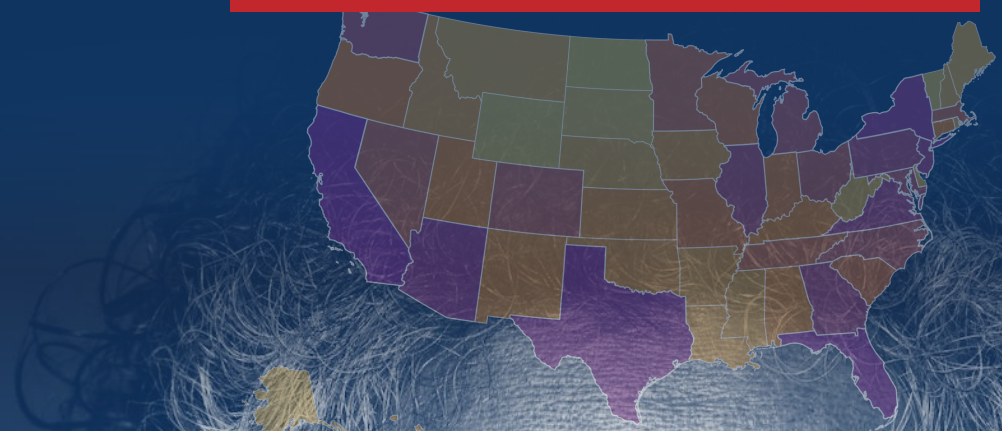
STOLEN TRUST

Billions stolen from Americans 60 and over.
Almost none made whole.

AMERICA'S ELDER FRAUD LANDSCAPE



★ ★ ★ ★ ★

Published by seniors.hcsk.org · Independent nonprofit analysis

SPECIAL STUDY 2026

Table of Contents

Key Findings

Reported elder fraud reached $7.748 billion in 2025 (FBI IC3, adults 60+), up from $1.685 billion in 2021, a +360 percent five-year increase and eight times the 2020 figure of $966 million. Recovery turns on catching the money within hours, and most reports never reach a federal channel that fast. America has the agencies, the laws, and the data. What this study finds it lacks is a single front door, a single message, and a single clock. Three findings point to the same gap. Chapter 9 sets out a coordinated response we believe could help: the Three Ones.

THE PROBLEM: A FRAGMENTED RESPONSE	CHAPTER 9'S PROPOSED RESPONSE
1 Fragmented intake Ten federal actors handle elder fraud, most through their own hotline, portal, or form. None is dysfunctional. None is the front door.	**One Front Door** One national number to call and one website to report, 24/7.
2 Inconsistent messaging Anti-fraud advice is borrowed from cybersecurity and misses the real threat, which is manipulation, not technical exploitation. Seniors get no single rule to fall back on.	**One Message** Federal and state agencies adopt one protective rule, *Think First, Verify Always.*
3 Speed mismatch A fraudulent wire can be frozen only if it is reported within hours, but most reports never reach a federal channel that fast. Once the money clears, recovery is almost impossible.	**One Day** A 24-hour coordinated response standard: from agencies to family support.

Chapter 9 proposes a coordinated framework, the Three Ones, built from infrastructure that already exists.

Foreword

Yuksel Aydin
Founder & Director,

HCSK, Human Cybersecurity Knowledge for Seniors

About This Study

In 2025, Americans aged 60 and over reported $7.748 billion stolen to fraud. The FBI's Recovery Asset Team, the federal government's main tool for clawing money back, freezes about half the money in the cases caught in time, but almost no case reaches it that fast, so less than half of one percent of the stolen total was frozen. The country is not standing still: ten federal actors, dozens of state units, banks, and platforms fight elder fraud every day. America has the agencies, the laws, and the data.

Stolen Trust: A Special Study on America's Elder Fraud Landscape is published by HCSK Inc. (https://seniors.hcsk.org), a nonprofit resource focused on online scams targeting older adults, with a special focus on AI-enabled fraud.

Existing federal reports document important parts of the elder fraud crisis. The FBI publishes detailed data on cybercrime complaints. The FTC publishes thorough analysis of consumer fraud demographics. The Consumer Financial Protection Bureau publishes the leading federal framework on what financial recovery actually requires. The U.S. Senate Special Committee on Aging publishes a Fraud Book. Academic researchers produce valuable studies on specific aspects of the problem. Journalists cover individual cases with skill and empathy.

This study's contribution is to bring those parts together into one picture, the scale, the trajectory, the geography, the criminal mechanics, the human cost, and the structural reasons why so little stolen money is ever recovered (the FBI's recovery team freezes about half the money in the cases that reach it in time, but almost no case reaches a federal freeze that fast, so under one percent of 2025 losses was frozen) and to respectfully suggest a unifying response framework: the Three Ones.

The Three Ones

After eight chapters of analysis, Chapter 9 proposes a single coordinated framework, built from existing infrastructure, to address three findings about America's elder-fraud response: no single front door (a dozen actors and reporting sites, with no single number to call or website to visit), inconsistent protective messaging (cybersecurity-borrowed advice that does not address

manipulation-based scams), and a speed mismatch between how fast a fraudulent wire must be caught to be frozen and the response timeline.

Its three parts, **One Front Door**, **One Message** (*Think First, Verify Always*), and **One Day**, are set out in full in Chapter 9, after the evidence.

What We Did

This study integrates data from the federal and state actors profiled in Chapter 6 (which also maps a wider web beyond them) plus an original news corpus:

1. Six years of FBI IC3 data (2020–2025). The FBI's Internet Crime Complaint Center publishes annual elder fraud reports with state-level victim counts and financial losses across all major crime categories. We compiled, cleaned, and analyzed six years of this data plus the broader IC3 Annual Reports for the same period, spanning 2020 through 2025, from $966 million in 2020 to $7.748 billion in 2025 in reported losses by victims aged 60 and over (with 2021–2025 used as the canonical five-year growth window, +360 percent).

2. The FTC's *Protecting Older Consumers* report (December 2025) plus five years of Consumer Sentinel Network Data Books (2020–2024). The Federal Trade Commission's annual analyses provide the federal government's most detailed demographic picture of how elder fraud operates, contact methods, payment methods, demographic breakdowns, and the FTC's $10.1B–$81.5B estimate of the true (underreporting-adjusted) overall cost of fraud to older adults.

3. Seven years of DOJ Elder Abuse Prevention and Prosecution Act (EAPPA) annual reports (2019–2025). The complete federal enforcement record: 283 enforcement actions in 2025 alone, 608 defendants, $2.36 billion stolen across more than one million victims.

4. Seventeen quarters of SSA Office of Inspector General Quarterly Scam Reports (Issues 2–18, July 2021–September 2025). Quarterly granularity on Social Security impersonation scam trends, including the dramatic decline from FY 2019–2021 peak volumes.

5. The CFPB's *Recovering from Elder Financial Exploitation* framework (September 2022), the leading federal analysis of what financial recovery actually requires: the four-stage process every victim must navigate, and the Trusted Contact framework this study builds on in Chapter 9.

6. FinCEN advisories, the September 2023 Pig Butchering Alert (FIN-2023-Alert005), the December 2024 FinCEN-impersonation alert (FIN-2024-Alert005), and the 2024 Financial Trend Analysis on Elder Financial Exploitation (documenting $27 billion in related Suspicious Activity Report filings June 2022 – June 2023).

7. The U.S. Secret Service Elder Fraud Advisory (April 2026), the U.S. Postal Inspection Service Annual Reports (FY 2023 and FY 2024), an HHS Office of Inspector General Special Fraud Alert (the March 1998 alert on nursing-home arrangements with hospices, a Medicare provider-side anti-kickback alert), and the U.S. Senate Special Committee on Aging's Fraud Books (2021, 2023, 2025).

8. An original news corpus of 1,910 articles (August 2025 – May 2026). Beginning in August 2025, we established daily monitoring of news coverage on elder fraud, senior scams, and related topics. Over ten months, this produced 1,910 unique articles from approximately 1,000 distinct news sources. Each article was categorized by scam type, theme, and geography. The corpus drives Chapter 5's news-analysis findings.

This study's contribution is to bring those parts together into one picture.

What This Study Is Not

This study is not a government publication. It is an independent nonprofit analysis with an explicit recommendation, not an annual report, designed to stand alone rather than open a series. It is built for this moment: we have aimed for one focused, evidence-led contribution to the public debate. It is an independent analysis produced by a nonprofit that tracks, analyzes, and explains elder fraud. Our aim is that this problem be understood, measured, and addressed in proportion to its severity.

How to Use This Study

If you are a policymaker: Chapters 1–2 provide the scale. Chapter 7 maps the legislative landscape. Chapter 9 sets out the study's proposed framework, the Three Ones, built on authority that already exists.

If you are a journalist: Chapter 5 provides a news-media meta-analysis built on 1,910 articles. Chapters 3–4 provide expertise for investigative or explanatory reporting. The state rankings in Chapter 2 provide local angles for every market in America.

If you are a law enforcement professional: Chapter 3 details criminal methods. Chapter 6 maps the full response (the family and community front line, state prosecutors, banks and platforms, and the federal and state agencies) and profiles the enforcement work and partnerships most relevant to your role.

If you are a financial institution: Chapter 1 traces the payment channels the money now moves through (bank transfers and cryptocurrency carry the largest losses) and the $27 billion your industry flagged through Suspicious Activity Reports in a single year of FinCEN review (June 2022 to June 2023). Chapters 3 and 4 detail the scam mechanics your customers face, from the four dominant fraud types to the AI voice-cloning and impersonation tactics now in active use. Chapter 9 proposes the One

Message (*Think First, Verify Always*) for voluntary adoption in customer-facing channels, and a One Day recovery standard.

If you are a caregiver or a family member of an older adult: Chapter 8 explains the human experience of fraud victimization. Chapter 9 presents the Three Ones framework, including the One Message (*Think First, Verify Always*) we propose for adoption.

If you are a senior: This website and this study were built for you. If a scam happens, a victim may feel ashamed or guilty. Please remember two things. First, former FBI and CIA Director William H. Webster has spoken publicly about being targeted by an elder-fraud scheme; if criminals targeted him, they can target anyone. Second, the person who was scammed is the victim. The blame belongs to the fraudster.

Acknowledgments

This study would not be possible without the public data published by the federal and state sources whose work is documented in the source archive.

The 1,000+ news sources whose journalism informed our analysis, from local television stations to international wire services, provide the daily record of elder fraud.

We acknowledge the individuals whose stories appear in these pages. Sharing one's experience of fraud requires courage, and their willingness to speak publicly makes prevention possible.

We welcome corrections, challenges, and additions from any reader, government official, researcher, journalist, or citizen. The data in this study is publicly available and our analysis is transparent. If we have made an error, we want to know about it.

Corrections, data submissions, and feedback: press@hcsk.org · https://seniors.hcsk.org

Published June 9, 2026.

CHAPTER 01

Chapter 1: The Numbers We Should Read Together

> *$7.748 billion, reported stolen from Americans aged 60 and over in 2025. 201,266 complaints. Up 59 percent in a single year, and roughly 360 percent in five.*

The Reports America Should Read Together

Every year, multiple federal agencies publish reports on fraud against older Americans. The FBI's Internet Crime Complaint Center (IC3) releases state-level data on cybercrime victims aged 60 and over. The Federal Trade Commission publishes a broader analysis of consumer fraud through its Sentinel Network. The Treasury Department's Financial Crimes Enforcement Network (FinCEN) publishes financial-institution suspicious-activity data. The Department of Justice publishes an annual EAPPA Report to Congress documenting federal enforcement. The Consumer Financial Protection Bureau publishes the principal federal framework on what financial recovery actually requires.

All of these reports are public. All are thorough. Reading them together brings an interesting view because each report answers questions the others don't.

The **FBI's IC3 data** tells you *where* elder fraud is happening. It provides victim counts and dollar losses for every state, broken down by crime type, going back to 2020: granularity no other federal source matches. What it does not capture is the scale of fraud that is never reported to it.

The **FTC's Sentinel data** tells you *how* elder fraud happens, and *how much stays hidden*. It provides the most detailed picture available of how scammers make contact and how victims pay, broken down by age, and, uniquely among these sources, it estimates the true scale of fraud that goes unreported. What it does not provide is state-level granularity.

The **FinCEN SAR data** tells you what *banks* are flagging, independently from victim reports. It corroborates or extends the official complaint data with what financial-institution monitoring detects.

The **DOJ's EAPPA reports** tell you what *federal prosecutors are doing about it*, and what fraction of the documented problem is being met with enforcement (detailed in Chapter 6).

The **CFPB's recovery framework** tells you what happens *after* the loss, and why so little of what is stolen is ever recovered.

This study brings these datasets together into a single picture. What that picture reveals is the subject of this chapter.

Five Years of Escalation

Between 2020 and 2025, the FBI's Internet Crime Complaint Center recorded elder fraud loss totals that increased more than eightfold, from $966 million in 2020 to $7.748 billion in 2025.

The growth has not been gradual. It has been steep and accelerating.

Year	Reported Complaints (60+)	Total Losses (60+)	Year-over-Year
2020	105,301	$966 million	
2021	92,371	**$1.685 billion**	+74%
2022	88,262	**$3.098 billion**	+84%
2023	101,068	**$3.428 billion**	+11%
2024	147,127	**$4.885 billion**	+43%
2025	201,266	**$7.748 billion**	+59%

Source: FBI IC3 Elder Fraud Reports 2020–2023 and IC3 Annual Reports 2024–2025. All categories of elder fraud combined.

Compound growth from 2021 to 2025: approximately +360 percent ($1.685B → $7.748B). Cumulative reported losses over the five years 2021–2025: over $20.8 billion.

The number of reported elder fraud complaints has nearly doubled in this period, rising about 91 percent (from 105,301 in 2020 to 201,266 in 2025). The total dollar losses have increased more than eightfold. And 2025 is the worst year on record by every measure.

The disparity between elder fraud and fraud against younger adults is stark. Adults aged 60 and over accounted for just 20 percent of all IC3 complaints in 2025 but 37 percent of all losses, $7.748 billion out of $20.877 billion (FBI IC3, *2025 Internet Crime Report*). Elder fraud losses grew 59 percent year-over-year, compared to 26 percent for all ages combined. Older adults are losing far more than their share of complaints would predict, a pattern consistent with their being targeted for higher-value schemes and with the greater assets many hold.

To put this in perspective: $7.748 billion spread across the 201,266 elder fraud complaints filed in 2025 averages about $38,500 per complaint. That average is pulled sharply upward by a small number of catastrophic losses; 12,444 complainants reported losing more than $100,000. A typical victim loses far less: the FTC puts the median loss for adults 60 and over near $900. And even $38,500 represents only what was *reported*, a fraction of the true cost.

What the FTC Adds: The Iceberg Beneath the Surface

While the FBI counts internet-related complaints filed with IC3, the FTC collects a broader universe of consumer reports through its Sentinel Network. In 2024, Sentinel received 6.5 million reports from

consumers of all ages. Of those, 2.6 million were about fraud, and 1.1 million were about identity theft. Total reported consumer fraud losses across all ages reached $12.8 billion in 2024 (FTC, *Protecting Older Consumers 2024-2025*, December 2025).

Among consumers aged 60 and over, the FTC documented nearly $2.4 billion in reported losses, up from approximately $600 million in 2020, a 300 percent increase (FTC, *Protecting Older Consumers 2024-2025*, December 2025).

One of the FTC's most important contributions to understanding elder fraud is what it estimates goes *unreported*.

The Reporting Gap

Research the FTC cites finds that just 4.8 percent of fraud victims report their experience to a government entity or the Better Business Bureau. Reporting rates vary dramatically by loss amount:

- 2.0 percent of victims who lost under $1,000 file a report
- 6.7 percent of victims who lost over $1,000 file a report

Even among those who do report, the oldest and most vulnerable victims often rely on others to do so. For adults aged 80 and over, 16 percent of fraud reports were filed by a third party (an adult child, spouse, or caregiver), the highest rate of any age group. The median loss in those third-party reports was $6,000, nearly four times the $1,650 overall median for that age group. This suggests that cases severe enough to come to a family member's attention involve substantially more money than what victims report on their own.

Yet the reporting data also reveals an important counternarrative: 74 percent of fraud reports filed by older adults indicated no monetary loss. Adults 60 and over were 62 percent more likely than younger adults to file a no-loss report, meaning they recognized the scam and reported it without losing money. Older Americans are not, as stereotype suggests, uniformly vulnerable. Many are vigilant and report fraud attempts even when they do not lose a cent. The crisis is not that seniors cannot detect fraud, it is that when fraud succeeds, the consequences are catastrophic.

Using these reporting rates to extrapolate from actual Sentinel data, the FTC estimates the true cost of fraud to older adults in 2024 falls between:

- $10.1 billion (conservative, assuming everyone who lost $10,000 or more reported)
- $81.5 billion (full extrapolation using research-based reporting rates)

Even the conservative estimate, $10.1 billion, is more than four times what older victims reported to the FTC ($2.4 billion). The $2.4 billion older adults reported is only about one-quarter of the FTC's most conservative true-cost estimate ($10.1 billion), and a far smaller share of its full research-based extrapolation ($81.5 billion). FinCEN's $27 billion in bank-flagged suspicious activity over a comparable period, discussed below, points the same way: the reported totals capture only a fraction of true losses.

The FinCEN Confirmation

A third federal data source corroborates the FTC's estimates, and suggests they may still be conservative.

The Treasury Department's FinCEN tracks Bank Secrecy Act (BSA) reports, predominantly Suspicious Activity Reports (SARs), filed by banks and financial institutions. Per FinCEN's *Financial Trend Analysis: Elder Financial Exploitation* (April 2024), between June 15, 2022 and June 15, 2023, financial institutions filed 155,415 elder-financial-exploitation reports worth more than $27 billion under the Bank Secrecy Act (banks accounted for 72 percent of those filings).

This figure represents what *financial institutions* flag as suspicious, not what victims report or what law enforcement investigates, but what automated monitoring systems and trained bank employees identify as potentially fraudulent activity involving older adults. Because it is bank-flagged suspicious activity rather than completed, adjudicated loss, FinCEN cautions it may include attempted as well as duplicate transactions, so it is not a dollar-for-dollar match with the FBI's reported losses. Even so, it shows banking-side detection registering fraud on a scale several times larger than the complaint data captures.

The CFPB Recovery Gap

A fourth federal data source completes the picture, by documenting what happens *after* the loss.

The FBI's Recovery Asset Team is the federal government's primary tool for clawing stolen funds back, and where it can act, it works: in the 642 elder-fraud cases reported fast enough for it to step in, it froze about half the money at risk ($32.9 million of $65.4 million). The limit is not the team's effectiveness but the system's reach. Only those 642 cases, out of 201,266 elder fraud complaints, reached the freeze window in time, so of the $7.748 billion lost by older Americans, less than half of one percent was frozen. The Consumer Financial Protection Bureau's *Recovering from Elder Financial Exploitation: A Framework for Policy and Research* (September 2022) traces this to a four-stage process every victim must navigate, from identification to reporting to investigation to the eventual return of funds, with different actors at each stage and no automatic handoff between them. Once a fraudulent transfer clears, the money is almost always gone.

Four federal data sources point the same way: the FBI's more-than-eightfold growth in reported losses, the FTC's iceberg estimate of unreported losses, FinCEN's banking-side detection of suspect activity, and the CFPB's documentation of post-loss recovery. Together they confirm one conclusion: the scale of elder fraud is enormous, the visible figure is a small fraction of the true total, and only a fraction of what is stolen is recovered.

What This Means in Human Terms

Research the FTC cites finds that only about 1 in 20 fraud victims ever files a report. The FBI and FTC count fraud through different channels, so no precise headcount is possible. But if anything close to

those reporting rates holds, the roughly 200,000 elder complaints the FBI logged in 2025 represent only a fraction of true victims, a rough signal that the real number runs into the millions, not the hundreds of thousands.

Each number represents a person, typically someone over 60, often living alone, frequently losing a significant portion of their retirement savings to a criminal who, in the vast majority of cases, is never identified or held to account.

The Concentration of Devastation

One of the most striking findings from the FTC data is how concentrated the financial damage is among a relatively small number of high-loss victims.

In 2024, across all ages, just 13 percent of consumers who reported a fraud loss lost $10,000 or more, yet their combined losses equaled 93 percent of all reported losses to the FTC's Sentinel Network. The number of older adults reporting losses over $100,000 has increased 351 percent since 2020, from 1,136 reports in 2020 to 5,125 in 2024. Reports in the $10,000–$100,000 tier also rose sharply, nearly tripling, from 6,965 to 19,679 (a 183 percent increase).

The FBI's IC3 data corroborates this concentration pattern. In 2025, the average loss per elder fraud complaint was $38,500, but this average masks enormous variance. Of the 201,266 elder complaints filed that year, 12,444 complainants reported losses exceeding $100,000. These high-loss victims, roughly six percent of all elder complainants, account for a disproportionate share of the $7.748 billion total.

These are not people losing $50 to a phishing email. These are retirees losing $200,000 to an investment scam. Widows wiring $75,000 to someone impersonating the FTC. Grandfathers handing $30,000 in cash to a courier they believe was sent by their bank.

