.5B	$115
36	Iowa	$72,860,333	0.44%	$0.5B	$161
37	Mississippi	$65,613,936	0.40%	$0.5B	$159

Rank	State/Territory	IC3 Reported 2024 Losses	% of National Losses	Estimated True Losses	Per Capita (approx)
38	Idaho	$63,035,342	0.38%	$0.5B	$225
39	Hawaii	$55,180,901	0.33%	$0.4B	$273
40	New Hampshire	$52,811,455	0.32%	$0.4B	$268
41	Arkansas	$51,714,039	0.31%	$0.4B	$120
42	Nebraska	$46,730,894	0.28%	$0.3B	$166
43	Wyoming	$43,502,744	0.26%	$0.3B	$530
44	Delaware	$37,611,598	0.23%	$0.3B	$255
45	Montana	$31,603,407	0.19%	$0.2B	$198
46	Maine	$31,455,797	0.19%	$0.2B	$160
47	Alaska	$26,296,803	0.16%	$0.2B	$254
48	South Dakota	$24,957,446	0.15%	$0.2B	$193
49	West Virginia	$24,196,661	0.15%	$0.2B	$98
50	Rhode Island	$23,597,036	0.14%	$0.2B	$152
51	North Dakota	$21,831,953	0.13%	$0.2B	$196
52	Vermont	$11,285,112	0.07%	$0.1B	$124
53	Guam	$2,532,544	0.02%	$0.0B	---
54	Virgin Islands, U.S.	$1,441,830	0.01%	$0.0B	---
55	U.S. Minor Outlying Islands	$1,107,380	0.01%	$0.0B	---
56	American Samoa	$195,182	0.00%	$0.0B	---
57	Northern Mariana Islands	$121,874	0.00%	$0.0B	---

Notes: *Per-capita omitted where data unavailable for small territories.*
Sources: *FBI Internet Crime Complaint Center (IC3) 2024; U.S. Census Bureau; Author calculations.*

APPENDIX D: REFERENCES

AARP. (2023, June 15). *AARP report: $28.3 billion a year stolen from adults 60+*. https://states.aarp.org/colorado/aarp-report-28-3-billion-a-year-stolen-from-adults-60

Acemoglu, D., & Restrepo, P. (2020). The wrong kind of AI? Artificial intelligence and the future of labor demand. *Cambridge Journal of Regions, Economy and Society*, 13(1), 25–35. https://academic.oup.com/cjres/article/13/1/25/5738870

Anderson, K. B. (2021). *To whom do victims of mass-market consumer fraud complain?* SSRN. https://doi.org/10.2139/ssrn.3852323

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2019). Measuring the changing cost of cybercrime. *The Journal of Cybersecurity*, 5(1), tyz002. https://academic.oup.com/cybersecurity/article/5/1/tyz002/5370281

Better Business Bureau. (2025, February). *2024 BBB scam tracker risk report*. BBB Institute for Marketplace Trust. https://bbbmarketplacetrust.org/riskreport2024/

Brynjolfsson, E., & McAfee, A. (2017). *Machine, platform, crowd: Harnessing our digital future.* W. W. Norton & Company. https://wwnorton.com/books/9780393254297

Bureau of Justice Statistics. (2019). *Financial fraud in the United States, 2017.* U.S. Department of Justice, Office of Justice Programs. https://bjs.ojp.gov/library/publications/financial-fraud-united-states-2017

Federal Bureau of Investigation. (2025). *2024 internet crime report*. Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Federal Trade Commission. (2023, March 2). *FTC issues orders to social media and video streaming platforms regarding efforts to address surge in advertising scams*. https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-issues-orders-social-media-video-streaming-platforms-regarding-efforts-address-surge-advertising

Federal Trade Commission. (2023, October). *Protecting older consumers 2022–2023: A report of the Federal Trade Commission*. https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf

Federal Trade Commission. (2024, October 1). *FTC issues annual report to Congress on the agency's actions to protect older adults*. https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults

Federal Trade Commission. (2025, March 10). *New FTC data show a big jump in reported losses to fraud to $12.5 billion in 2024*. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

Federal Trade Commission. (2025, December). *Protecting older consumers, 2024–2025: A report of the Federal Trade Commission*. https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf

Financial Crimes Enforcement Network. (2024, April). *Financial trend analysis: Elder financial exploitation: Threat pattern & trend information, June 2022 to June 2023*. https://www.fincen.gov/sites/default/files/shared/FTA_Elder_Financial_Exploitation_508Final.pdf

Global Anti-Scam Alliance. (2025a). *State of scams in the U.S.* https://www.gasa.org/_files/ugd/2594f1_3d99d0490aa74d49bab2f8d4af327928.pdf

Global Anti-Scam Alliance. (2025b, October 15). *Scams total $64 billion in losses and impact 7 in 10 Americans, finds State of Scams USA 2025 report.* PR Newswire. https://www.prnewswire.com/news-releases/scams-total-64-billion-in-losses-and-impact-7-in-10-americans-finds-state-of-scams-usa-2025-report-302570885.html

IPX1031. (2024). *Fraud and identity theft in America 2024 statistics.* https://www.ipx1031.com/fraud-and-identity-theft-in-america/

Office for National Statistics. (2020). *Nature of fraud and computer misuse in England and Wales: Year ending March 2019.* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019

Pew Research Center. 2025. *Online Scams and Attacks in America Today.* July 31. https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/

Reuters. (2025, November 6). *Meta is earning fortune from a deluge of fraudulent ads, documents show.* https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

Romanosky, S. (2016). Examining the costs and causes of cybercrime. *Journal of Cybersecurity*, 2(1), 121–135. https://academic.oup.com/cybersecurity/article/2/1/121/2367098

Stanford Center on Longevity. (2016). *Prevalence.* https://longevity.stanford.edu/prevalence/

The New York Times. (2018, February 5). An 'iceberg' of unseen crimes: Many cyber offenses go unreported. https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html

UK Finance. (2024, May 22). *Annual fraud report 2024.* https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024

UK Finance. (2025, May 27). *Fraud continues to pose a major threat with over £1 billion stolen in 2024.* https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2025-press-release

ConsumerFed.org