The combined median loss for all adults 60 and over was $900 in 2024, up 38 percent from $650 the year before (FTC, *Protecting Older Consumers 2024-2025*). And the median rises sharply with age. The median loss for Americans aged 80 and over was $1,650 in 2024, far higher than any other age group. For those aged 70–79, the median was $1,000. For those aged 60–69, it was $691.

The older the victim, the more they lose.

How Scammers Make Contact

The FTC's Sentinel data reveals a critical shift in how scammers reach their victims, and it differs significantly by age group.

Social Media: The New Vector

In 2024, social media surpassed all other contact methods as the leading source of elder fraud by total reported losses. Older adults reported $561 million in losses from fraud initiated on social media platforms, a 44 percent increase from the previous year, with the median social media loss surging 91 percent year-over-year to $650. Losses to social-media-initiated fraud have increased nearly ninefold since 2020.

The highest aggregate losses from fraud that started on social media were on investment scams (51 percent of social-media-initiated losses) and romance scams (28 percent). By number of loss reports, however, the most common social-media fraud older adults reported was online shopping scams (31 percent).

Phone Calls: Highest Loss Per Victim

While social media generates more aggregate losses, phone calls remain the costliest contact method per victim: the $2,210 median loss is the highest of any channel the FTC tracks, more than three times the $650 median for social media fraud.

This disparity reflects the different nature of phone-based scams: they typically involve high-pressure impersonation of government agencies or financial institutions, targeting victims who are less active online but highly responsive to authoritative-sounding callers.

For Americans aged 80 and over, phone calls remain the dominant contact method by both total losses and number of reports, with social media a distant second.

Contact Method	Total Losses (60+)	Change from 2023	Median Loss
Social Media	$561M	+44%	$650
Phone Call	$502M	+24%	$2,210
Website or App	$303M	+45%	$272
Text Message	$183M	+41%	$1,560
Online Ad/Pop-up	$147M	+24%	$288
Email	$143M	+14%	$1,000

Source: FTC Consumer Sentinel Network, 2024. Adults aged 60 and over.

How Victims Pay: The Money Trail

Understanding how stolen money moves is essential for both prevention and recovery. The FTC data reveals that the most expensive payment methods for older adults are not the most commonly reported, a distinction with important implications.

Bank Transfers and Cryptocurrency: Where the Big Money Goes

Bank transfers accounted for the highest total losses by older adults at $832 million (up 24 percent from 2023), followed by cryptocurrency at $454 million (up 15 percent). Together, bank transfers and cryptocurrency were the two costliest payment methods for older adults, about $1.29 billion in losses, more than half of the nearly $2.4 billion older adults reported losing to the FTC in 2024.

Since 2020, elder fraud losses involving bank transfers have increased eightfold. Losses involving cryptocurrency have increased twentyfold. The broader IC3 data underscores cryptocurrency's dominance: total cryptocurrency fraud across all ages reached $11.4 billion from 181,565 complaints in 2025, making it the single highest-loss descriptor in IC3's 2025 all-ages data (cryptocurrency is a payment-method descriptor that spans multiple crime types, not a standalone crime category). Adults 60 and over bear a disproportionate share: 38 percent of all cryptocurrency losses ($4.35 billion, the IC3's combined Cryptocurrency and Cryptocurrency Wallet descriptor).

Gift Cards and Credit Cards: Most Frequently Reported

Despite generating lower total losses, credit cards (26 percent of loss reports) and gift cards (16 percent) were the payment methods most frequently reported by older adults. Gift cards remain the signature payment method for government impersonation scams, tech support scams, romance scams, and family impersonation scams.

Payment Method	Total Losses (60+)	Change from 2023	Share of Reports
Bank Transfer	$832M	+24%	11%
Cryptocurrency	$454M	+15%	10%
Cash	$156M	+57%	4%
Gift Card	$124M	+5%	16%
Check	$121M	+19%	3%
Wire Transfer	$105M	-16%	3%
Credit Card	$77M	+33%	26%
Payment App	$80M	+156%	14%

Source: FTC Consumer Sentinel Network, 2024. Adults aged 60 and over.

The rise of payment apps (+156 percent) and cash payments (+57 percent) signals that scammers are constantly adapting to evade fraud detection systems built around traditional wire transfers. Payment apps and money-transfer services, the kind used to send money directly to another person, were cited in 90,571 fraud reports across all ages in 2024, with losses totaling $391 million.

For older adults, the rapid adoption of payment apps combined with limited understanding of their irrevocable nature, has created a new vulnerability that did not exist five years ago.

The Combined Picture

When the FBI's state-level data, the FTC's national demographic data, FinCEN's banking-side detection data, and the CFPB's recovery-process documentation are read together, the same picture emerges from every angle:

1. The problem is growing faster than any response. Annual reported losses for the 60+ age group have grown from $1.685 billion (2021) to $7.748 billion (2025), approximately +360 percent in five years.

2. Reported numbers dramatically understate reality. With fewer than one in twenty frauds reported, the true number of elder fraud victims likely runs several times higher than the reported count, into the millions per year on an order-of-magnitude basis, since the FBI and FTC count through different channels. The true annual cost is likely several times higher than what is reported, consistent with the FTC's wide underreporting estimate.

3. The channels of attack are shifting. Social media has overtaken phone calls as the leading contact method for elder fraud by total losses. Cryptocurrency and bank transfers have replaced gift cards as the principal money-moving channels. The infrastructure of the threat is moving faster than the infrastructure of the response.

4. Recovery depends on speed, and most cases do not reach the freeze window in time. In 2025 the FBI froze about half the money in the few hundred cases reported fast enough to act, but the system reached that freeze window in fewer than one in three hundred cases, so less than half of one percent of the dollars stolen from older Americans was frozen.

The Three Findings

The data presented in this chapter, five years of FBI growth, FTC underreporting, FinCEN's banking detection, and the FBI's own recovery results, points consistently in one direction. The visible scale of the problem is large and growing. The hidden scale is several times larger still. And the money, once gone, is almost never recovered: in 2025 less than half of one percent of it was frozen in time, not for want of an effective tool but because almost no case reached that tool fast enough:

- **No single front door**, ten federal actors, most with their own separate intake channels, and a scatter of federal reporting sites, plus 50+ state portals, with no single number to call and no designated first-click destination
- **Inconsistent protective messaging**, taglines borrowed from cybersecurity that do not address the manipulation-based threat model documented in the FTC's research
- **Speed mismatch**, the FBI's Recovery Asset Team can freeze a fraudulent wire only when it is reported almost immediately

America has the people, the agencies, the laws, and the data. What it does not yet have is a way to connect them, the coordination and simplification that Chapter 9 takes up.

In the next chapter, we examine where in America elder fraud losses are most severe, ranking the 50 states, the District of Columbia, and Puerto Rico by losses, per-capita impact, and five-year growth trajectory.

Data Sources for Chapter 1:

- FBI Internet Crime Complaint Center (IC3), *Elder Fraud Annual Reports*, 2020–2023
- FBI IC3, *2024 Internet Crime Report* and *2025 Internet Crime Report*
- Federal Trade Commission, *Protecting Older Consumers 2024-2025*, December 1, 2025
- Federal Trade Commission, *Consumer Sentinel Network Data Book 2024*, March 2025
- Federal Trade Commission, *Consumer Sentinel Network Data Books* 2020-2023
- U.S. Treasury FinCEN, *Financial Trend Analysis: Elder Financial Exploitation*, April 2024
- Consumer Financial Protection Bureau, *Recovering from Elder Financial Exploitation: A Framework for Policy and Research*, September 2022

CHAPTER 02

Chapter 2: State-by-State Rankings

> *Elder fraud is a national crisis, but it does not strike every state equally.*

The Map of Loss

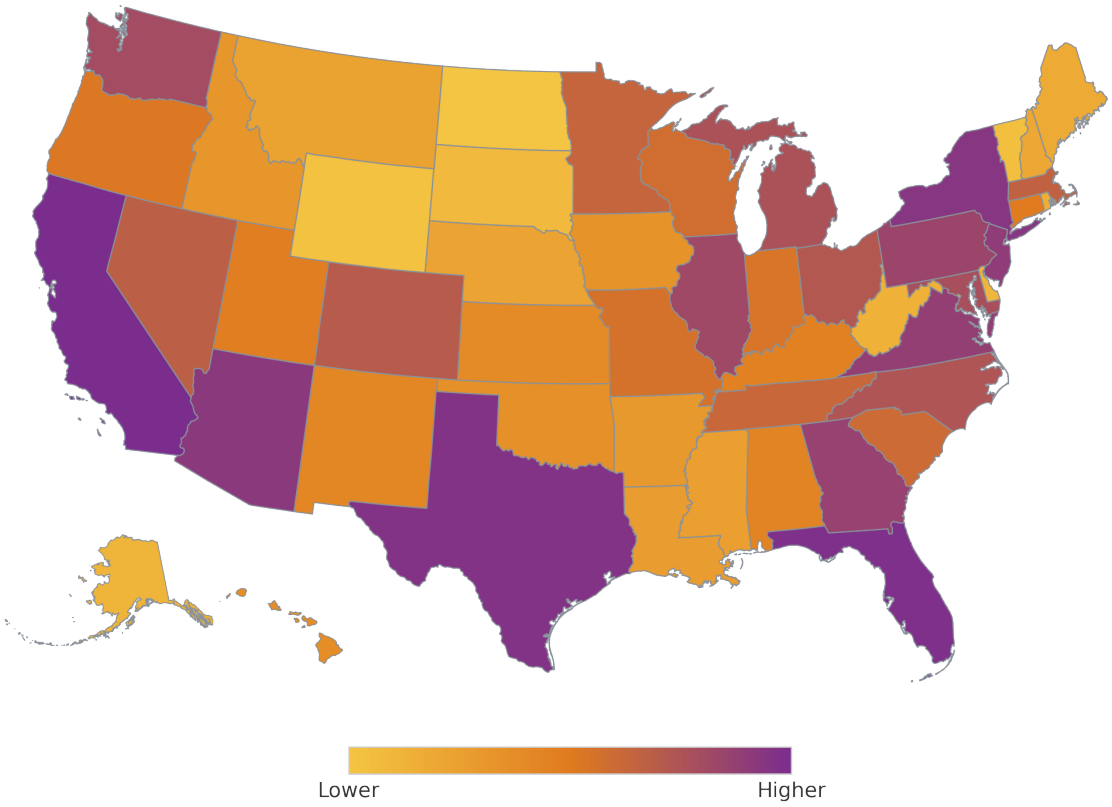
In 2025, elder fraud reached every corner of the United States. All 50 states, the District of Columbia, and Puerto Rico, the 52 reporting jurisdictions in FBI IC3 state-level data, recorded victims and financial losses. But the distribution of those losses reveals a geography of vulnerability that challenges simple assumptions about who is most at risk and why.

This chapter presents four distinct rankings. Each tells a different story:

1. **Total losses**, which states bear the greatest aggregate financial burden
2. **Per-capita losses** (loss per older resident), which states show the highest reported losses per senior
3. **Five-year growth rate**, where the problem is accelerating fastest
4. **Cadence of harm** (how often an older adult is scammed), which states see victims most frequently

Understanding all four is essential. A state can rank low in total losses but high in growth rate, signaling a crisis in its early stages. A state with moderate totals may have devastating per-capita numbers because its senior population is small. Policymakers and journalists who rely on a single ranking miss the full picture.

The map shows that geography at a glance, built from the same state-loss data as the report's cover.

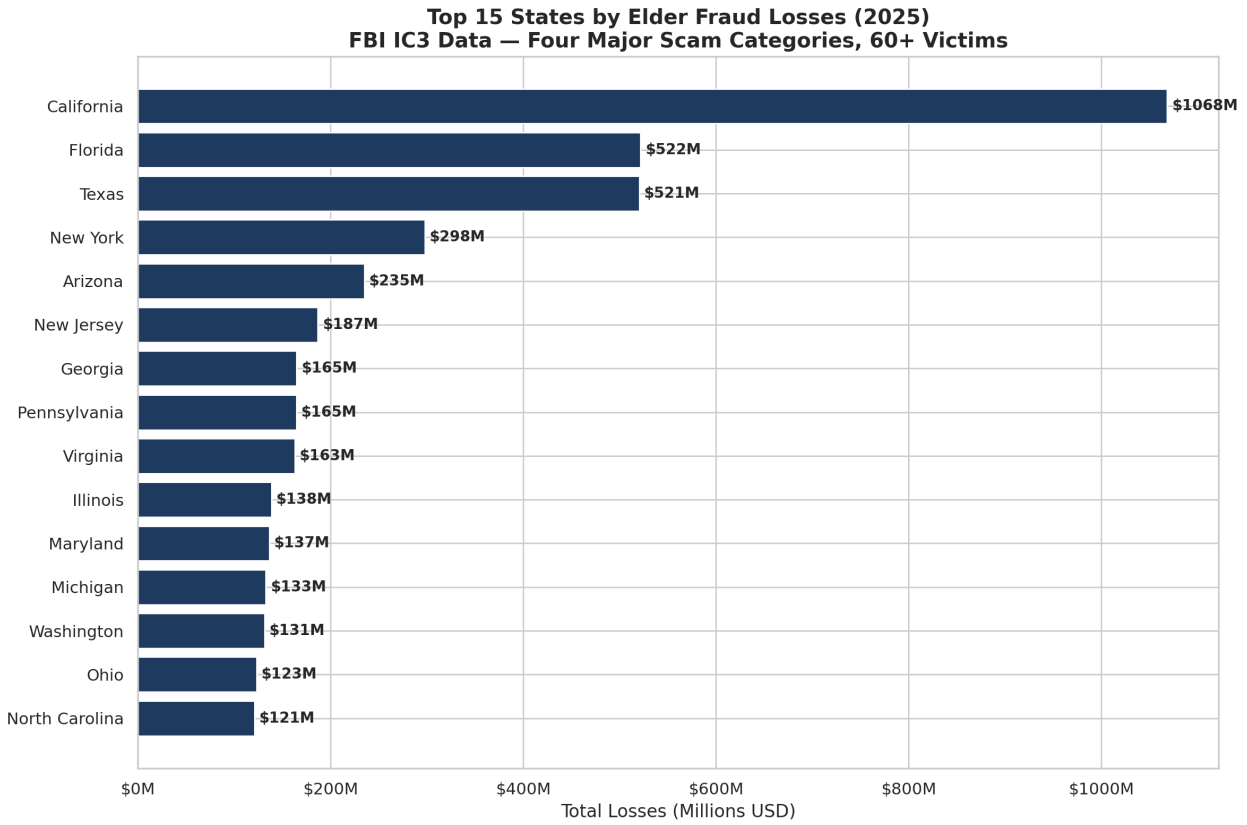


The geography of loss: reported 2025 elder-fraud losses by state (FBI IC3; four major scam categories; victims aged 60+). States are shaded by their rank on total reported losses, lighter for lower and darker for higher, as the color key shows; the exact state-by-state figures appear in the rankings that follow.

Ranking 1: Total Losses by State (2025)

California led the nation in elder fraud losses by a wide margin, with $1.068 billion, just over double the second-ranked state. Florida and Texas were separated by less than $2 million.

The top ten states accounted for $3.46 billion, or 63% of all reported losses across the four scam categories tracked in this ranking (investment, tech support, romance, and government impersonation). The bottom ten accounted for just $90 million. (All-crime-type state totals run higher: California's all-type total is $1.404 billion versus $1.068 billion across these four categories.)



Top 15 states by elder fraud losses, 2025. Source: FBI IC3 state-level files, four major scam categories, victims aged 60+.

Complete State Ranking by Total Losses (2025)

Rank	State	Total Losses	Victims	5-Year Growth
1	California	$1,068.3M	7,987	+481%
2	Florida	$521.7M	5,847	+433%
3	Texas	$520.5M	5,087	+612%
4	New York	$297.7M	3,034	+369%
5	Arizona	$234.8M	3,402	+745%
6	New Jersey	$186.8M	1,546	+389%
7	Georgia	$164.7M	1,677	+1,101%
8	Pennsylvania	$164.6M	2,221	+381%
9	Virginia	$162.9M	1,799	+393%
10	Illinois	$138.4M	1,919	+512%
11	Maryland	$136.5M	1,189	+691%
12	Michigan	$132.8M	1,554	+786%

Rank	State	Total Losses	Victims	5-Year Growth
13	Washington	$131.5M	1,644	+518%
14	Ohio	$123.1M	1,800	+632%
15	North Carolina	$120.7M	1,763	+571%
16	Colorado	$103.1M	1,225	+416%
17	Massachusetts	$81.0M	1,173	+343%
18	Tennessee	$77.6M	1,124	+397%
19	Minnesota	$77.0M	850	+624%
20	South Carolina	$72.6M	1,050	+690%
21	Nevada	$71.5M	1,082	+178%
22	Missouri	$70.0M	1,216	+764%
23	Wisconsin	$67.9M	927	+563%
24	Indiana	$59.8M	1,054	+540%
25	Oregon	$58.3M	1,078	+428%
26	Kentucky	$53.0M	728	+535%
27	Utah	$52.1M	613	+527%
28	Hawaii	$48.1M	394	+677%
29	Connecticut	$47.4M	659	+683%
30	New Mexico	$43.6M	560	+1,537%
31	Kansas	$43.6M	502	+743%
32	Alabama	$43.6M	769	+498%
33	Oklahoma	$39.3M	738	+729%
34	Idaho	$28.7M	437	+1,305%
35	Louisiana	$26.6M	645	+114%
36	Montana	$25.7M	251	+1,214%
37	Iowa	$25.6M	419	+678%
38	Arkansas	$23.7M	599	+1,235%
39	Nebraska	$23.1M	335	+1,276%
40	Mississippi	$22.7M	349	+568%
41	New Hampshire	$19.0M	307	+2,247%
42	Maine	$17.8M	253	+1,449%
43	West Virginia	$14.7M	330	+748%

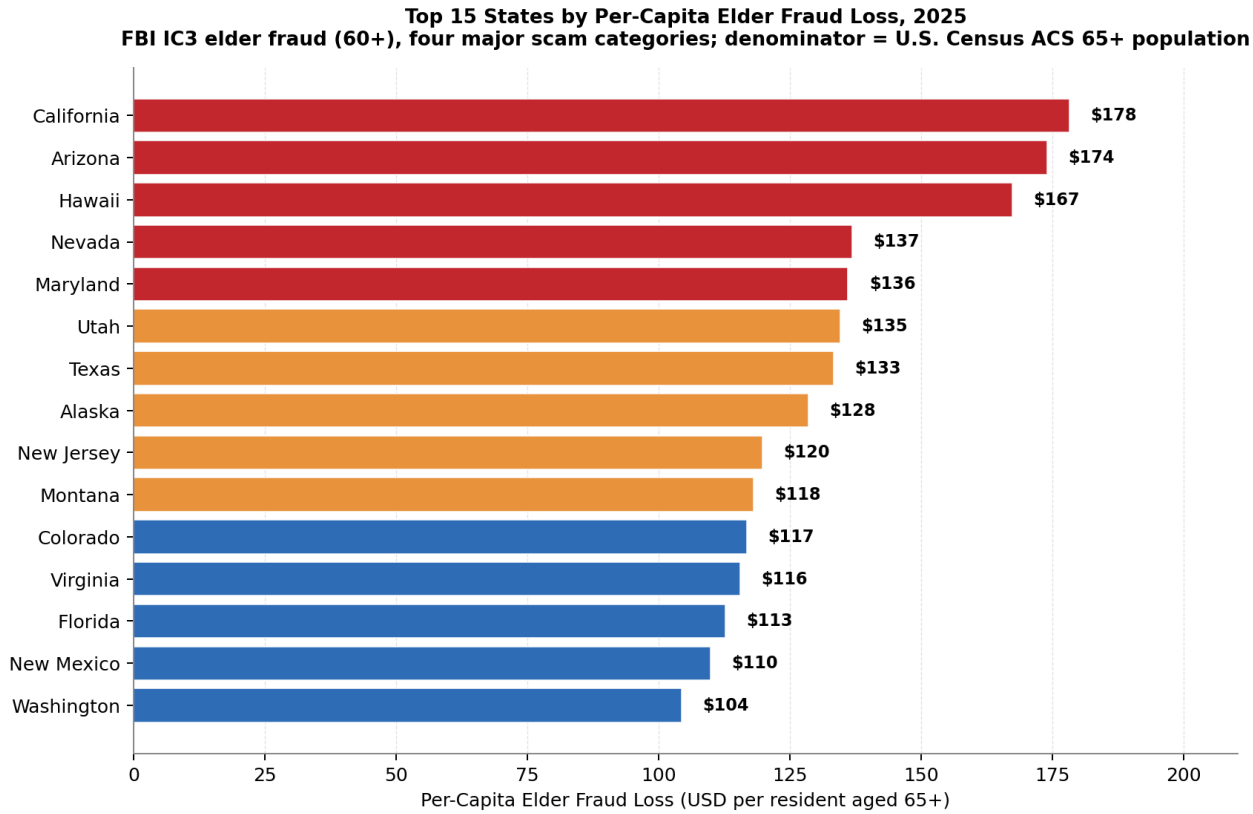
Rank	State	Total Losses	Victims	5-Year Growth
44	Delaware	$12.9M	225	+331%
45	Alaska	$12.6M	231	+260%
46	South Dakota	$12.4M	146	+682%
47	Rhode Island	$11.8M	172	+234%
48	District of Columbia	$7.6M	94	+527%
49	Vermont	$6.8M	133	+158%
50	Puerto Rico	$4.4M	154	+216%
51	Wyoming	$3.6M	126	+12%
52	North Dakota	$3.3M	87	+286%

Source: FBI IC3 Elder Fraud Reports, 2021–2025. Four major scam categories, victims aged 60+.

Ranking 2: Per-Capita Losses, Adjusting for Population

Total loss rankings inevitably favor large states. California, with nearly 6 million residents over 65, will generate more fraud reports than Montana, with 220,000.

The per-capita ranking produces some surprises.



Source: FBI IC3 2025 Elder Fraud Reports + U.S. Census ACS 65+ population estimates. Data matches Appendix A, Table A-1 of *Stolen Trust* report.

Top 10 States by Reported Losses Per Older Resident (2025)

Per-Capita Rank	State	Loss Per Senior	Total Losses	Total Loss Rank
1	California	$178	$1,068M	1
2	Arizona	$174	$235M	5
3	Hawaii	$167	$48M	28
4	Nevada	$137	$72M	21
5	Maryland	$136	$137M	11
6	Utah	$135	$52M	27
7	Texas	$133	$521M	3
8	Alaska	$128	$13M	45
9	New Jersey	$120	$187M	6
10	Montana	$118	$26M	36

Hawaii, ranked only 28th in total losses, jumps to 3rd highest per capita, at $167 per senior. Utah, 27th in total losses, rises to 6th, and Alaska, 45th in total losses, to 8th per capita. Montana, 36th in total losses, reaches 10th per capita.

These are states where fewer seniors live, but those who do face disproportionate risk. Per-capita numbers reveal where reported losses per senior are highest, a better proxy for individual exposure than state totals.

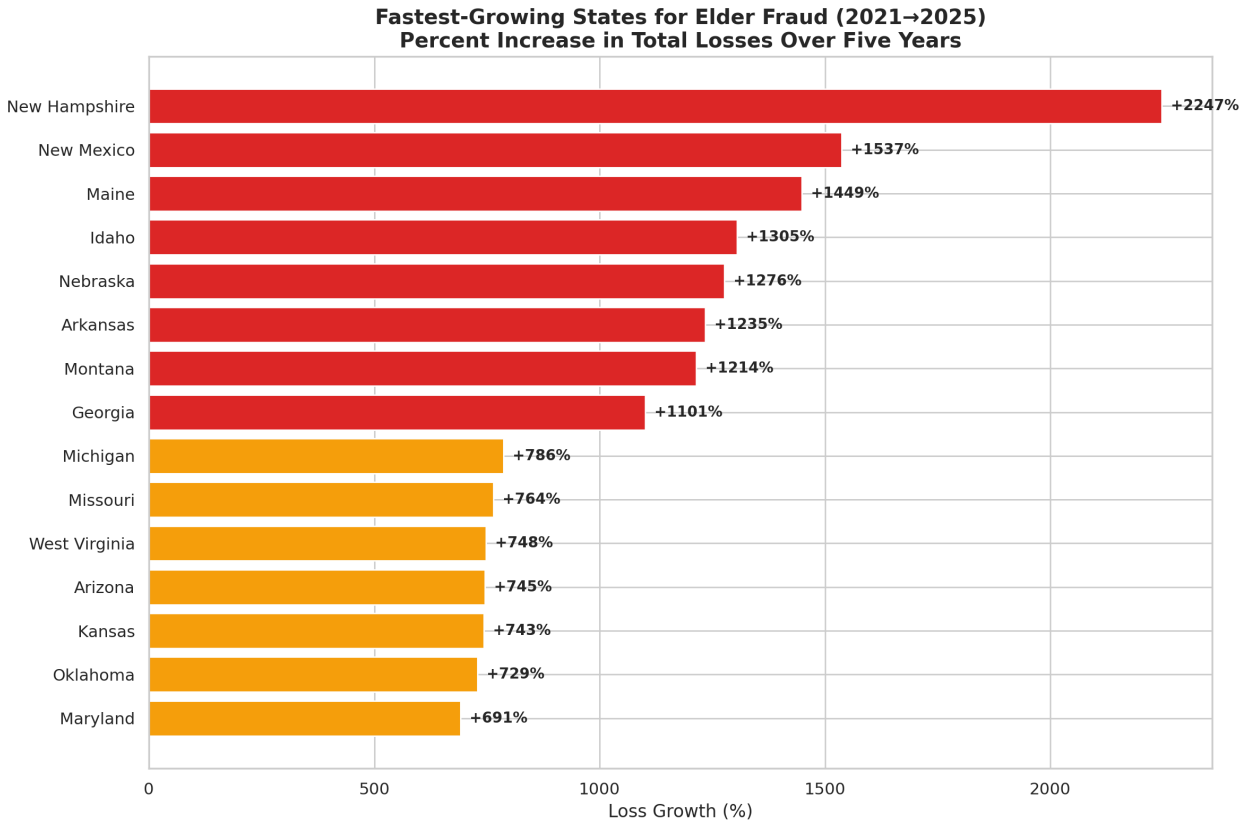
Bottom 5: Lowest Reported Losses Per Older Resident

Per-Capita Rank	State	Loss Per Senior	Total Losses
48	West Virginia	$40	$14.7M
49	Louisiana	$35	$26.6M
50	Wyoming	$34	$3.6M
51	North Dakota	$26	$3.3M
52	Puerto Rico	$6	$4.4M

Per-capita figures divide reported four-category losses by each jurisdiction's residents aged 65 and over, using U.S. Census Bureau American Community Survey estimates (2019–2023), an external dataset; see Data Sources. ACS publishes a standard 65-and-over older-adult denominator used consistently across all jurisdictions, so these figures are best read as a normalized state-to-state comparison rather than a literal loss-per-60+-resident calculation.

Ranking 3: Where the Crisis Is Accelerating

The five-year growth rate shows the widest variation of the four rankings. While every state has seen elder fraud increase since 2021, the rate of acceleration varies enormously, from Wyoming's 12 percent increase to New Hampshire's 2,247 percent.



Fastest-growing states for elder fraud, 2021 to 2025 five-year growth. Source: FBI IC3 state-level files, four major scam categories.

Top 15 Fastest-Growing States (2021 → 2025)

Rank	State	2021 Losses	2025 Losses	Growth
1	New Hampshire	$0.8M	$19.0M	+2,247%
2	New Mexico	$2.7M	$43.6M	+1,537%
3	Maine	$1.1M	$17.8M	+1,449%
4	Idaho	$2.0M	$28.7M	+1,305%
5	Nebraska	$1.7M	$23.1M	+1,276%
6	Arkansas	$1.8M	$23.7M	+1,235%
7	Montana	$2.0M	$25.7M	+1,214%
8	Georgia	$13.7M	$164.7M	+1,101%
9	Michigan	$15.0M	$132.8M	+786%
10	Missouri	$8.1M	$70.0M	+764%
11	West Virginia	$1.7M	$14.7M	+748%
12	Arizona	$27.8M	$234.8M	+745%
13	Kansas	$5.2M	$43.6M	+743%
14	Oklahoma	$4.7M	$39.3M	+729%
15	Maryland	$17.3M	$136.5M	+691%

A pattern emerges in this data: the states growing fastest are smaller, less-populous states. New Hampshire, Maine, Idaho, Montana, Nebraska, Arkansas, these are not the states that dominate headlines about cybercrime. Yet these states post some of the highest elder-fraud growth rates in the nation. New Hampshire's reported losses in these four categories rose 2,247% over five years, for example, against roughly 360% growth in the nationwide all-category elder-fraud total. The two figures sit on different bases, one state's four tracked categories versus the national all-category total, and New Hampshire's percentage is amplified by its very small 2021 starting point of $0.8 million, but the underlying jump from $0.8 million to $19.0 million is real.

One possible explanation is that elder fraud is no longer concentrated in large metro areas: as more seniors in smaller states and rural areas come online, they face the same threats, often with thinner local support to fall back on. The loss data in this report cannot confirm that mechanism; what it does show is that loss growth is now steepest in smaller, less-populous states, exactly the places where coordinated scam-awareness and victim-services resources can be hardest to reach.

Georgia is the only state to rank in the top ten for both total losses (7th) and five-year growth (8th). Its losses grew twelvefold, from $13.7 million in 2021 to $164.7 million in 2025. That combination of scale and acceleration makes Georgia notable for ranking high on both measures at once.

Ranking 4: The Cadence of Harm

Behind every state-level loss total is a victim count, and behind every victim count is a cadence. How often is an older adult, in a given state, being scammed online?

The answer in California is every 66 minutes. In Florida, every 90 minutes. In Texas, every 1.7 hours. In Arizona, every 2.6 hours. In New York, every 2.9 hours. In Pennsylvania, every 3.9 hours. In Illinois, Virginia, Ohio, and North Carolina, every 4 to 5 hours. Even in the smallest, lowest-loss reporting jurisdictions, the cadence is not "rare": in North Dakota and the District of Columbia, an older adult is scammed online every four days; in Wyoming, every 2.9 days; in Vermont, every 2.7 days.

These counts include reported victims only. Research the FTC cites finds that just 4.8 percent of fraud victims report the incident to a government entity or the Better Business Bureau, so true victim counts, and the true cadence, are several times higher.

The table below shows the FBI IC3 2025 four-category victim cadence for all 52 reporting jurisdictions, sorted by 2025 rank:

Rank	State	2025 victims	An older adult is scammed online...
1	California	7,987	every **66 minutes**
2	Florida	5,847	every **90 minutes**
3	Texas	5,087	every **1.7 hours**
4	New York	3,034	every **2.9 hours**
5	Arizona	3,402	every **2.6 hours**
6	New Jersey	1,546	every **5.7 hours**
7	Georgia	1,677	every **5.2 hours**
8	Pennsylvania	2,221	every **3.9 hours**
9	Virginia	1,799	every **4.9 hours**
10	Illinois	1,919	every **4.6 hours**
11	Maryland	1,189	every **7 hours**
12	Michigan	1,554	every **5.6 hours**
13	Washington	1,644	every **5.3 hours**
14	Ohio	1,800	every **4.9 hours**
15	North Carolina	1,763	every **5 hours**
16	Colorado	1,225	every **7 hours**
17	Massachusetts	1,173	every **7 hours**
18	Tennessee	1,124	every **8 hours**

Rank	State	2025 victims	An older adult is scammed online...
19	Minnesota	850	every **10 hours**
20	South Carolina	1,050	every **8 hours**
21	Nevada	1,082	every **8 hours**
22	Missouri	1,216	every **7 hours**
23	Wisconsin	927	every **9 hours**
24	Indiana	1,054	every **8 hours**
25	Oregon	1,078	every **8 hours**
26	Kentucky	728	every **12 hours**
27	Utah	613	every **14 hours**
28	Hawaii	394	every **22 hours**
29	Connecticut	659	every **13 hours**
30	New Mexico	560	every **16 hours**
31	Kansas	502	every **17 hours**
32	Alabama	769	every **11 hours**
33	Oklahoma	738	every **12 hours**
34	Idaho	437	every **20 hours**
35	Louisiana	645	every **14 hours**
36	Montana	251	every **1.5 days**
37	Iowa	419	every **21 hours**
38	Arkansas	599	every **15 hours**
39	Nebraska	335	every **26 hours**
40	Mississippi	349	every **25 hours**
41	New Hampshire	307	every **29 hours**
42	Maine	253	every **1.4 days**
43	West Virginia	330	every **27 hours**
44	Delaware	225	every **1.6 days**
45	Alaska	231	every **1.6 days**
46	South Dakota	146	every **2.5 days**
47	Rhode Island	172	every **2.1 days**
48	District of Columbia	94	every **4 days**
49	Vermont	133	every **2.7 days**

Rank	State	2025 victims	An older adult is scammed online...
50	Puerto Rico	154	every **2.4 days**
51	Wyoming	126	every **2.9 days**
52	North Dakota	87	every **4 days**

Source: HCSK computation, based on the FBI IC3 Elder Fraud Report, 2025 (victims aged 60+, four major scam categories: investment, tech support, romance, government impersonation). Cadence = 525,600 minutes per year ÷ 2025 reported victim count, rounded.

For the high-loss states (California, Florida, Texas, Arizona, New York), the cadence is a matter of minutes or a few hours. For mid-sized states, it is several hours to half a day. For the smallest states and territories, it is days. No reporting jurisdiction's cadence is "rarely". Whether someone lives in Los Angeles or Bismarck, frauds arrive often enough that nearly every community will see one. That is why the cadence of harm puts steady pressure on the systems around an older adult: family, bank, police, and agency hotlines.

In the largest states, the next reported victim is, on average, less than two hours away. Chapter 9 returns to what that cadence implies for response timing.

Regional Patterns

When viewed by region, distinct patterns emerge:

Sun Belt states (Arizona, Florida, Texas, Nevada) rank high on at least one of total or per-capita losses; Arizona and Texas rank high on both, while Nevada is driven by per-capita risk and Florida by aggregate scale. Large retiree populations, high average wealth, and extensive internet connectivity create a target-rich environment.

Mountain West states such as Montana, Idaho, and New Mexico show among the highest growth rates but relatively low total losses, for now. These may be states where the crisis is still in its early stages.

Northeast states (New York, New Jersey, Massachusetts) show high total losses but below-median five-year growth (343 to 389 percent versus a 52-jurisdiction median of 551 percent), consistent with a fraud problem that scaled earlier rather than recently. Connecticut is an exception within the region, with above-median growth (683 percent).

Deep South states (Louisiana, Mississippi, Alabama) report among the lowest per-capita losses. As the caveats below note, reported figures depend on awareness and reporting behavior, which this report cannot measure state by state, so lower reported numbers should not be read as lower true risk.

What These Rankings Don't Capture

Two important caveats apply to all state rankings in this report:

1. **These are reported numbers.** If reporting rates vary by state, and they almost certainly do, then states with better awareness and easier reporting mechanisms may appear worse than states where victims suffer in silence.
2. **These figures cover four crime types.** The FBI's IC3 data used in this analysis covers tech support, investment, romance, and government impersonation scams. Other forms of elder fraud, such as lottery scams, grandparent scams, and extortion, are not included.

Even with these caveats, the data points in one direction: no reporting jurisdiction is untouched, and reported losses rose in every one over the five years.

In Chapter 3, we examine the four major scam categories driving these losses, and reveal how criminal tactics have shifted dramatically over five years.

Data Sources for Chapter 2:

- FBI Internet Crime Complaint Center (IC3), Elder Fraud Reports, 2021–2025
- U.S. Census Bureau, American Community Survey 5-Year Estimates, 2019–2023 (population aged 65+)
- seniors.hcsk.org analysis: per-capita calculations and growth rate analysis

CHAPTER 03

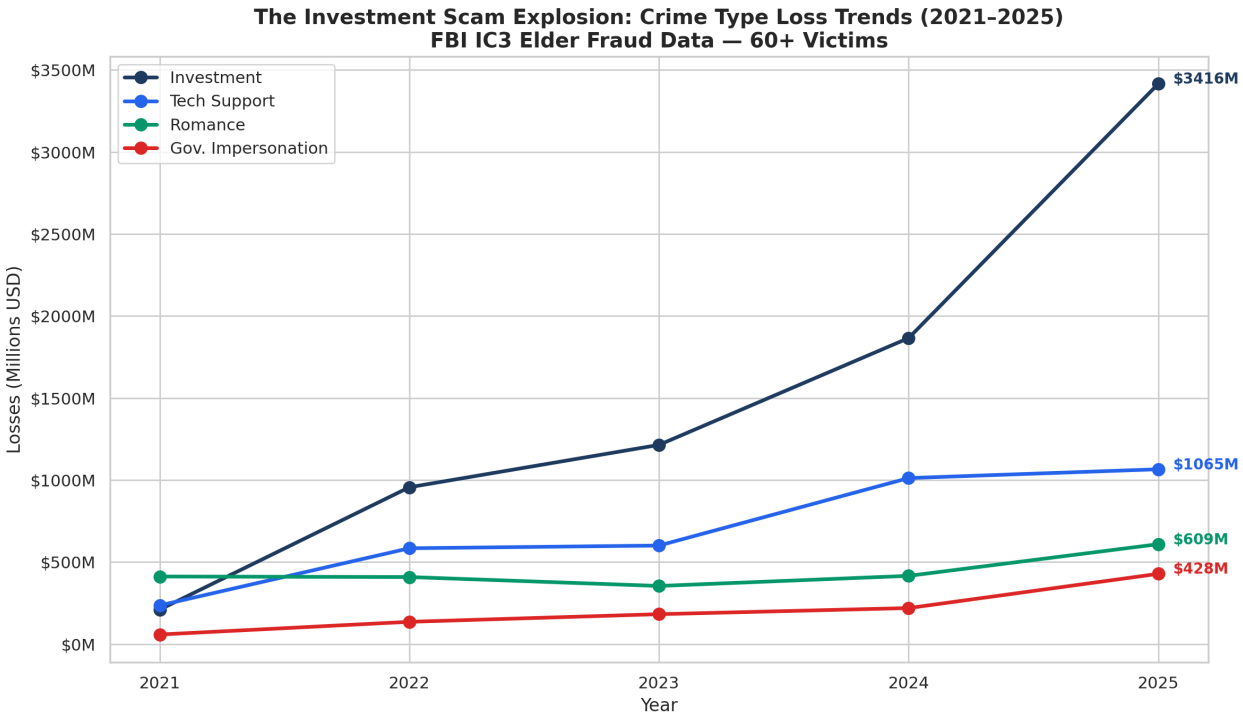
Chapter 3: The Four Scams That Account for Most Elder Fraud Losses

> *In 2021, investment scams cost seniors aged 60 and over $239 million and $3.519 billion in 2025. That is roughly a fifteen-fold increase in five years.*

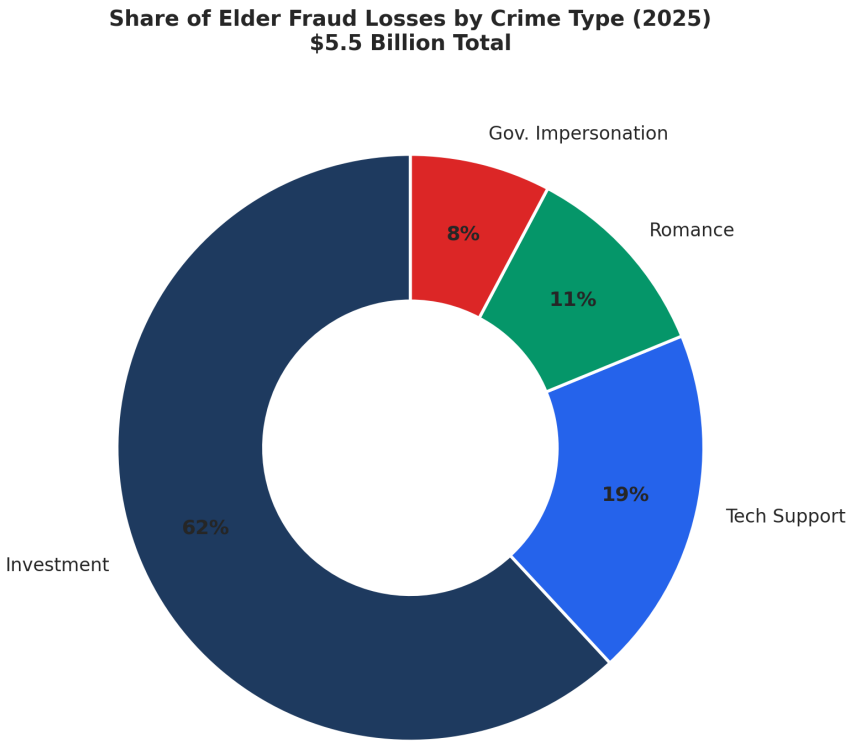
A Shifting Landscape

Not all scams are created equal, and not all scams age the same way. Over the past five years, the composition of elder fraud in America has undergone a dramatic transformation. One crime type has grown faster than any other, roughly fifteen-fold in five years. Another has quietly declined in volume while growing more sophisticated. Two others have surged in ways that reflect broader shifts in technology and social behavior.

Understanding these four scam categories, how they work, how they're evolving, and how they differ from one another, is essential for anyone trying to protect older adults or allocate resources to fight fraud.



Crime-type loss trends, 2021 to 2025. Source: FBI IC3 Elder Fraud Reports, four major scam categories, victims aged 60+.



Share of elder fraud losses by crime type, 2025. Source: FBI IC3 Elder Fraud Report 2025, four major scam categories, victims aged 60+.

> *A note on the two FBI elder-fraud datasets used in this chapter. Section headings for each scam category cite FBI national elder-fraud totals from the IC3 Annual Report's 60+ chapter (e.g., 2025 investment scams: $3.519 billion / 16,926 complaints). The per-year trend tables that follow use state-aggregated totals built up from the 52 FBI IC3 state files. The two differ slightly: by category and year, the national figure runs a little higher or a little lower than the state-file sum (for example, in 2025 the national investment total runs slightly higher, while in 2024 it runs slightly lower), because the national 60+ chapter and the per-state files aggregate and categorize complaints differently. Both are FBI IC3 figures; we cite each consistently to its own basis rather than mixing them. The trend tables in this chapter carry the state-aggregated category totals; the national 60+ chapter figures are the ones cited in each section heading above.*

1. Investment Scams: The Dominant Threat

2025 losses (FBI IC3 Annual Report, 60+ chapter): $3.519 billion | 16,926 complaints | 45% of $7.748B total elder fraud losses

Investment scams are no longer one of four major threats to seniors. They are now the single largest category of elder fraud losses. In 2025, investment fraud accounted for the largest share of elder fraud losses tracked by the FBI, and its five-year growth has been the steepest in the entire elder-fraud category set.

The Numbers Show Steep, Sustained Growth

Year	Victims	Losses	Avg. Loss Per Victim
2021	1,747	$210M	$119,863
2022	4,204	$956M	$227,283
2023	5,925	$1,214M	$204,904
2024	9,969	$1,865M	$187,130
2025	16,831	$3,416M	$203,000

Table values are aggregated from FBI IC3 state-level files (the basis for this report's state-level rankings). For investment scams, the FBI's annual Elder Fraud Report cites slightly higher national 60+ totals, $239 million in 2021 and $3.519 billion in 2025, reflecting differences in how the national chapter and the per-state files aggregate and categorize complaints (see the dataset note above).

Verified against the FBI IC3 2025 Annual Report 60+ chapter, elder investment losses grew +92 percent year-over-year from 2024 ($1.834 billion) to 2025 ($3.519 billion). Average loss per complaint in 2025 (national 60+ basis) was approximately $208,000, by far the most financially devastating category. A single successful investment scam can destroy a lifetime of savings in weeks.

How It Works

The modern investment scam targeting seniors has evolved far beyond the old boiler-room cold call. Today's operations typically follow a pattern known as "pig butchering" (*sha zhu pan*), a term coined by the criminal networks that run them, referring to the practice of "fattening" a victim before "slaughtering" them. The six stages below are a composite drawn from documented cases and FBI and DOJ descriptions of pig butchering; specific amounts and timelines vary.

Stage 1, The Approach. The scammer makes initial contact, most commonly through social media or dating apps. The initial message may appear to be a wrong number, a friend request, or a response to a post in an investment group. There is no mention of money.

Stage 2, The Relationship. Over days or weeks, the scammer builds rapport. Conversations are warm, personal, and frequent. The scammer presents themselves as successful, financially savvy, and genuinely interested in the victim's well-being. For older adults, these conversations often fill a genuine social void.

Stage 3, The Introduction. The scammer casually mentions their own investment success, often in cryptocurrency. They offer to "teach" the victim or share access to a "private" trading platform. The

platform looks professional, complete with real-time charts, account dashboards, and customer service chat.

Stage 4, The Hook. The victim makes a relatively small initial investment, commonly a few hundred to a few thousand dollars. The fake platform shows immediate, impressive returns and the dashboard may display large fabricated gains, encouraging the victim to invest more.

Stage 5, The Escalation. Encouraged by apparent returns, the victim invests larger amounts, often liquidating retirement accounts, taking out home equity loans, or borrowing from family. The platform's fabricated balance continues to climb.

Stage 6, The Slaughter. When the victim attempts to withdraw funds, they are told they must first pay "taxes", "verification fees", or "unlock charges". These demands escalate until the victim either runs out of money or realizes the fraud. By this point, all invested funds have been transferred overseas through multiple cryptocurrency wallets and are unrecoverable.

Why Seniors Are Disproportionately Targeted

The FTC reports that older adults are actually much *less* likely than younger adults to report a loss to an investment scam. Yet investment scams generate the highest aggregate losses for older adults of any fraud type. This apparent paradox reveals the reality: when seniors do fall victim, they lose far more money.

The reason is straightforward. Older Americans are more likely to have accumulated substantial savings, retirement accounts, home equity, pension payouts, and are more likely to make large financial decisions without consulting others. The average investment scam loss for a senior exceeds $200,000. For younger adults, it is significantly lower.

The Role of Social Media

The FTC found that social media is now the leading contact method for investment scams among all age groups. For older adults, this represents a fundamental shift. Five years ago, most investment fraud targeting seniors came through phone calls or email. Today, the attack begins with a Facebook message, an Instagram comment, or a WhatsApp group invitation.

2. Tech Support Scams: Declining Volume, Evolving Tactics

2025 losses (FBI IC3 Annual Report, 60+ chapter): $1.041 billion | 21,333 complaints | 13% of $7.748B total elder fraud losses

Tech support scams remain the second-largest financial-loss category by aggregate dollars among the four tracked categories (and the largest of the four by complaint volume). But their trajectory tells a more complex story than the raw numbers suggest.

Trend Analysis

Year	Victims	Losses	Avg. Loss Per Victim
2021	13,723	$235M	$17,154
2022	17,693	$584M	$32,994
2023	18,172	$600M	$33,034
2024	18,735	$1,012M	$54,003
2025	23,271	$1,065M	$45,778

Trend table: state-aggregated FBI IC3 totals. The FBI national 60+ figure for 2025 (cited in the section heading above) is $1.041 billion / 21,333 complaints; see the dataset note at the top of this chapter.

While total losses have grown from $235 million to over $1 billion, the rate of growth has slowed significantly compared to investment scams. The victim count has plateaued near 18,000–23,000 per year. What has changed is the *average loss per victim*, which has nearly tripled, from $17,154 in 2021 to $45,778 in 2025.

This rising per-victim loss is consistent with several non-exclusive drivers: more effective extraction tactics, a shift toward higher-balance targets, or the reclassification of large hybrid "Phantom Hacker" losses into this category (see "A Notable Exception" below). The aggregate data cannot distinguish among them.

The "Phantom Hacker" Evolution

The FBI issued a specific warning in 2023 about a new variant called the "Phantom Hacker" scam, which combines tech support fraud with government impersonation in a devastating three-stage attack:

1. **The Tech Support Call.** The victim receives a pop-up warning or phone call claiming their computer is compromised. A "technician" gains remote access and shows the victim that their financial accounts are "at risk".
2. **The Bank Impersonation.** A second caller, posing as the victim's bank, confirms that the accounts are under attack and instructs the victim to transfer funds to a "safe" account for protection.
3. **The Government Impersonation.** A third caller, claiming to be from the FBI, Treasury, or Federal Reserve, validates the previous calls and provides wire transfer instructions to a "government-secured" account.

Each stage builds on the authority established in the previous call. By the time the third caller contacts the victim, they have already spoken with two "officials" who confirmed the threat. The psychological pressure is immense.

The FTC reported that older adults are five times more likely than younger adults to report losing money on a tech support scam, the largest such gap among the fraud types where older adults are more likely to report.

A Notable Exception

Despite the FTC reporting a 9% *decrease* in aggregate tech support losses for older adults in its Sentinel data for 2024, the FBI's IC3 data shows continued growth through 2025. This discrepancy reflects differences in how the two systems collect and categorize data. The FBI and FTC collect data through entirely different channels: IC3 accepts complaints filed directly by victims or their representatives, while the FTC's Sentinel Network aggregates reports from multiple sources including state attorneys general, the BBB, and other agencies. The two systems use different category definitions: what one classifies as "tech support" may overlap with the other's "business impersonation". Additionally, hybrid scams like Phantom Hacker, which combine tech support tactics with government impersonation, may be categorized differently depending on which agency receives the report and which stage of the scam the victim describes. Readers should treat both datasets as valid but complementary, each capturing a different slice of the same underlying problem.

3. Romance Scams: Months of Trust, Minutes of Theft

2025 losses (FBI IC3 Annual Report, 60+ chapter, Confidence/Romance): $584 million | 10,188 complaints | 8% of $7.748B total elder fraud losses

Romance scams occupy a unique position in the elder fraud landscape. They are not the largest category by dollar amount, nor the fastest growing. But because they exploit months of cultivated emotional trust, the personal harm reaches well beyond the dollars lost; victims often describe lasting shame and grief alongside the money.

Trend Analysis

Year	Victims	Losses	Avg. Loss Per Victim
2021	7,212	$412M	$57,068
2022	6,835	$408M	$59,730
2023	6,770	$354M	$52,286
2024	9,447	$416M	$44,011
2025	11,557	$609M	$52,672

Trend table: state-aggregated FBI IC3 totals. The FBI national 60+ figure for 2025 (cited in the section heading above) is $584 million / 10,188 complaints; see the dataset note at the top of this chapter.

Romance scams dipped in both victims and losses between 2021 and 2023, potentially reflecting increased public awareness. But the numbers surged in 2024 and again in 2025, driven in part by AI tools that make it easier to create convincing fake personas and maintain multiple "relationships" simultaneously (see Chapter 4).

The Long Con

Unlike other scam types that operate on a timeline of hours or days, romance scams unfold over weeks or months. The scammer invests significant time building emotional trust before any mention of money. This makes them uniquely difficult to interrupt.

Typical patterns observed in our news corpus analysis:

- **Military impersonation** remains common, scammers claim to be deployed soldiers who cannot video-call due to "security restrictions"
- **Professional personas**, doctors, engineers, or oil rig workers in remote locations explain why they cannot meet in person
- **The crisis**, after weeks of emotional bonding, the scammer introduces a financial emergency: a medical bill, a frozen bank account, a customs fee for a package
- **Graduated requests**, initial asks are small ($200–$500), building trust that the money will be "repaid". Requests escalate over time
- **Isolation tactics**, the scammer encourages the victim to keep the relationship private, warning that "friends and family won't understand"

The FTC found that older adults are 39% more likely than younger adults to report romance scam losses, and that romance scams accounted for 28% of all social-media-initiated fraud losses for older adults.

The Scale of the Enterprise

A federal prosecution in the Southern District of New York illustrates the enterprise-level scale of modern romance fraud. A defendant was convicted at jury trial in 2024 and sentenced to 13 years in federal prison after laundering nearly $12 million in stolen funds through ten bank accounts in the Bronx, New York. Between 2020 and 2022, the defendant received money from more than 40 victims, many of them older adults, who were manipulated through fabricated online relationships. The defendant was ordered to forfeit $11.7 million and pay about $7.7 million in restitution. At trial, at least four older victims testified about how they had been deceived.

The Convergence With Investment Scams

An increasingly common variant combines romance and investment fraud. The scammer builds a romantic relationship, then introduces the victim to a "lucrative" investment opportunity. This hybrid approach, sometimes called a "romance-baited investment scam", appears in the FBI data under either or both categories, potentially undercounting both.

4. Government Impersonation: Exploiting Fear of Authority

2025 losses (FBI IC3 Annual Report, 60+ chapter): $413 million | 8,628 complaints | 5% of $7.748B total elder fraud losses

Government impersonation scams have experienced the second-steepest growth trajectory of any major category over five years, behind only investment. State-aggregated FBI IC3 totals for elder government-impersonation losses grew from $58 million in 2021 to $428 million in 2025, a +638 percent five-year increase. Year-over-year growth from 2024 to 2025 was particularly steep, +99 percent at the FBI national level ($208M → $413M elder gov-imp losses in the IC3 Annual Report's 60+ chapter), making it the fastest-accelerating major category in the most recent year.

Trend Analysis

Year	Victims	Losses	Avg. Loss Per Victim
2021	3,187	$58M	$18,144
2022	3,303	$135M	$40,951
2023	3,743	$182M	$48,569
2024	6,939	$219M	$31,571
2025	11,845	$428M	$36,130

Trend table: state-aggregated FBI IC3 totals. The FBI national 60+ figure for 2025 (cited in the section heading above) is $413 million / 8,628 complaints; see the dataset note at the top of this chapter.

Victim counts have roughly quadrupled since 2021 (from 3,187 to 11,845); losses have grown more than seven-fold over the same period (from $58 million to $428 million, a +638 percent increase). The IC3 annual report shows government impersonation elder losses nearly doubled year-over-year in 2025 ($413M vs. $208M in 2024, a 99% increase), making it the fastest-accelerating major category in the most recent year. The average loss per victim has settled around $36,000, lower than investment scams but still devastating for a retiree on a fixed income.

The Playbook

Government impersonation scams exploit a simple psychological principle: most people, especially older Americans who grew up in an era of greater institutional trust, feel compelled to comply with perceived authority.

The most common variations include:

- **IRS scams**, threatening arrest for unpaid taxes, demanding immediate payment via gift cards or wire transfer
- **Social Security scams**, claiming the victim's SSN has been "suspended" or linked to criminal activity
- **Medicare scams**, demanding payment for supposed coverage gaps or threatening benefit cancellation
- **Law enforcement scams**, claiming there is a warrant for the victim's arrest that can be resolved with a payment
- **FTC impersonation**, ironically, scammers now impersonate the very agency investigating fraud, telling victims their accounts are "at risk" and must be moved to "protected" accounts

The FTC notes that these scams increasingly blur the line with business impersonation. A single attack may involve callers claiming to represent Microsoft, then the victim's bank, then the FBI, in sequence. The Phantom Hacker variant described above is a textbook example of this convergence.

The Courier Network

An increasingly common, and increasingly brazen, variant involves physical couriers who arrive at victims' homes to collect cash or gold. Victims are instructed to withdraw their savings, convert them to gold bars or cash, package them, and hand them to a "government agent" who will appear at their door. The FBI tracked $311.8 million in gold courier scam losses across approximately 725 complaints in 2025 (all ages, per the FBI's 2025 Internet Crime Report).

DOJ prosecutions have begun to dismantle these networks. In the Western District of Texas, a courier was sentenced to 97 months in federal prison on February 20, 2025 for a role in an operation tied to nearly $7 million in victim losses. A second defendant in the same scheme received 63 months on June 26, 2025; that defendant and a third co-defendant were tied to approximately $3 million in victim losses. A fourth defendant, who coordinated the receipt of victim property from couriers nationwide and from overseas co-conspirators, was indicted in May 2025 and, per the DOJ's 2025 EAPPA report, has been tied to between approximately $150 million and $200 million in victim losses, among the largest individual loss figures cited in that report.

The Gift Card Connection

Government impersonation scams are the primary driver of gift card payments in elder fraud. Victims are told to purchase gift cards from retailers and read the codes to the caller as "payment" or "verification". This payment method is virtually impossible to trace or recover.

The FTC found that older adults are 36 percent more likely than younger adults to report government impersonation losses, and that government impersonation was the #3 fraud type by total dollars lost among older adults in FTC Sentinel data.

The SSA Imposter Quarterly Picture

The Social Security Administration's Office of Inspector General has published quarterly scam reports continuously since July 2021. Across 17 quarters of data (Issues 2–18, covering Q4 FY 2021 through Q4 FY 2025), the SSA OIG documents the dominant variant within government impersonation: someone calling, emailing, or texting claiming to be from the Social Security Administration. The quarterly data reveals two important counter-trends to the broader elder-fraud growth story:

- SSA-related scam allegations have declined dramatically from their FY 2019–FY 2021 peak. During the peak quarters, SSA OIG was receiving more than 150,000 scam allegations per quarter, in some quarters over 225,000. From April 2022 onward, the agency has received fewer than 10,000 SSA-related scam allegations per month (roughly 30,000 or fewer per quarter), an approximately 80–90 percent decline from peak.
- Despite the decline, SSA-impersonation remains a top reported government-imposter scam type to the FTC. The decline reflects partial success of public-awareness campaigns and law-enforcement disruption, not the elimination of the threat.

The pattern is a useful counter-example to the broader narrative that all elder-fraud categories are growing without limit. Targeted federal-state-private campaigns *can* bend the curve on a specific scam type. The lesson is not that the SSA imposter scam is solved, it is that dedicated, coordinated federal-state-private response on a single threat can produce measurable reduction. Source: SSA OIG, *Quarterly Scam Reports* Issues 2–18 (2021–2025).

The Medicare-Adjacent Hospice Fraud Variant

A second variant within the government-impersonation category that warrants attention is the Medicare-hospice enrollment scam, in which fraudsters enroll Medicare beneficiaries into hospice care without the beneficiary's knowledge or consent, sometimes through door-to-door "Medicare benefit review" approaches. The victim may not realize they have been enrolled in hospice (which under Medicare rules cancels coverage for curative treatments) until they next attempt to access regular medical care. (HHS OIG has long warned about hospice fraud in a different form: its 1998 *Special Fraud Alert* on nursing-home arrangements with hospices documents illegal kickbacks paid to influence hospice enrollment, a provider-side scheme distinct from the consumer-facing enrollment fraud described here.)

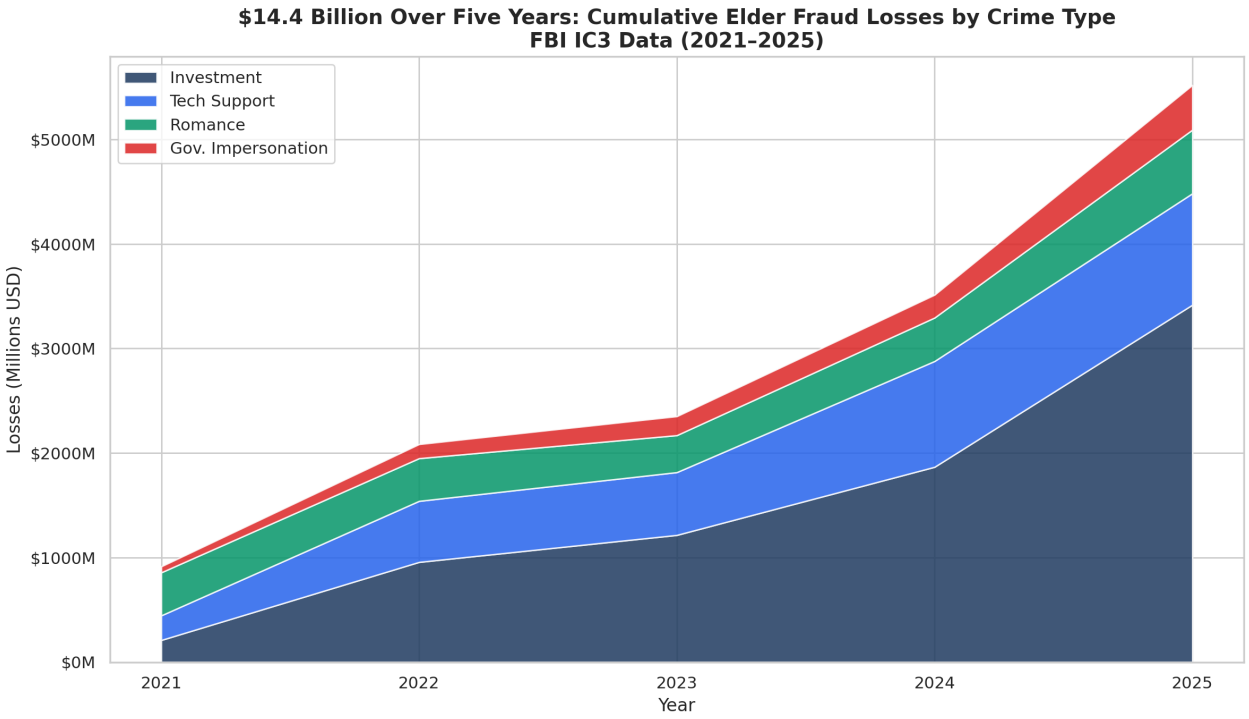
The HHS OIG hotline for reporting Medicare fraud is 1-800-HHS-TIPS (1-800-447-8477). The Senior Medicare Patrol national locator (1-877-808-2468) connects beneficiaries to their state SMP for one-on-one help. See Chapter 6 for the broader inventory of federal actors involved in Medicare fraud response.

The Veteran-Targeted Variant

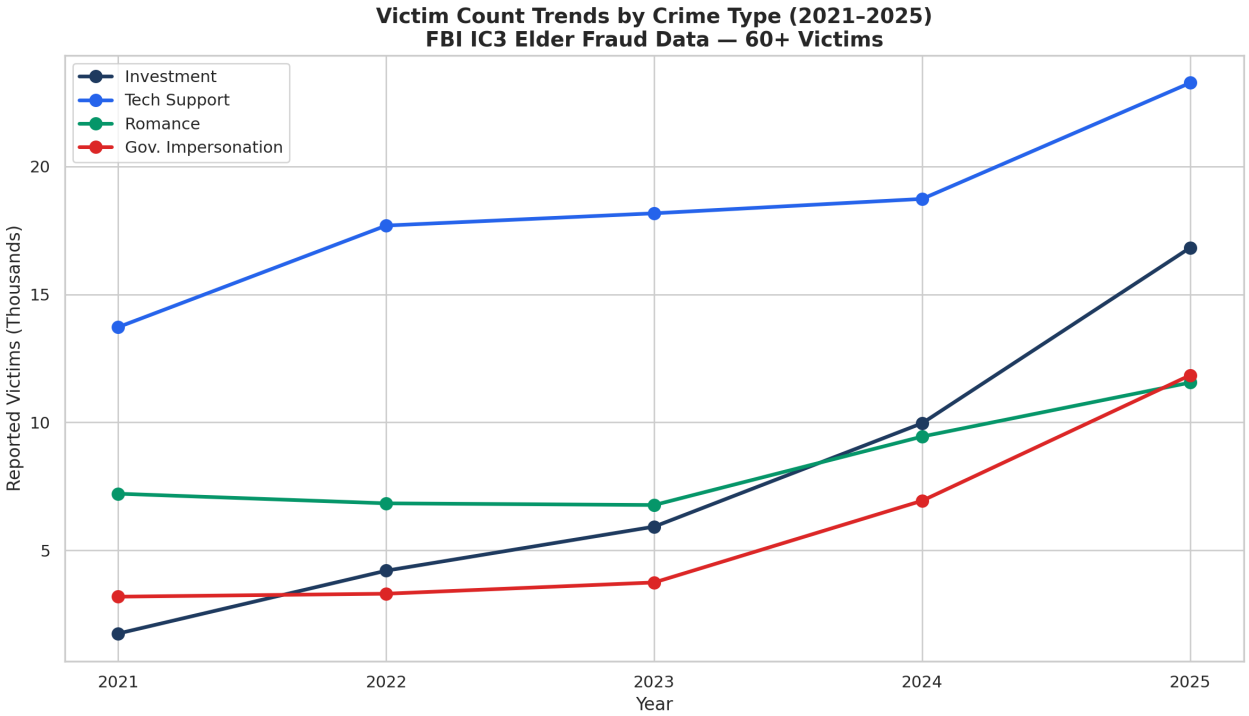
Veterans, service members, and their survivors face a government-impersonation subtype built around earned benefits. Fraudsters impersonating the VA tell veterans they owe money for a benefits "overpayment", use stolen personal information to redirect benefit payments to accounts they control, or operate as "claims predators" who unlawfully charge fees to "help" file an initial VA claim, assistance that VA-accredited representatives and Veterans Service Organizations provide for free. Because the lure is the veteran's own benefits and the impersonated authority is one they have every reason to trust, these schemes are both convincing and especially corrosive. Related schemes target the same population, including "pension poaching" (advisers who promise to boost benefits by restructuring assets into high-fee annuities or trusts) and "benefits buyout" offers that trade a lump sum for the far greater lifetime value of a veteran's payments. In a May 22, 2026 advisory, the Arizona Attorney General catalogued ten such schemes targeting the state's veterans. The VA's dedicated fraud line, VSAFE (vsafe.gov; 1-833-38V-SAFE / 1-833-388-7233), is the correct reporting channel. See Chapter 9 for how a single national front door builds on the VSAFE model.

Crime Type Migration: What Five Years of Data Reveal

Viewed together, the five-year trends reveal a criminal ecosystem that is constantly adapting.



Five-year stacked losses by crime type, 2021 to 2025. Source: FBI IC3 Elder Fraud Reports, four major scam categories.

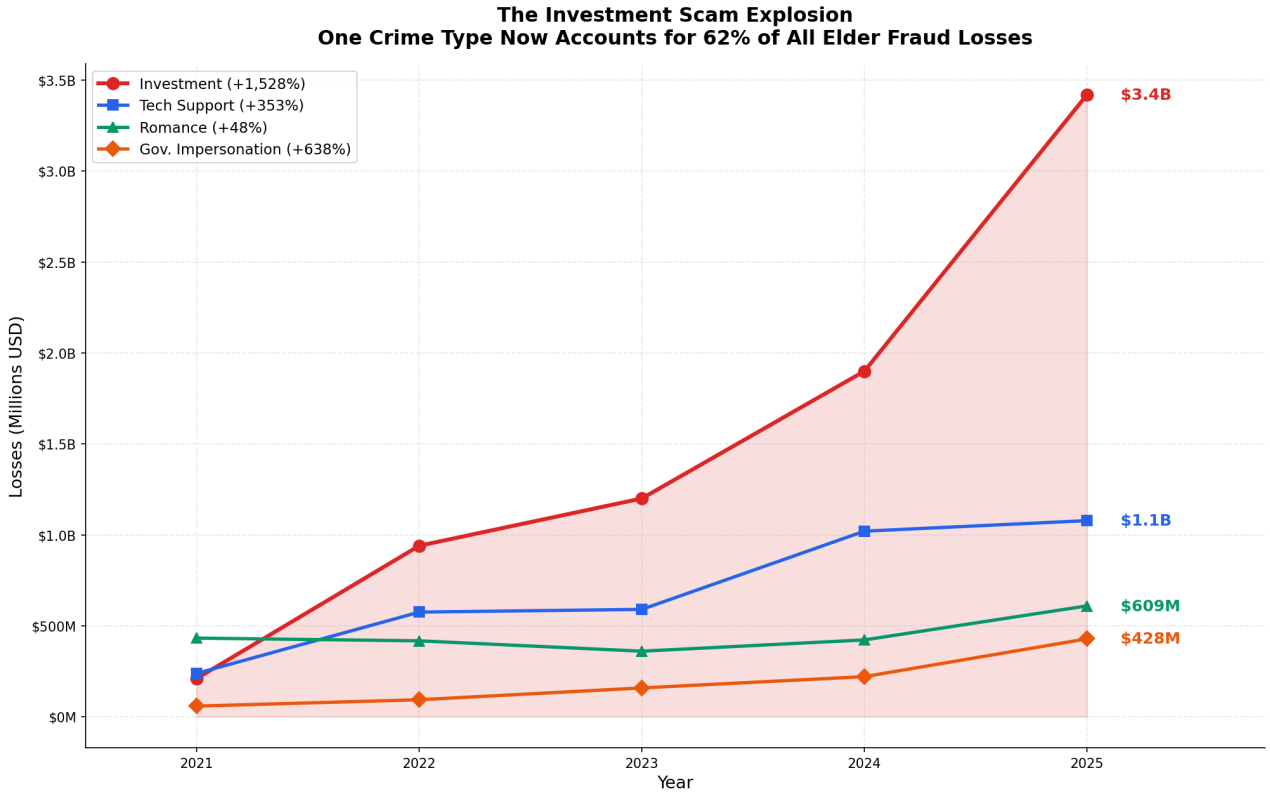


Crime-type victim trends, 2021 to 2025. Source: FBI IC3 Elder Fraud Reports, four major scam categories, victims aged 60+.

The FTC's Complementary Data

The FTC's Sentinel data provides a complementary view of the same landscape, with different categorization. For adults 60 and over in 2024, FTC data shows: investment scams $744 million (+38% YoY), business impersonation $377 million (+21%), government impersonation $375 million (+47%), romance scams $329 million (+19%), and tech support $159 million (-9%). The 47% jump in FTC-reported government-impersonation losses (2023 to 2024) echoes the steep IC3 trend for this category (IC3 elder gov-imp losses rose roughly 99 percent nationally from 2024 to 2025), reinforcing that government impersonation is among the fastest-accelerating fraud types.

Key Shifts



Investment scam loss growth, 2021 to 2025. Source: FBI IC3 Elder Fraud Reports, investment-scam category, victims aged 60+.

The investment scam explosion is the defining story of this five-year period. In 2021, investment scams accounted for $239 million; by 2025 they were by far the largest category at $3.519 billion, or 45% of all elder fraud losses (and, on the state-aggregated basis used in this report's trend tables, about 62% of the four tracked categories). This roughly fifteen-fold increase is the largest such jump on record across the four scam categories tracked by FBI IC3.

Tech support scams have plateaued in volume but increased in per-victim severity. The number of victims has grown modestly, but the average loss per victim has nearly tripled. This rising per-victim loss, alongside only modest growth in victim count, means the category's growth is now driven mainly by larger losses per case rather than by more victims.

Romance scams recovered from a mid-period dip. After declining in 2022–2023, they surged in 2024–2025. A likely catalyst is the spread of AI tools: widely available chatbots and deepfake generators have dramatically reduced the effort required to maintain convincing romantic personas at scale (see Chapter 4).

Government impersonation is the fastest-accelerating category in the most recent year, though it started from the smallest base. Its +638 percent five-year growth, second only to investment, combined with its integration into multi-stage scams like Phantom Hacker, makes it the category most likely to continue accelerating.

The Convergence Trend

Perhaps the most important insight from five years of data is that these categories are *converging*. The Phantom Hacker combines tech support with government impersonation. Romance-baited investment scams combine romance with investment fraud. Business impersonation scams (tracked separately by the FTC) share tactics with both tech support and government impersonation.

The scam of 2026 is not neatly categorizable. It is a multi-stage, multi-persona operation that may involve elements of all four categories in a single attack. This convergence poses a significant challenge for data collection, as crimes that span multiple categories may be undercounted in every category.

Across every category and every hybrid, the point of attack is the same. These scams rarely succeed by breaking into a device; they succeed by breaking into a person's trust and judgment. The vulnerability is human, not technical; no firewall stops a victim who has been persuaded to send the money themselves. It is why the response in Chapter 9 centers on a message about how people *decide*, not how they secure a machine.

Beyond the Four: Emerging Categories

While this report tracks four primary crime types, several additional categories deserve attention for their rapid growth:

- **Account Takeover (ATO):** Approximately 4,700 complaints (all ages, per the FBI's 2025 Internet Crime Report) totaling $359.7 million in 2025, scammers gain control of victims' financial accounts and drain them, often through SIM swaps (tricking a phone carrier into moving the victim's number to a phone the criminal controls, which intercepts security codes) or credential theft.
- **"Task scams" (gamified employment fraud):** A new variant where victims are recruited for fake online "tasks" (product reviews, data entry) and gradually induced to make increasing "deposits". Older-adult job-scam losses reported to the FTC grew 288 percent from 2023 to 2024 (to $33 million), with the FTC identifying task scams as the specific driver.
- **Sextortion:** 6,121 elder complaints totaling $14.9 million, relatively low in dollar terms but devastating in psychological impact, as victims face threats of intimate image exposure.

In Chapter 4, we examine the technological accelerant behind much of this growth: artificial intelligence and its rapidly expanding role in elder fraud.

Data Sources for Chapter 3:

- FBI Internet Crime Complaint Center (IC3), *Elder Fraud Reports*, 2020–2023
- FBI IC3, *2024 Internet Crime Report* and *2025 Internet Crime Report*, 60+ chapters (verified figures: Investment $3.519B, Tech Support $1.041B, Confidence/Romance $584M, Government Impersonation $413M)
- Federal Trade Commission, *Protecting Older Consumers 2024-2025 Report*, December 1, 2025 (fraud-type dollar breakdown for 60+)
- U.S. Department of Justice, *EAPPA Annual Report to Congress*, 2025 (S.D.N.Y. romance-laundering prosecution; W.D. Texas courier-network prosecutions)
- FBI Public Service Announcement: "Phantom Hacker" Scams, 2023
- SSA Office of Inspector General, *Quarterly Scam Reports* Issues 2–18, July 2021 – September 2025 (17 quarters of SSA-impersonation trend data)
- HHS Office of Inspector General, *Special Fraud Alert: Fraud and Abuse in Nursing Home Arrangements with Hospices* (March 1998; provider-side anti-kickback alert)
- seniors.hcsk.org news corpus analysis, August 2025–May 2026 (1,910 articles)

CHAPTER 04

Chapter 4: The AI Escalation

> *"That was my granddaughter's voice" Canadian senior targeted by an AI voice-cloning scam, December 2025 (CBC News)*

When a scammer uses AI to write a convincing phishing email, or a deepfake voice generator to impersonate a grandchild, the resulting crime is recorded as a phishing attack or a grandparent scam. The AI enablement, which made the attack more convincing, more scalable, and harder to detect, is mostly invisible in the data.

The AI Scam Timeline: 2021–2026

The integration of AI into elder fraud has not been a single event but a progressive escalation, each stage making scams cheaper, faster, and more convincing.

Phase 1: Template Enhancement (2021–2022)

Early AI applications in fraud were modest. Scammers used basic language tools to improve the grammar and spelling of phishing emails, making them harder to identify as foreign-originated. Automated translation tools enabled scam operations in non-English-speaking countries to target American seniors more effectively.

Impact: Incremental. Scam emails became slightly more polished, but the underlying methods were unchanged.

Phase 2: Generative Text at Scale (2023)

The public release of consumer AI chatbots in late 2022 and their rapid improvement through 2023 marked a turning point. In September 2025, Reuters and Malwarebytes reported that several AI chatbots could be prompted, using jailbreak-style modifications (wording crafted to slip past the AI's safety rules), to generate convincing phishing messages targeting seniors; the companies say such prompts violate their usage policies and that their safety systems are continually updated.

The researchers found that AI could produce in seconds what previously took a human scammer hours: personalized, emotionally manipulative messages tailored to specific demographics, written in fluent English, with no telltale grammatical errors.

Impact: Dramatic reduction in the effort required to generate high-quality scam content. A single operator could now produce thousands of unique, convincing messages per day.

Phase 3: Voice Cloning (2023–2024)

Voice cloning technology crossed a critical threshold in 2023–2024. Tools that once required hours of audio samples could now create a convincing voice replica from as little as a few seconds of recorded speech, a snippet easily obtained from a social media video, voicemail greeting, or phone call. (Multiple studies and vendor demonstrations, including Microsoft's VALL-E research (arXiv: 2301.02111) and commercial voice-synthesis platforms, have demonstrated few-second cloning capability since 2023).

In December 2025, CBC News reported the case of a Canadian senior who received a phone call from what sounded exactly like their granddaughter, crying and begging for bail money. "That was my granddaughter's voice", the victim said. It was not their granddaughter. The victim is convinced the voice was AI-generated; police could not confirm whether the scammers cloned it or assembled the call from personal details harvested online.

The grandparent scam, one of the oldest cons in the book, has been supercharged by voice cloning. Previously, scammers relied on vague impersonations and the hope that an upset grandparent wouldn't notice subtle differences. Now, the voice on the phone can be indistinguishable from the real person.

Impact: Transformed the grandparent scam from a low-success-rate cold call into a high-conviction targeted attack. Our news corpus surfaced numerous articles about grandparent scams during the monitoring period, many referencing AI or voice technology.

Phase 4: Deepfake Video (2024–2025)

Video deepfakes, AI-generated video of a person saying and doing things they never did, moved from research curiosity to practical fraud tool in 2024–2025.

The potential of this technology is illustrated by a case that, while not itself confirmed to involve deepfake video, shows the trajectory. In October 2025, a Florida resident was sentenced to one year in prison plus 28 years of probation for laundering money on behalf of scammers who posed as Elon Musk on Facebook to defraud a 74-year-old Texas woman of $250,000 through a fake celebrity-endorsed investment (Bradenton Herald, October 2025). The actual Musk impersonators (an overseas operation) used a fabricated Facebook profile and months of messaging to build trust, convincing her to invest in what she believed were Musk-endorsed business ventures.

That scam required only a fake profile and text-based deception. Now consider the same attack enhanced with deepfake video: the victim could video-call "Musk" and see a convincing real-time deepfake confirming the story. This capability exists today and is advancing rapidly toward indistinguishability from live video.

Video calls, long considered a reliable way to verify someone's identity, are becoming unreliable. When a senior's family member advises them to "just video-call the person to make sure they're real", that advice is becoming a weaker safeguard than it used to be.

Impact: Deepfake video threatens one of the last reliable methods of remote identity verification available to non-technical users. Romance and investment scams could become materially harder for non-experts to distinguish from legitimate relationships through digital communication alone.

Phase 5: Autonomous Scam Agents (2025–Present)

The current frontier is the deployment of AI agents that can conduct entire scam conversations autonomously, without human intervention. These systems can:

- Maintain consistent personas across hundreds of simultaneous conversations
- Respond to questions in real time with contextually appropriate answers
- Adapt their approach based on the victim's responses and apparent vulnerability
- Operate 24 hours a day at marginal cost per interaction

While documented cases of fully autonomous scam agents targeting seniors are still emerging, the technical capability exists today. The economics are irresistible: a human-operated scam operation that can maintain ten simultaneous conversations could, with AI agents, maintain ten thousand.

Impact: We are in the early stages of this phase. Within the next major federal reporting cycle, autonomous scam agents are likely to become a documented, significant threat.

The Attack Surface: A Rapidly Expanding Online Population

Older adults are now overwhelmingly online. Pew Research Center finds that 95 percent of all U.S. adults now use the internet, and 78 percent of adults aged 65 and over own a smartphone (Pew Research Center, Mobile Fact Sheet, 2025 update; *Americans' Use of Mobile Technology and Home Broadband*, 2024). The generation that once formed a "digital divide" barrier to online fraud is now almost fully connected. Every smartphone is a potential attack surface. Every social media account is a potential point of contact. The question is no longer whether seniors are online, it is whether their online presence is defended.

The Companionship Vulnerability

The AI escalation is colliding with a social crisis that makes it uniquely dangerous. The U.S. Surgeon General's 2023 Advisory *Our Epidemic of Loneliness and Isolation* documents the scale of the crisis, and December 2025 loneliness research finds that 23 percent of lonely adults 45 and over are interested in emerging AI technologies for companionship and conversation, more than double the 10 percent share among adults who are not lonely (see Chapter 8 for the broader loneliness crisis).

Millions of isolated older adults are actively seeking connection, and a growing number are open to finding it through AI. Meanwhile, autonomous AI agents are becoming capable of sustaining

convincing, emotionally engaging relationships at scale. The same underlying capability can power a disclosed "AI companion" or a hidden "AI romance scammer", and the user often cannot tell which they are dealing with.

What the News Tells Us

Our monitoring of 1,910 news articles between August 2025 and May 2026 identified 100 articles specifically referencing AI in the context of elder fraud. Analysis of these articles reveals several patterns:

AI as Attack Tool

The majority of AI-related articles describe AI being used *by* scammers:

- Voice cloning for grandparent scams (CBC, BBB reports)
- AI-generated phishing at scale (Reuters, Malwarebytes investigation)
- Deepfake video capabilities advancing toward real-time use in romance scams
- AI-enhanced social engineering (multiple reports)

AI as Defense Tool

A smaller but growing number of articles describe AI being used *against* scammers:

- Behavioral-monitoring AI engines that track financial-behavior changes and patterns consistent with scam victimization, with announced bank-software deployments in 2025–2026
- AI platforms to detect and block scam communications
- ChatGPT used by a victim to identify and expose a $1 million pig-butchering scam (Decrypt, December 2025)

The defensive applications are promising, but there is a structural asymmetry. AI defenses today are mostly device-centered (transaction monitoring, malware detection, content filtering). As Chapter 3 argues, these scams target a person's trust and judgment, not the device they happen to be using, and AI tools built to defend the person, rather than the device, do not yet exist. Scammers exploit this directly, and they hold a first-mover advantage: they have been integrating AI since 2023, while person-centered defenses are only now being designed. Closing that gap is a built problem, and it is the kind of gap a coordinated national response is meant to drive.

The Coverage Arc

AI-related coverage in our corpus shows a notable pattern: a spike in September–October 2025 (15 and 13 articles, driven by the Reuters/Malwarebytes investigation and the first wave of high-profile deepfake cases), a December 2025 dip (6 articles), and then sustained coverage running 10–13 articles per month from January through April 2026. Unlike many emerging-tech stories that decay sharply

after their initial novelty fades, AI elder-fraud coverage stabilized rather than declined. The data suggests editors and reporters have recognized AI-enabled scams as a continuing story rather than a one-cycle headline. That is encouraging, but the absolute volume (~5 percent of the corpus, 100 articles) remains low relative to the trajectory of the underlying threat documented earlier in this chapter.

The Measurement Gap, and Its First Fix

For years, the most fundamental challenge in understanding AI-enabled elder fraud was that the official data collection systems were not designed to capture it. When a senior was scammed by a voice clone, the FBI recorded it as a confidence/romance scam. When an AI-generated phishing email led to a tech support scam, it was recorded as a tech support scam. The AI component, which may be the difference between a failed attempt and a successful one, was invisible in the data.

The IC3's Breakthrough: First AI Data

In a significant development, the FBI's 2025 IC3 Annual Report included AI-related complaint data for the first time, adding "AI Related" as a descriptor that could be attached to any crime type. The initial results are striking:

All ages:

- 22,364 AI-related complaints reported to IC3 in 2025
- $893.3 million in total losses from AI-related fraud

Adults aged 60 and over:

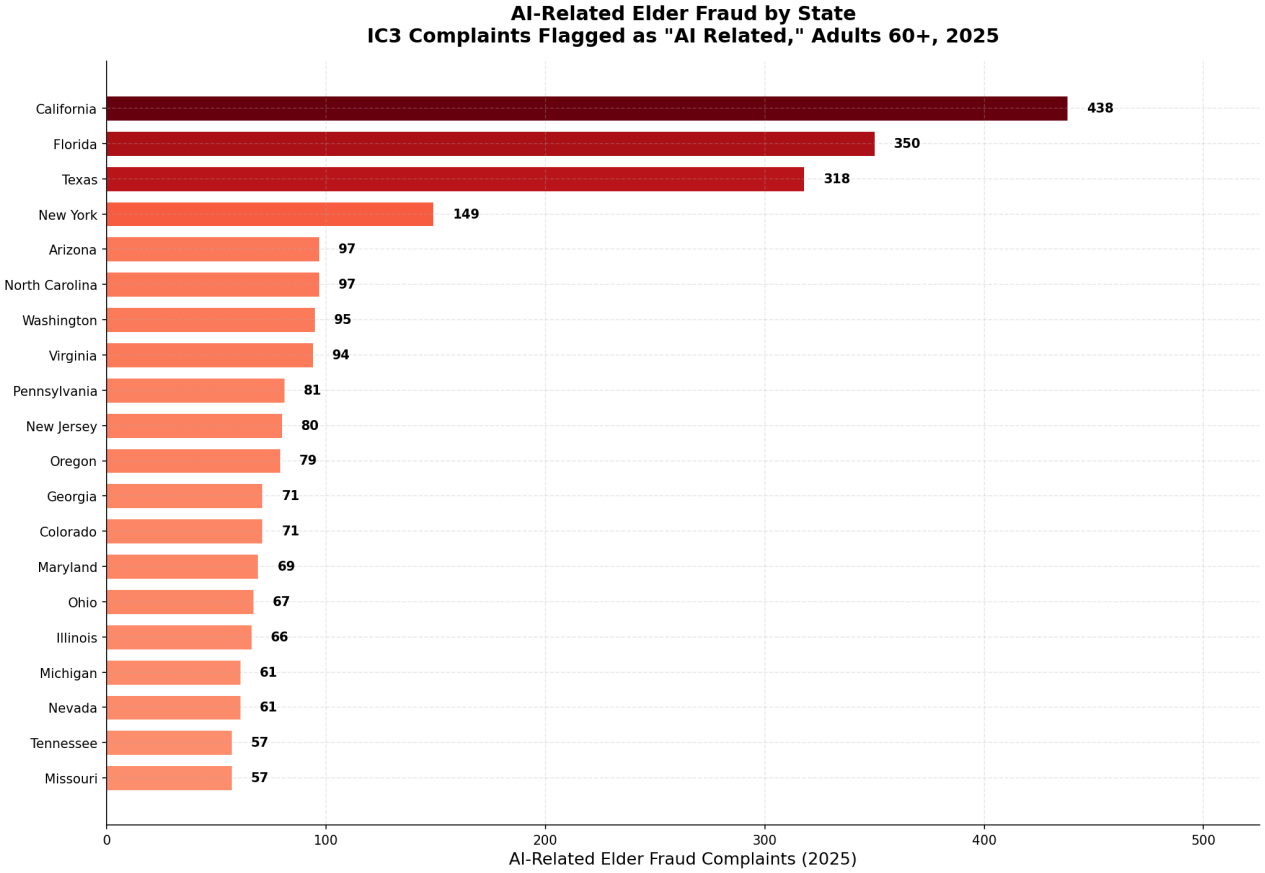
- 3,143 AI-related elder fraud complaints
- $352.5 million in losses from AI-related elder fraud

The breakdown by crime type reveals where AI is having the greatest impact:

Crime Type (AI-Related, All Ages)	Complaints	Losses
Investment Scams	4,356	$632M
Extortion	1,764	$2.9M
Personal Data Breach	1,204	$18.8M
Phishing/Spoofing	803	$10.3M
Confidence/Romance	626	$19M
Tech/Customer Support	574	$19.5M

Investment scams dominate AI-related fraud, with $632 million in AI-linked losses, against all-ages investment scam losses exceeding $8 billion (the table above is all ages; 60+ investment losses were

$3.519 billion). As the IC3 itself noted: "many victims do not realize the extent AI may be involved in scams".



AI-related elder fraud complaints by state, 2025. Source: FBI IC3 Internet Crime Report 2025, victim-identified "AI Related" descriptor, victims aged 60+.

The 3,143 elder AI complaints almost certainly represent a fraction of the actual AI-enabled elder fraud occurring, because victims cannot detect AI involvement they don't know about.

What This Data Does and Does Not Tell Us

The IC3's addition of AI tracking is a welcome and necessary step. It begins to build the data foundation necessary for every other AI-related response.

But the initial data also confirms our concern: AI-enabled elder fraud is already a $352.5 million problem *in its first year of measurement, counting only what victims recognize and report*. Given that the vast majority of AI involvement is invisible to victims, the true figure is almost certainly many times higher.

The gap between $352.5 million in *reported* AI elder fraud and the $7.748 billion in *total* reported elder fraud does not mean AI plays a small role. It means we are still measuring the shadow, not the object.

What to Watch in Late 2026 and 2027

Based on the current trajectory of AI capabilities and their adoption by criminal enterprises, the following developments are plausible over the next 12–24 months. These are scenarios to prepare for, not forecasts:

1. Real-time multilingual scam operations. AI translation and voice synthesis will enable scam call centers to operate in any language with native-sounding fluency. A call center in one country will be able to target seniors in the United States, Canada, the United Kingdom, and Japan simultaneously, with each victim hearing a caller who sounds American, Canadian, British, or Japanese.

2. Hyper-personalized attacks. AI systems that combine publicly available data (social media posts, property records, obituaries, family member information) with generative capabilities will produce scam approaches tailored to individual victims with unprecedented specificity. "Your grandson Jacob, who goes to Ohio State, was in a car accident on Route 33" is far more convincing than "your grandson is in trouble". Material harvested from the steady stream of data breaches (passwords, addresses, family relationships, financial details) amplifies this further, providing AI with non-public, victim-specific facts a stranger should not know but already does.

3. Video deepfakes in real-time video calls. While current deepfake video requires some preparation, the technology is advancing toward real-time generation indistinguishable from live video. As this threshold is crossed on a near-term timeline, video verification will become increasingly unreliable as an identity confirmation method.

4. AI-generated documentation. Fake legal documents, court orders, bank statements, and government correspondence generated by AI will become commonplace. These documents will be visually indistinguishable from legitimate ones, removing another traditional method of verifying a scammer's claims.

5. Scale without precedent. The combination of all these capabilities will enable scam operations to target millions of potential victims simultaneously while maintaining the appearance of personalized, one-on-one human interaction. The marginal cost per target will approach zero.

One additional consideration belongs in this section, even though it sits outside the elder-fraud frame proper. The same technical capabilities documented above (voice cloning, deepfake video, autonomous conversational agents) can be turned to electoral and political attacks as readily as to financial fraud. In January 2024, AI-generated robocalls impersonating President Biden's voice were sent to New Hampshire Democratic primary voters, telling them to save their vote for November and skip the primary. In July 2025, the State Department warned diplomats that an impostor had used AI to impersonate Secretary of State Marco Rubio in text, Signal, and voice-mail messages aimed at three foreign ministers, a U.S. senator, and a U.S. governor. The FBI separately warned in spring 2025 of a broader campaign impersonating senior U.S. officials. With the 2026 midterm elections approaching, older adults are not just an elder-fraud target: they vote in large numbers, and the phone remains a channel many of them trust. The defensive infrastructure that would protect them from a fake-

grandchild voice call is the same infrastructure that would protect them from a fake-candidate or fake-official voice call, and it has not yet been built.

The faster and more convincing AI makes these attacks, and the less reliable identity verification becomes, the more a senior needs one obvious place to turn, one clear instruction to follow, and a response that moves in hours rather than weeks. Chapter 9 suggests that framework.

Chapter 5 examines what our analysis of the 1,910-article news corpus reveals about elder fraud trends that the official data has not yet captured.

Data Sources for Chapter 4:

- seniors.hcsk.org news corpus: 100 AI-related articles, August 2025–May 2026
- FBI IC3, *2025 Internet Crime Report*, 2026 (AI section: 22,364 complaints/$893.3M all ages; 3,143 complaints/$352.5M for 60+)
- Reuters/Malwarebytes AI phishing investigation, September 2025
- CBC News: AI voice-cloning grandparent scam report, December 2025
- Bradenton Herald (via Yahoo): Elon Musk impersonation investment scam, court-record sentencing, October 27, 2025 (Manatee County; $250,000 invested/restitution; 28 years' probation)
- Decrypt: ChatGPT exposes pig-butchering scam, December 2025
- Pew Research Center, *Mobile Fact Sheet*, 2025 update (78 percent smartphone ownership for 65+; 91 percent smartphone ownership overall) and *Internet/Broadband Fact Sheet* (95 percent internet adoption among U.S. adults)
- U.S. Surgeon General, *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, 2023
- FBI IC3 Elder Fraud Reports, 2021–2025
- New Hampshire Department of Justice press release, May 2024 (AI-generated President Biden robocall, January 2024 New Hampshire Democratic primary)
- NPR / Associated Press, *Impostor uses AI to impersonate Rubio and contact foreign and U.S. officials*, July 9, 2025
- FBI Internet Crime Complaint Center, Public Service Announcement I-051525-PSA, *Senior US Officials Impersonated in Malicious Messaging Campaign*, May 15, 2025

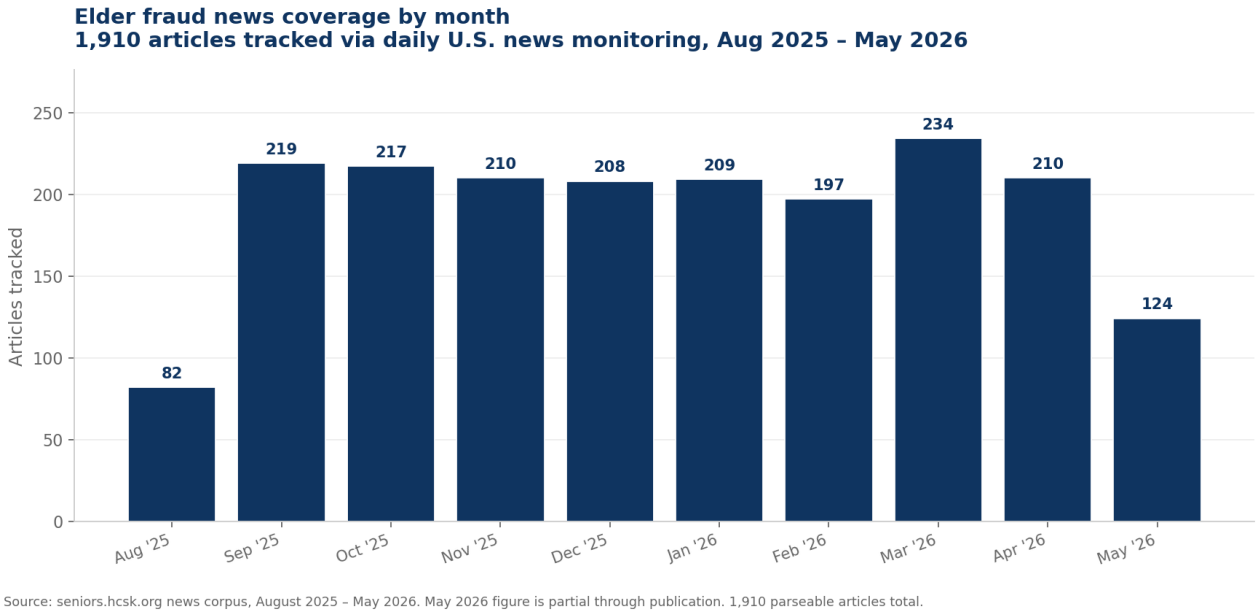
CHAPTER 05

Chapter 5: What 10 Months of News Coverage Reveal

> *Between August 2025 and May 2026, we tracked elder fraud stories published in media that surfaced through daily news monitoring. The analyzable corpus is 1,910 articles. This chapter presents the analysis of that ten-month record.*

The Volume of Coverage

Elder fraud generated consistent coverage throughout the monitoring period, averaging roughly 213 articles per month across the eight complete months (September 2025 – April 2026), with no pronounced seasonal swing.



Elder fraud news coverage by month, August 2025 to May 2026. Source: seniors.hcsk.org news corpus

Month	Articles
Aug 2025 (partial through publication)	82
Sep 2025	219
Oct 2025	217
Nov 2025	210
Dec 2025	208
Jan 2026	209
Feb 2026	197
Mar 2026	234
Apr 2026	210
May 2026 (partial through publication)	124

The consistency of this coverage suggests that elder fraud is not a seasonal story or a topic that only surfaces during awareness months. In our feed, it was a steady presence in every month we tracked.

What the Media Covers, and What It Doesn't

The Enforcement Drumbeat

The consistency of enforcement coverage, roughly 40 articles per month across the full ten-month window, reflects a real and active law-enforcement response; though, as this section shows, coverage volume is not the same as accountability at scale. The week-by-week record from our corpus reads as a national, almost daily drumbeat. In a single month, October 2025, our corpus surfaced a near-daily run of elder-fraud prosecutions across five states in the space of three weeks. The Justice Department's "Operation Silver Shores", a $30 million case tied to a violent California-based gang, drew coverage from multiple outlets (*"Amarillo trio arrested in $30 million elder fraud scheme linked to violent California gang"*, NewsChannel 10, October 22, 2025; *"Operation Silver Shores dismantles $30M fraud targeting elderly victims"*, KMPH Fresno, October 23, 2025). In the same weeks came *"AG: Leominster woman sentenced after admitting scam of elderly residents"* (The Gardner News, October 15, 2025), *"Bradenton man sentenced for role in $250,000 'Elon Musk' scam, prosecutors say"* (Bradenton Herald/Yahoo, October 27, 2025), *"Two Utah men plead guilty to attempting to scam 94-year-old out of thousands of dollars"* (ABC4 Salt Lake, October 8, 2025), and *"Police: Elder scam costs East Rockaway woman $117G"* (Newsday, October 7, 2025), spanning Texas, Massachusetts, Florida, Utah, and New York.

Many of the enforcement articles cover the same high-profile cases from multiple outlets. The $65 million multinational fraud ring dismantled in August 2025, with the assistance of "Youtube Scambaiters", generated coverage across dozens of publications. Individual arrests and sentencings,

particularly when they involve dramatic details, receive attention: *"Last of 8 defendants sentenced in money laundering 'phantom hacker' conspiracy"* (Mahoning Matters, September 14, 2025), *"Five plead guilty in $9.3M tech support scam targeting elderly"* (KTTN, September 29, 2025), *"Saipan woman gets 71 months in prison for bitcoin fraud targeting senior victims"* (The Block, April 28, 2026), *"New Jersey brothers indicted for alleged financial scam targeting seniors"* (Brooklyn Eagle, September 3, 2025), *"Two men pleaded guilty in connection to $100K scam of Petersburg senior"* (Petersburg Pilot, October 31, 2025), and *"Man sentenced to prison for fraud scheme that targeted elderly Arizonans"* (KTAR News, March 17, 2026).

Meanwhile, the everyday, small-dollar cases that make up most reported elder fraud (the FTC puts the median 60+ loss near $900) rarely surfaced in our monitoring, even though they are far more common than the headline-grabbing megacases.

Prevention and Education

Prevention and education articles covered awareness campaigns, community workshops, training programs, scam-warning advisories from local police, and expert advice columns aimed at older adults and their families. The corpus contains warnings issued by sheriffs, attorneys general, librarians, banks, senior-center directors, congressional offices, and high-school cybersecurity clubs, typically in the form of local-TV segments and regional-newspaper columns. Representative headlines include *"Police warn senior citizens of prevalence of scams"* (Mesa Valleys Progress, October 8, 2025), *"Schuyler County Warns Seniors: Holiday Scams on the Rise"* (Finger Lakes Daily News, November 28, 2025), *"Cybercrime expert, sheriff warn Knox seniors about fast-evolving scams"* (Your Ohio News, November 22, 2025), *"Iowa State Extension to host senior fraud prevention program March 5 in Carroll"* (Carroll Times Herald, February 19, 2026), *"Over 150 Seniors Attend Assemblymember Mike Fong's 'Scam Stopper Fair' in Monterey Park"* (Colorado Boulevard, October 23, 2025), *"Pa attorney general warns seniors about ongoing Medicare scam"* (WFMZ, September 24, 2025), and *"FBI Warns Louisiana Seniors: Watch Out for This 'Phantom' Scam"* (KPEL 96.5, September 2, 2025). Notable initiatives included:

- Fulton County, Georgia's cyber scam training program for seniors (August 2025)
- SSA OIG "Slam the Scam Day" outreach and the FTC *Pass It On* campaign, continuing federal prevention programming
- Senior Medicare Patrol (SMP) volunteer presentations in community senior centers
- Silicon Valley's AI safety course for seniors (September 2025)
- "Savvy Senior" syndicated columns and similar advisory content in regional newspapers
- Police-department "uptick in scams" advisories pushed through local broadcast outlets

Other typical examples from the corpus include *"Senior Scam Seminar on Slate in Stafford Township"* (The SandPaper, January 22, 2026), *"December Scam Patrol: Free State Events Warn Seniors and Families of Rising Fraud"* (MyChesco, December 1, 2025), and a Connecticut attorney general campaign to curb online exploitation of seniors (Fox 61, January 7, 2026).

The volume of prevention coverage is substantial, suggesting that reporters and local institutions are devoting real attention to helping seniors and families recognize and avoid scams *before* they become victims.

Investment and Cryptocurrency Dominance

Investment and cryptocurrency scams aligned with the FBI data showing investment fraud as the dominant loss category. Coverage frequently emphasized:

- Pig-butchering operations, often linked to international organized crime
- Cryptocurrency as both the scam vehicle and the payment method
- Individual losses in the hundreds of thousands of dollars
- The difficulty of recovery once cryptocurrency is transferred

Specific stories from the corpus capture the per-victim damage that headlines often led with: *"Parksville woman loses $200,000 in crypto scam"* (Times Colonist, October 10, 2025), *"Police recover money stolen from elderly Pleasant Hill resident in $350,000 crypto scam"* (CBS News, January 13, 2026), *"Man gets 21 years for crypto fraud targeting seniors in their 90s"* (Tampa Beacon, February 21, 2026), *"Crypto ATM scams rising, stealing millions from Alabamians"* (WSFA, November 21, 2025), and *"Grand Island Enforces New Ordinance to Combat Cryptocurrency Fraud"* (Blockmanity, December 30, 2025).

The AI Attention Cycle

AI-related articles showed a distinctive coverage pattern: intense interest in fall 2025, with a long tail through spring 2026. Coverage peaked in September–October 2025, driven by the Reuters/ Malwarebytes investigation into AI chatbots generating phishing content (Malwarebytes, September 16, 2025), and by several high-profile deepfake cases. AI coverage did not collapse the way many emerging-tech stories do; it stabilized at roughly 6–15 articles per month and trended upward again in the spring, with headlines like *"AI Voice Clone Scams Are Becoming Harder for Seniors to Detect"* (Saving Advice, May 9, 2026), *"AI-driven scams exploit Medicare changes to target seniors"* (MSN, May 15, 2026), *"Pa. scams rise as AI enhances fraud tactics"* (WGAL, January 8, 2026), *"Port Richey senior loses $47K in AI romance scam"* (WLTX, September 2, 2025), and *"AI-Powered Scams Devastates Seniors, Draining Billions"* (Cord Cutters News, August 31, 2025).

The AI capabilities that made headlines in October 2025 have continued to advance, and the corpus suggests the media has *not* lost interest, contrary to the typical "news-cycle decay" pattern for emerging-tech stories.

Legislation: Low Coverage Volume in the Corpus

Legislation and policy articles included coverage of proposed bills, attorney general policy actions, regulatory announcements, hearings, and commemorative-resolution efforts.

The volume of legislative coverage is low given the substantive activity actually happening at the federal and state levels during the monitoring period: the SCAM Act's Senate passage in December 2025, the GUARD Act, multiple state-AG announcements, the CFPB Interagency Statement implementation, congressional hearings on AI-driven scams, and so on.

The few stories the corpus did surface appeared at a fraction of the rate of enforcement coverage. They included *"Britt-led GUARD Act advances in Senate to combat senior-targeted fraud"* (Yellowhammer News, February 17, 2026), *"Financial Exploitation Prevention Act introduced to combat scams against seniors"* (WVNS, September 25, 2025), *"Gillibrand touts legislation to protect seniors from scammers"* (Rome Sentinel, December 10, 2025), *"Proposed act aims to protect Illinois senior citizens from financial scams"* (25 News Now, November 22, 2025), *"Consumer Reports backs bipartisan legislation to combat predatory online scams"* (Consumer Reports Advocacy, April 2, 2026), *"D.C. Attorney General sues Crypto ATM operator for alleged CPPA and elder-exploitation violations"* (Consumer Finance and Fintech Blog, September 18, 2025), and the American Bankers Association's *"Letter to the House on the Safeguarding Consumers from Advertising Misconduct or SCAM Act"* (ABA, February 19, 2026).

Part of that gap reflects where this kind of news is published, in trade outlets rather than mainstream local media, so we read it cautiously as a feature of our monitoring sample rather than as proof of how visible the response is to the public.

Emerging Scam Variants

One of the primary values of real-time news monitoring is the ability to identify emerging scam variants before they appear in official annual data. Our corpus revealed several trends worth watching:

The "Phantom Hacker" Multi-Stage Attack

First flagged by the FBI in 2023, the Phantom Hacker scam appeared repeatedly in our corpus throughout the monitoring period. Local reporting picked it up explicitly: *"'Phantom Hacker' scam targets seniors using three phases"* (Sun Community News, September 11, 2025), *"FBI Warns Louisiana Seniors: Watch Out for This 'Phantom' Scam"* (KPEL 96.5, September 2, 2025), and the enforcement bookend, *"Last of 8 defendants sentenced in money laundering 'phantom hacker' conspiracy"* (Mahoning Matters, September 14, 2025). Multiple articles described the same three-stage pattern (tech support → bank impersonation → government impersonation), suggesting this variant has become a standard playbook rather than an isolated tactic. The FBI has attributed over $1 billion in cumulative losses to the Phantom Hacker scam, with tech support fraud reaching $2.1 billion across all ages in 2025 alone.

Disaster Fraud

Hurricane Helene revealed another dimension of elder fraud: disaster targeting. Scammers exploited the hurricane's aftermath to target older victims with fake FEMA claims, fraudulent charity appeals, and identity theft schemes. As U.S. Attorney Sandra J. Hairston (Middle District of North Carolina) warned: "These criminals take advantage of victims before, during and after a natural disaster strikes, targeting people when they are most vulnerable". Disaster fraud is difficult to quantify because it is spread across multiple crime categories, but it represents a recurring exploitation of community

crises and was a notable theme during our monitoring period as recovery efforts and follow-up enforcement actions continued through 2025–2026.

Romance-to-Investment Pipeline

A growing number of articles described scams that began as romance frauds and transitioned into investment scams. The scammer builds a romantic relationship, then introduces the victim to cryptocurrency trading. This hybrid approach appears to be a deliberate strategy to combine the emotional manipulation of romance scams with the higher dollar yield of investment fraud. Examples from the corpus include *"Romance scams target older adults with cryptocurrency schemes"* (WBAY, February 13, 2026), *"Florida AG: $5.4M stolen in a crypto 'romance-turned-investment scam' found, recovered"* (Fox 35 Orlando, April 15, 2026), and the surprising counter-example *"ChatGPT Helps Expose a $1 Million Crypto 'Pig-Butchering' Scam"* (Decrypt, December 9, 2025), one of the very few articles in the corpus in which AI appeared on the defensive side of the ledger rather than the offensive one.

Doctor Impersonation

In February 2026, a Fresno doctor warned that scammers were using his identity in an AI-driven scheme to target his older patients. This represents an evolution beyond generic impersonation: scammers are now impersonating individuals with a specific, trusted relationship to the victim.

The Story the Data Tells

Reading 1,910 elder fraud stories over ten months produces an impression that no individual statistic can convey: this is a crisis that touches every state, every type of community, and every level of income.

The media covers elder fraud as a collection of discrete events, an arrest here, a victim there, a new technology in the background. What it does not cover is the cumulative picture: a $7.748 billion annual reported-loss industry that grew 59 percent year-over-year in 2025, spread across more than 201,000 documented complaints (FBI IC3 2025), while the coordinated response to it remains fragmented and hard for the public to see in any single story.

A companion visual timeline, *Ten Months in Two Columns*, renders these same ten months month by month, each month's reported scam activity set beside the enforcement, court, legislative, and awareness response.

Chapters 6 and 7 turn from the threats to the response: who is fighting back, from families and communities outward to the states, the private sector, and the federal agencies (Chapter 6), and what the legislative landscape looks like (Chapter 7).

Data Sources for Chapter 5:

- seniors.hcsk.org news corpus: 1,910 articles, August 2025–May 2026. The 42 distinct headlines quoted in this chapter are verbatim titles from the corpus. Names have been anonymized.
- Phantom Hacker cumulative-loss figure (over $1 billion): FBI statement as relayed by corpus articles (e.g., KPEL 96.5, September 2, 2025; AOL, October 17, 2025), in ARTICLES/2025/; FBI IC3 *2025 Internet Crime Report* (tech-support fraud data)
- U.S. Attorney Sandra J. Hairston, Middle District of North Carolina, Hurricane Helene fraud statement
- U.S. Senate Special Committee on Aging, *Age of Fraud*, 2025 (disaster fraud)

CHAPTER 06

Chapter 6: Who Is Fighting Back

It starts at the kitchen table

The defense against elder fraud begins in a kitchen, at a bank counter, in a single phone call, and radiates outward from there. An older woman hears the pressure in a "Treasury agent's" voice and hangs up. A son, uneasy about a call his mother just took, phones her back on a number he already has, not the one that rang her. A teller slows down a wire that doesn't feel right. Case for case, they are among the most effective defenders that exist.

This chapter follows the defense outward, from the people closest to the victim, to the community workers and state offices around them, to the banks and platforms that move and host the money, to the federal apparatus farthest away. At every ring it finds the same two things: capable people and institutions doing real work, and no reliable thread connecting any of them to the next. That gap, not any shortage of effort, expertise, or actors, is the subject of this chapter, and the reason for the proposal in Chapter 9.

The people closest: family, caregivers, and older adults themselves

The innermost ring of the defense is also the least visible in any dataset: the family members, caregivers, social workers, and older adults who meet the scam in real time, before it ever becomes a complaint.

Family, caregivers and social workers

The single most common early-warning system for elder fraud is an adult child, a son or daughter who notices that a parent has grown secretive about money, is taking calls at odd hours, or has made a withdrawal that does not fit a lifetime of habits. Adult children are exactly who the bank-sector tools described later in this chapter are built to enlist: the Trusted Contact a customer names, the limited account visibility that banks such as Wells Fargo, Huntington, and KeyBank now offer, the confidential call an institution can place when something looks wrong. None of that infrastructure functions without a trusted person on the other end of it.

Caregivers, paid and family alike, are often the first to see the warning signs and the best placed to intervene gently. The same closeness can cut the other way, which is why the answer is better-supported and better-supervised caregivers, not fewer of them.

Social workers occupy a related place in this inner ring, not as family, but as the professionals who often know an individual older adult best. The geriatric or clinical social worker, the hospice or hospital care manager, and, for veterans, the VA social worker see the same person on a regular schedule and learn their baseline: how they usually handle money, who is usually around them, what is normal for them. That familiarity is exactly what lets them catch what a stranger could not (a benefit check suddenly redirected, a "new friend" who appeared from nowhere, a once-meticulous bill-payer falling behind), and in many states the law makes them mandated reporters of the exploitation they suspect. What they lack is what everyone else in this ring lacks: not skill or duty, but a shared channel that guarantees the concern they raise reaches the bank, the police, and the federal system fast enough to matter.

Seniors themselves

The most underleveraged defenders are older adults themselves, and the framing matters. The dominant version of the elder-fraud story casts the senior as a passive victim; the evidence does not support it. Older adults recognize and turn away scam approaches every day, they hang up on the spoofed call, decline the gift-card demand, and walk away from the kiosk, and many then do the thing that protects the next person: tell a friend, raise it at the senior center, or report it so the pattern enters the record. Peer-to-peer education, an older adult showing other older adults what a scam call actually sounds like, carries a credibility no government brochure can match, as the next section makes concrete. Treating older adults as the agents of their own protection, rather than as a problem to be managed, is both more accurate and more effective. The older adult is at once the first line of defense and the very person the scam is aimed at.

What this layer lacks is not commitment but coordination and simplification. A daughter, a caregiver, an APS worker, and an older adult who has just been targeted may all be defending against the same scheme on the same day with no shared number to call, no common message to repeat, and no assurance that what one of them reports ever reaches the others. That is the gap a single shared channel is built to close, and the reason it is designed to be usable by a family at a kitchen table, not only by an investigator at a federal agency.

From victim to advocate

In Montgomery County, Maryland, two women who together lost much of their savings to scammers have become among the most effective anti-fraud educators in their community.

A retired nurse in a Maryland suburb lost nearly $600,000 to a government-impersonation scam in 2023–2024. The scammers claimed to be from her local police, then transferred her to a fake FBI agent. Over months, she withdrew large portions of her savings and dropped them at a designated locker at a Washington, D.C., courthouse, believing she was helping take down a fentanyl ring. "I grew up in a culture that had respect for government officials and law enforcement", she said in subsequent advocacy.

A second Montgomery County resident lost $10,000 to a scammer claiming there was a murder warrant for her arrest. Ordered to deposit cash via a cryptocurrency kiosk, she complied. Afterward, she described feeling that her sense of self had been wiped away in an instant.

Both women now volunteer through the Montgomery County Police's "Keeping Seniors Safe" program, working with the International Association of Financial Crimes Investigators to train seniors in assisted-living facilities and community centers. They illustrate one underused resource in elder-fraud prevention: the victim-to-advocate pipeline. No brochure, no PSA, no government website carries the credibility of a person who says: *"This happened to me. Here is how. Don't let it happen to you"*.

The same pipeline runs nationwide. One Florida woman has publicly described watching her elderly mother be drawn into an online romance scam. In 2023 she founded the nonprofit Stop Elderly Scams with the mission to protect senior citizens from scammers who foster relationships for financial gain.

The community that is physically there

One ring out sit the people a senior actually encounters in an ordinary week, and who are often the last to stand between the senior and the money: the bank teller at the counter, the Adult Protective Services investigator, the local police officer, the senior-center director, the clinician. The bank's institutional machinery (Trusted Contacts, fraud-detection AI, dedicated investigation units) sits a ring further out, among the national private actors; but at the counter it comes down to one employee choosing to slow down. Much of the rest of this community layer is held together by a state or a federal agency.

The aging-services network

That federal home is the Administration for Community Living (ACL), the HHS operating division that funds and coordinates the Older Americans Act network: the state units on aging and the national network of Area Agencies on Aging, the local organizations that coordinate senior services in communities across the country. They are reachable through a single public number, the Eldercare Locator (1-800-677-1116), which also routes callers to their local Adult Protective Services (APS). APS is, in many states, the public agency legally designated to receive and investigate reports of suspected financial exploitation: the public counterpart to the bank's Trusted Contact, a channel through which a worried clinician, neighbor, or relative can escalate a concern to a caseworker empowered to act. Eligibility varies by state, and APS most often serves older or vulnerable adults who cannot fully protect themselves.

Beyond the community sits the first tier of government built to investigate and prosecute these crimes: the states.

The States: Attorneys General, and Puerto Rico's Secretary of Justice

State attorneys general occupy a unique position in elder-fraud enforcement. They are close enough to victims to understand local patterns, empowered to bring criminal and civil actions, and politically motivated to demonstrate visible results. Across these offices in the 50 states, DC, and Puerto Rico, capacity varies enormously.

States with dedicated elder-fraud units (current as of 2026-05)

- **Pennsylvania, Elder Exploitation Section** (launched in late 2025 by AG Dave Sunday). Pennsylvania has the fifth-largest senior population in the country (behind California, Florida, Texas, and New York).
- Arizona, Elder Affairs Unit + Task Force Against Senior Abuse (TASA) (under AG Kris Mayes). TASA was split in 2023 into a law-enforcement coordination unit and a community-engagement unit. On May 22, 2026, AG Mayes issued a consumer advisory warning Arizona's veterans of ten scams targeting military benefits, pensions, and personal information, from VA impersonation and pension poaching to benefits-buyout and claims-shark schemes.
- **Connecticut, Elder Justice Hotline** (1-860-808-5555).
- California, Division of Medi-Cal Fraud & Elder Abuse. Operates as both the state's Medicaid Fraud Control Unit and its Elder Abuse prosecution arm.
- New York, Texas, Florida, Maryland, Massachusetts, Washington, Oregon, Illinois, New Jersey, all maintain identifiable elder-fraud capacity within their consumer-protection divisions, varying in dedicated-unit status.

The private sector at national scale: banks, platforms, and nonprofits

Farther out sits a layer that operates nationally rather than locally: the banks and broker-dealers that hold the money, the platforms that carry the scam's first contact, and the nonprofits that educate and support.

Bank-sector elder protection, the trusted-contact era

Across the largest U.S. retail banks and broker-dealers, four design patterns are now table stakes:

- **Trusted Contact frameworks.** The CFPB's December 2024 *Interagency Statement on Elder Financial Exploitation*, signed by five federal financial regulators plus FinCEN and the state regulator coalition, formalized a framework that Charles Schwab and FINRA-member broker-dealers have operated since 2017 under FINRA Rule 4512. A Trusted Contact does not have transactional authority; the contact exists so that an institution that suspects exploitation has a confidential channel to confirm or escalate concerns. This is the bank-side analog of a parallel-notification design.

- **Caregiver banking access.** Keynova Group's Q4 2025 Online Banker Scorecard, an evaluation of 18 major banks, found that Wells Fargo, Huntington, and KeyBank were among the first to offer controlled or limited account-information access for trusted family members or professional advisors, with U.S. Bank adding the feature by early 2026. This is the first generation of "joint guardrails without joint signing authority", the user retains control while a trusted family member retains visibility.
- **AI behavioral fraud detection.** Bank of America's Erica virtual assistant has crossed 3 billion client interactions by 2025 and serves 42 million consumer clients. Its layered Zelle controls, daily-tuned models, MFA/biometrics, name-match checks, and "speed-bump" warnings establish a per-customer behavioral baseline and pause transfers when the pattern deviates. JPMorgan Chase, Wells Fargo, and Schwab operate analogous systems.
- Dedicated elder-customer investigation units. Charles Schwab's Senior and Vulnerable Investor Investigations Team focuses on clients aged 60+ or with diminished capacity. JPMorgan Chase's Elderly and Vulnerable Persons Team is the equivalent at the retail-banking side. Wells Fargo's investigation team operates with similar scope.

In November 2025, JPMorgan Chase announced the largest fraud and scam prevention initiative in the firm's history, including nearly $14 million in philanthropic investments, more than 20 public workshops during International Fraud Awareness Week, and ongoing workshops across more than 5,000 branches. Chase Consumer Banking CEO Jennifer Roberts framed the announcement in language that maps directly onto this report's diagnosis: *"Protecting our customers from fraud and scams requires a united front, banks, technology companies, social media platforms, and law enforcement all have a role to play"*.

The Bank of America Foundation, JPMorgan Foundation, and Wells Fargo Foundation all funded community-based senior-fraud education in 2025, including a $200,000+ Wells Fargo Foundation grant that expanded the San Diego Seniors Community Foundation's elder-fraud prevention work across Southern California.

Platform-sector scam-ad enforcement, the verification era

The two largest platform ecosystems, Meta (Facebook / Instagram) and Google, have published 2025 enforcement metrics at scale:

Platform	2025 metric
Meta	159 million scam ads removed for policy violations
Meta	10.9 million accounts disabled on Facebook and Instagram associated with criminal scam-center networks
Meta	92 percent of scam ads taken down before any user reported them
Meta	150,000 accounts disabled in the second Joint Disruption Week with the Royal Thai Police since December 2025 (an earlier week removed over 59,000 pages and accounts)
Google	8.3 billion ads blocked or removed for policy violations
Google	24.9 million advertiser accounts suspended; 602 million scam-tagged ads
Google	99 percent of policy-violating ads caught before reaching a person

Source: Meta 2025 Integrity Reports and March 2026 disruption announcement; Google 2025 Ads Safety Report. All platform takedown and prevention percentages in this table are company-reported.

Both companies signed the United Nations Office on Drugs and Crime Industry Accord Against Online Scams and Fraud at the Vienna Global Fraud Summit in March 2026, alongside Adobe, Amazon, Levi's, LinkedIn, Match Group, Microsoft, OpenAI, Pinterest, and Target. Google helped launch the National Elder Fraud Coordination Center (NEFCC) in 2025, a public-private coalition designed to reduce elder fraud through shared coordination and the creation of actionable investigative packages for law enforcement.

Meta is expanding its verified-advertiser program with the stated goal of 90 percent of ads revenue coming from verified advertisers by the end of 2026 (up from 70 percent as of March 2026).

Both platforms have rolled out on-device or near-real-time AI scam detection: Google's Scam Detection in Google Messages and Phone by Google flags suspicious patterns in calls and texts; Meta's Q3 2025 Integrity Report documents AI-powered enforcement against Criminal Scam Syndicates.

Microsoft, OpenAI, Anthropic, and the AI-platform layer

Three other technology actors operate further upstream of the ad-network surface, at the account-infrastructure, foundation-model, and policy-publication layer where many scam workflows now originate and where many defenses must be applied. The work each does is less consumer-visible than Meta's or Google's ad takedowns, but no less important.

Microsoft. The Microsoft Digital Crimes Unit (DCU), founded in 2008, conducts court-ordered takedowns and supports law-enforcement raids against criminal online infrastructure. The most directly elder-fraud-relevant Microsoft action of the past two years is the June 5, 2025 transnational tech-support-scam disruption: working with India's Central Bureau of Investigation, Japan's National Police Agency, and the Japan Cybercrime Control Center, Microsoft's DCU helped dismantle overseas call centers running tech-support fraud schemes that impersonated Microsoft and targeted Japanese seniors. The operation produced 19 raid locations and the takedown of 2 illegal call centers, with

approximately 200 victims identified, around 90 percent of whom were over age 50. As Microsoft Assistant General Counsel Steven Masada put it: *"We must continue to look at the full ecosystem in which these actors operate and coordinate with multiple international partners to meaningfully address cybercrime"*.

In the same announcement, Microsoft reported that its DCU has taken down approximately 66,000 malicious domains and URLs globally since May 2024. Microsoft is also one of eleven signatories to the UN Office on Drugs and Crime's Industry Accord Against Online Scams and Fraud, signed at the Vienna Global Fraud Summit in March 2026, and as background, the December 2023 Storm-1152 takedown (a U.S. District Court, Southern District of New York seizure of infrastructure that had created and sold an estimated 750 million fraudulent Microsoft accounts) remains a foundational example of Microsoft DCU's enforcement against the cybercrime-as-a-service ecosystem that elder-fraud operations rely on.

OpenAI. OpenAI's Usage Policies (most recent update October 29, 2025) explicitly prohibit using its services for *"deceit, fraud, scams, spam, or impersonation"* (in the *Empower people* section) and for *"use of someone's likeness, including their photorealistic image or voice, without their consent in ways that could confuse authenticity"* (in the *Respect privacy* section, directly naming voice cloning and deepfake video). The most consequential primary document, however, is OpenAI's recurring Disrupting malicious uses of AI threat-report series. The June 2025 edition (46 pages, authored by Ben Nimmo, Albert Zhang, Sophia Farquhar, Max Murphy, and Kimo Bumanglag) documents ten cases of OpenAI banning accounts engaged in social engineering, cyber espionage, deceptive employment schemes, covert influence operations, and scams.

One case study is directly elder-fraud-relevant: Operation "Wrong Number", a transnational task-scam network OpenAI banned for generating recruitment-style scam messages in six languages (English, Spanish, Swahili, Kinyarwanda, German, Haitian Creole) and translating conversations between operators and targets in a documented *"ping → zing → sting"* pattern, cold contact promising high pay for trivial work, then enthusiasm-generation with motivational messages and small upfront payments, then money extraction through deposits, cryptocurrency purchases, and handling fees. In OpenAI's own words: *"OpenAI's policies strictly prohibit use of output from our tools for fraud or scams. We are dedicated to collaborating with industry peers and authorities to understand how AI is influencing adversarial behaviors and to actively disrupt scam activities abusing our services"*.

Anthropic. Anthropic's Acceptable Use Policy (effective September 15, 2025) is the most explicit upstream commitment we have verified from the foundation-model layer. It prohibits using Claude to *"generate content for fraudulent activities, schemes, scams, phishing, or malware that can result in direct financial or psychological harm"*, to *"impersonate a human by presenting results as human-generated"*, and to *"engage in deceptive or abusive practices that exploit individuals based on age, disability or a specific social or economic situation"*.

Nonprofit organizations

A layer of nonprofit and community organizations works to fill gaps that a fragmented response leaves unaddressed. It ranges widely in scale and focus: national consumer-protection helplines and scam-

tracking programs; state and regional nonprofits that deliver senior-tailored education through community presentations, newsletters, and law-enforcement partnerships; organizations that center the post-victimization experience, giving victims and families a place to learn, share, and find recovery resources; and a long tail of volunteer groups operating where larger national programs do not reach.

Their methods differ, but the work is consistent and hard to replace: prevention education, victim support, and keeping elder fraud in public conversation.

The federal government

Farthest from the kitchen table sits the federal government: the layer with the deepest investigative reach and the most data.

The ten lead federal actors

Federal actors maintain elder-fraud programs of meaningful scale: nine executive-branch agencies and the U.S. Senate Special Committee on Aging, the congressional committee that oversees the field and runs its own fraud hotline. They are grouped below by function, not ranked.

Intake and enforcement

1. FBI / Internet Crime Complaint Center (IC3)

In 2025, the FBI's Internet Crime Complaint Center received 201,266 complaints from adults aged 60 and over, a 37 percent increase from 2024, reporting total losses of $7.748 billion (up 59 percent). The average loss per complaint reached $38,500, and 12,444 complainants reported losses exceeding $100,000.

Beyond data collection, the FBI's Recovery Asset Team (RAT) works to freeze stolen funds before they are transferred beyond recovery. In 2025, the RAT processed 3,900 Financial Fraud Kill Chain (FFKC) incidents, freezing $679 million out of $1.16 billion in attempted theft, a 58 percent success rate. For elder fraud specifically, the FFKC initiated 642 incidents involving victims aged 60+, freezing $32.9 million of the $65.4 million at risk in those cases, a 50.3 percent freeze rate. The contrast tells the story: when fraud is reported fast enough to act, roughly half the money can be frozen, but those 642 cases are a fraction of the 201,266 elder fraud complaints filed in 2025, and the $32.9 million frozen is less than half of one percent of the $7.748 billion lost. Recovery is not impossible; it is a race against the clock that today's fragmented response usually loses. The elder FFKC workload breaks down by crime type: tech support / account takeover scams dominate at 360 incidents (56%), followed by business email compromise (BEC) at 104 (16%) and investment fraud at 64 (10%).

Operation Level Up, launched in January 2024 jointly with the U.S. Secret Service, uses IC3 complaint data to identify ongoing cryptocurrency-investment scams and notify victims *before* their losses escalate. Since launch:

- Over 8,000 victims notified
- An estimated $500 million in additional losses prevented
- In 2025 alone, 3,780 victims notified and an estimated $225.9 million saved
- 78 percent of notified victims had no idea they were being scammed at the moment of FBI contact
- 38 victims were referred to FBI Victim Specialists for suicide intervention in 2025

Recovery is also possible after the fact where blockchain tracing works: in a DOJ-reported Ohio case, an older adult who wired $425,000 to cryptocurrency exchanges in a tech-support scam achieved full restoration through blockchain tracing, asset seizure, and DOJ remission proceedings (DOJ EAPPA 2025).

The **Transnational Elder Fraud Strike Force**, also FBI-led, coordinated eleven joint operations with India's Central Bureau of Investigation in 2024, producing 215+ arrests, a 700 percent increase over 2023 (DOJ EAPPA 2025), and reports a cumulative 27 operations and 475+ arrests since 2022 (FBI IC3 2025). The program is expanding to other countries.

Hotline / portal: ic3.gov for reporting; FBI field-office fbi.gov/contact-us/field-offices.

2. Federal Trade Commission (FTC)

The FTC fights elder fraud on three fronts: enforcement, data, and education.

Enforcement. The FTC returned more than $311 million to consumers of all ages in fiscal year 2025. Significant settlements and consumer-redress distributions during our monitoring period included a deceptive tech-support and PC-repair scheme (more than $25.5 million in consumer refunds following a $26 million settlement), a major sweepstakes marketer the FTC found targeted older and lower-income consumers (more than $18 million in consumer refunds from an $18.5 million settlement fund), and a large national retailer that settled FTC allegations it let scammers use its in-store money-transfer services to defraud consumers ($10 million settlement, no admission of wrongdoing).

Data. The FTC publishes the *Protecting Older Consumers* report annually (most recent: December 2025) and the *Consumer Sentinel Network Data Book* (most recent: March 2025, covering 2024). The Sentinel Data Book aggregates more than 6.5 million consumer reports annually across dozens of categories. The Protecting Older Consumers report provides the most cited estimate of elder fraud's true scale: $10.1 to $81.5 billion annually (the $10.1B floor assumes everyone who lost $10,000 or more reported; the $81.5B ceiling extrapolates from the FTC's 2.0 percent and 6.7 percent reporting-rate research).

Education. The FTC's "Pass It On" campaign distributed 1.7 million educational items in fiscal year 2025; over the same period FTC staff took part in nearly 500 outreach events, about 140 of them specifically focused on older adults.

Hotline / portal: reportfraud.ftc.gov; Office of Public Affairs at opa@ftc.gov.

3. Department of Justice / Elder Justice Initiative

The DOJ remains the most visible actor in elder-fraud enforcement. During our ten-month monitoring period (August 2025–May 2026), justice.gov published 56 press releases announcing charges, plea agreements, and sentencings in elder fraud cases, averaging more than one per week.

The EAPPA 2025 Annual Report to Congress documents the most recent reporting period: 283 criminal and civil enforcement actions, 608 defendants, over $2.36 billion stolen from more than one million older victims. Thirty-six percent of cases involved international schemes. Seventy-eight percent of U.S. Attorney's Offices nationwide engaged in some form of elder-justice enforcement. The Department held over 1,000 public awareness and training events, reaching nearly 15 million Americans.

The DOJ's most significant action during our monitoring period was the takedown of a $65 million multinational fraud ring announced in August 2025, prosecuted by the U.S. Attorney's Office in San Diego, resulting in indictment of 28 members of a transnational organized-crime network operating through overseas call centers.

Other significant DOJ actions during our monitoring period:

- **Operation Silver Shores** (October 2025): a transnational organized crime takedown
- Multiple romance-scam prosecutions, including one defendant charged with $8+ million in fraud
- Sentencing of a defendant to 18 years for a $15 million elder fraud scheme in Florida
- A transnational call-center case in which an indicted lead defendant has been tied, per the 2025 EAPPA report, to an estimated $150–200 million in elder fraud losses (trial pending)
- A "lead list" prosecution in which the defendant maintained personal data on more than 7 million older Americans, names, phone numbers, financial details, sold to fraud operations as targeting data. A co-defendant in the same family separately pled guilty to laundering $1.6 million in fraudulent funds. The case illustrates the industrial supply chain behind elder fraud.

The DOJ also funds the National Elder Fraud Hotline (1-833-FRAUD-11 / 1-833-372-8311), operated by the Office for Victims of Crime. Since its 2020 launch, the hotline has received 202,050 total calls. It currently operates Monday–Friday, 10 a.m. to 6 p.m. Eastern Time, a limitation Chapter 9 returns to.

Hotlines / portal: justice.gov/elderjustice; **1-833-FRAUD-11** for the hotline.

4. SSA Office of Inspector General (SSA OIG)

The SSA OIG focuses on Social Security impersonation scams, the long-running fraud variant in which scammers pose as SSA officials and threaten Social Security number suspension, arrest, or benefit termination. Since July 2021, SSA OIG has published 17 quarterly scam reports (Issues 2–18) documenting the trend. The series shows:

- Peak FY 2019 – FY 2021: more than 150,000 SSA-related scam allegations per quarter, with some quarters over 225,000

- April 2022 onward: fewer than 10,000 allegations per month (roughly 30,000 or fewer per quarter), an approximate 80–90 percent decline from the per-quarter peak
- SSA-impersonation remains a top reported government-imposter scam to the FTC despite the decline

The SSA OIG also leads the annual "Slam the Scam" Day campaign, observed during the first week of March (National Consumer Protection Week).

Hotlines / portal: ssa.gov/scam (online, 24/7); 1-800-269-0271 for the OIG hotline (weekdays, business hours ET).

5. U.S. Secret Service (USSS)

The U.S. Secret Service investigates financial crimes, including elder fraud, through its Cyber Fraud Task Forces (CFTFs). Of the ten federal actors in this inventory, the Secret Service does work that is highly relevant to elder fraud yet operates largely out of the public eye. In April 2026, the U.S. Secret Service published a dedicated Elder Fraud Advisory documenting government-impersonation, tech-support, investment, and romance-scam patterns and providing prevention guidance.

USSS participation in Operation Level Up (jointly with the FBI) has been a major factor in the program's documented success. In June 2025, just before the opening of our monitoring window, the U.S. Secret Service announced the largest-ever seizure in agency history of funds related to cryptocurrency confidence scams: $225.3 million in cryptocurrency, with more than 430 suspected victims worldwide, including victims identified across Texas, Arizona, Virginia, Iowa, California, and other states (civil forfeiture complaint, U.S. District Court for the District of Columbia, June 18, 2025). "Pig butchering" confidence schemes of this type disproportionately target older Americans, who account for the largest share of cryptocurrency investment fraud losses reported to the FBI IC3. The USSS's existing investigative mandate, financial crimes broadly, gives it natural authority on the crypto-conversion and gold-bar logistics that increasingly characterize large-loss elder fraud.

Portal: secretservice.gov/investigations/elderfraud; 2026 Elder Fraud Advisory PDF.

6. U.S. Postal Inspection Service (USPIS)

The USPIS is the federal investigative agency for mail fraud, historically a major elder-fraud vector and still significant for sweepstakes scams, fake-check schemes, and physical-mail-based government impersonation. The USPIS's *FY 2024 Annual Report* documents:

- A COVID-era surge in mail theft that reversed in FY 2024: mail-theft complaints fell 20 percent and letter-carrier robberies fell 27 percent after the May 2023 launch of Project Safe Delivery (USPIS FY2024 Annual Report)
- 5,563 reports of violent crime against postal employees in FY 2024 (threats, assaults, and robberies)
- 1,259 mail-theft convictions in FY 2024, with arrests for robberies up 32 percent

USPIS's FY 2024 results show what a single agency can do with a defined operation: after years of pandemic-era escalation, Project Safe Delivery moved mail-theft and robbery numbers in the right

direction. USPIS's mandate also gives it natural authority on the courier-pickup-of-cash variant that increasingly characterizes the high-loss government-impersonation playbook.

Hotline / portal: uspis.gov; 1-877-876-2455.

7. HHS Office of Inspector General (HHS OIG)

The HHS OIG's elder-fraud mandate centers on Medicare and Medicaid fraud. Senior-targeted patterns include hospice enrollment scams (HHS OIG's hospice oversight has documented schemes that enroll Medicare beneficiaries without their consent, including through door-to-door approaches), durable medical equipment scams, and Medicare-card impostor scams.

The HHS OIG also runs long-term-care-facility fraud enforcement initiatives. The OIG also publishes the *Medicaid Fraud Control Units Annual Report* documenting state-level Medicaid Fraud Control Unit (MFCU) activity. The 53 MFCUs operate in all 50 states, DC, Puerto Rico, and the U.S. Virgin Islands. California's MFCU is part of the state AG's Division of Medi-Cal Fraud & Elder Abuse, described earlier in this chapter under the states.

Two complementary HHS/ACL programs warrant mention here even though they sit outside the OIG's strict enforcement role:

- **Senior Medicare Patrols (SMP)**, ACL-funded grant programs in every state plus territories. Since 1997, SMP programs have helped Medicare beneficiaries identify, report, and recover improper Medicare billing. Find your local SMP at smpresource.org or call 1-877-808-2468.
- State Health Insurance Assistance Program (SHIP), ACL-funded one-on-one Medicare counseling. 1-877-839-2675 national technical-assistance line; shiphelp.org.

Hotlines / portal: oig.hhs.gov/fraud/report-fraud; 1-800-HHS-TIPS (1-800-447-8477).

Regulators and framework-setters

8. Consumer Financial Protection Bureau (CFPB)

The CFPB's elder-fraud work focuses on prevention, financial-institution coordination, and post-fraud recovery. Three primary publications anchor its contribution to the federal response:

- Recovering from Elder Financial Exploitation: A Framework for Policy and Research (September 2022). The principal federal analysis of what financial recovery actually requires. Its four-stage framework, identification, reporting, investigation, return of funds, is the principal federal analysis of why so little stolen money is recovered without fast, coordinated intervention between the actors at each stage.
- Interagency Statement on Elder Financial Exploitation (December 2024). Signed by five federal financial regulators plus FinCEN plus state regulators, this established the Trusted Contact framework and recommended best practices for financial institutions to identify, report, and intervene in suspected elder exploitation.

- Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends (CFPB Office for Older Americans, using FinCEN SAR data, February 2019). Documented 180,000+ such SARs and $6 billion+ in suspicious activity across 2013–2017, the foundational analysis that led to subsequent FinCEN advisories.

The CFPB's leverage is regulatory rather than prosecutorial: it can require, study, and recommend, but does not bring individual criminal cases and operates no public elder-fraud hotline of its own. The Trusted Contact framework, if fully adopted by financial institutions, could be among the more effective bank-side interventions against ongoing elder fraud, but adoption is currently voluntary and uneven.

Portal: consumerfinance.gov; for reporting elder financial exploitation: state Adult Protective Services via the Eldercare Locator at 1-800-677-1116.

9. FinCEN, Financial Crimes Enforcement Network

The Treasury Department's FinCEN tracks Suspicious Activity Reports (SARs) filed by banks and financial institutions. During June 15, 2022 – June 15, 2023, financial institutions filed 155,415 SARs worth $27 billion in suspected elder financial exploitation. The FinCEN figure represents what *financial institutions* flag as suspicious, not what victims report, not what law enforcement investigates, and is roughly eight times the FBI's reported elder fraud losses for the same period.

FinCEN's role extends to issuing advisories that trigger industry-wide SAR filing on specific patterns:

- FIN-2023-Alert005 (September 8, 2023), "Pig Butchering" cryptocurrency investment scam alert. Established the SAR key term "FIN-2023-PIGBUTCHERING". Documented the Southeast Asian compound origin of the scheme.
- FIN-2024-Alert005 (December 18, 2024), Alert on fraud schemes abusing FinCEN's name, insignia, and authorities (FinCEN-impersonation, beneficial-ownership-information (BOI), and money-services-business (MSB) scams).
- Financial Trend Analysis: Elder Financial Exploitation (April 2024), analysis of 155,415 related Suspicious Activity Reports (SARs) filed June 2022–2023.

The FinCEN advisories directly enable the bank-side intervention that the CFPB's Interagency Statement recommends. Together, they constitute a strong federal infrastructure for catching elder fraud at the financial-institution layer.

Portal: fincen.gov/news/news-releases.

Congressional oversight

10. U.S. Senate Special Committee on Aging

The U.S. Senate Special Committee on Aging is the congressional committee that oversees this field, and it also operates its own consumer-protection apparatus. The Committee maintains the Senate

Fraud Hotline at 1-855-303-9470, open weekdays 9 a.m. to 5 p.m. Eastern Time. Since 2013, nearly 12,400 complaints have been registered with the hotline (Senate Aging, *Age of Fraud*, 2025).

The Committee publishes the Fraud Book, which catalogs the top 10 scams reported to its hotline plus prevention guidance. The 2025 edition, *Age of Fraud: Scams Facing Our Nation's Seniors*, was published jointly by Chairman Rick Scott (R-FL) and Ranking Member Kirsten Gillibrand (D-NY). The Committee has also supported bipartisan recognition of National Slam the Scam Day (first week of March).

Hotline / portal: aging.senate.gov/fraud-hotline; 1-855-303-9470.

Beyond the ten: a wider federal web

The ten profiled above are the most prominent federal actors with dedicated elder-fraud programs. The federal patchwork extends further. At least seven additional agencies engage at the periphery, none operating senior-specific intake of its own, but each contributing a piece of the response, and each adding another channel a confused victim or family member might find:

- **FDIC** runs a *"Scams Targeting Older Adults"* consumer-resource center (1-877-ASK-FDIC).
- **OCC**, the national-bank regulator, publishes elder-financial-exploitation guidance and co-signed the December 2024 *Interagency Statement* alongside the CFPB and FinCEN.
- **SEC** operates the Office of Investor Education and Advocacy ((800) SEC-0330) and partners with state regulators on senior-targeted investment-fraud enforcement.
- **CFTC** pursues commodities and precious-metals fraud against retirees, often in joint actions with state securities regulators.
- **FCC** sits at the telecom layer where the first scam contact often happens; robocalls are its single largest consumer-complaint category, and it has penalized carriers that transmitted AI-voice robocalls.
- **IRS / IRS Criminal Investigation** addresses tax-impersonation directly (a perennial *"Dirty Dozen"* entry) and joins the transnational scam takedowns led by the FBI and DOJ.
- **CMS** runs a Medicare-specific fraud-reporting channel (1-800-MEDICARE) that operates in parallel to HHS OIG's 1-800-HHS-TIPS.

Adding these to the federal map deepens the report's diagnosis: the fragmentation is wider than ten actors would suggest, the overlaps denser, and the question of *which* federal door a worried senior or family member should walk through correspondingly harder to answer.

And yet: for one group, a single front door already works

In August 2024 the federal government launched VSAFE (vsafe.gov; 1-833-38V-SAFE / 1-833-388-7233), a single fraud-reporting number and website for veterans, service members, and their families. Its design is explicitly "no wrong door": one call is routed to the correct federal agency, drawing on resources from nine departments and agencies including the FTC, CFPB, SSA, and IRS. VSAFE

suggests the fragmentation described in this chapter is not inevitable: a single, unified front door already works for veterans. Chapter 9 returns to whether that design could extend more broadly.

Many layers, all real, and still the gap

Reading the rings back inward: At the center are the older adult and the family who meet the scam first. Around them, the caregivers, Adult Protective Services workers, and the ACL-funded aging-services network. Around them, the state attorneys general and Puerto Rico's Secretary of Justice. Around them, the banks, platforms, and nonprofits at national scale. And then, the ten lead federal actors and the wider federal web beyond them. Every one of these layers is real. Every one does work that saves money and protects people.

And it is still not enough. The reason is not any one layer: not because any layer is failing, and not because the country needs more layers. All of them are good. The problem is that they bring complexity when a confused victim needs clarity, and a quick response.

Data Sources for Chapter 6:

- FBI IC3, *2025 Internet Crime Report*, 2026, overall 2025 elder fraud figures, FFKC, Operation Level Up, Transnational Strike Force, AI Related data
- U.S. Department of Justice, *EAPPA Annual Report to Congress*, October 2025, 283 actions, 608 defendants, $2.36B figure
- Federal Trade Commission, *Protecting Older Consumers 2024-2025*, December 1, 2025, $10.1B–$81.5B true-cost estimate, Pass It On data
- Federal Trade Commission, *Consumer Sentinel Network Data Book 2024*, March 2025
- Consumer Financial Protection Bureau, *Recovering from Elder Financial Exploitation: A Framework for Policy and Research*, September 2022 (four-stage recovery framework)
- Consumer Financial Protection Bureau, *Interagency Statement on Elder Financial Exploitation*, December 2024, Trusted Contact framework
- FinCEN Alert FIN-2023-Alert005, *Pig Butchering*, September 8, 2023; FIN-2024-Alert005, *Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities*, December 18, 2024
- FinCEN, *Financial Trend Analysis: Elder Financial Exploitation*, April 2024, $27B SAR figure
- SSA Office of Inspector General, *Quarterly Scam Reports*, Issues 2–18 (July 2021 – September 2025), SSA imposter trend data
- U.S. Secret Service, *Elder Fraud Advisory*, April 2026
- U.S. Postal Inspection Service, *Annual Report FY 2024*, January 2026
- HHS Office of Inspector General, *Special Fraud Alert on Hospice* (March 1998); and OIG hospice oversight documenting enrollment-without-consent schemes (oig.hhs.gov/reports/featured/hospice)
- U.S. Senate Special Committee on Aging, *Age of Fraud: Scams Facing Our Nation's Seniors*, 2025 Edition (Senate Report 119-35, July 2025): Fraud Book; top-10 scams and Senate Fraud Hotline figures
- U.S. Department of Justice (justice.gov, Aug 28 2025) and *San Diego Union-Tribune* (Aug 29 2025): San Diego $65M / 28-defendant transnational fraud-ring takedown
- Administration for Community Living, Older Americans Act Aging Network (Area Agencies on Aging; state units on aging); Eldercare Locator (1-800-677-1116); state Adult Protective Services: structural basis for the inner-ring and community sections ("The people closest..." and "The aging-services network"); no new quantitative claims
- Pennsylvania Office of Attorney General (attorneygeneral.gov, "Year One" report, Jan 2026; Times Leader, Jan 30 2026): Elder Exploitation Section under AG Dave Sunday and the caregiver/conservator-perpetrator finding; Pennsylvania's fifth-largest 65+ population per U.S. Census ACS 2019-2023 (B09020)
- Arizona Office of the Attorney General (Kris Mayes), consumer advisory on veteran-targeted scams (~500,000 AZ veterans; ten schemes), May 22 2026
- Connecticut (CT.gov / portal.ct.gov), Elder Justice Hotline 1-860-808-5555

- Additional federal agencies engaged in elder fraud beyond the ten profiled (FDIC, OCC, SEC, CFTC, FCC, IRS / IRS-CI, CMS, VA / VSAFE, ACL)

Bank- and platform-sector references (for the "The private sector at national scale" section):

- Bank of America security center; Senior Financial Exploitation: Addressing a Hidden Threat; Erica AI fraud-detection coverage in *American Banker* and *Future Digital Finance*
- JPMorganChase press release, *Largest Financial Fraud and Scam Prevention Effort in Firm's History*, November 17, 2025
- JPMorganChase, *Philanthropic Initiative to Support Fraud and Scam Prevention*, May 15, 2025
- Wells Fargo, *Protecting older adults from fraud & scams* (wellsfargo.com); San Diego Seniors Community Foundation grant announcement
- Charles Schwab, *A task force committed to senior and vulnerable investors*; SchwabSafe documentation; Trusted Contact Person framework
- Keynova Group, *Q4 2025 Online Banker Scorecard* (Nov 19, 2025) + *Q1 2026 Mobile Banker Scorecard* (Mar 18, 2026): caregiver / limited account access (KeyBank, Huntington, Wells Fargo; U.S. Bank added early 2026)
- Meta Transparency Center, *Q3 2025 Integrity Reports*; *Fighting Scammers and Protecting People* (March 2026)
- Google, *2025 Ads Safety Report*; *Our fight against fraud, 5 ways we're keeping you safer*
- Microsoft On the Issues (blogs.microsoft.com), *Microsoft helps disrupt India-based tech support scam group targeting Japanese seniors*, June 5, 2025, by Steven Masada (Microsoft DCU + India CBI + Japan NPA + JC3 coordinated takedown
- Microsoft On the Issues (blogs.microsoft.com), *Disrupting the gateway services to cybercrime*, December 13, 2023, by Amy Hogan-Burney (Storm-1152 disruption announcement
- OpenAI, *Disrupting malicious uses of AI: June 2025*, 46-page threat report by Nimmo / Zhang / Farquhar / Murphy / Bumanglag: includes the Operation "Wrong Number" case study (pp. 41–45)
- OpenAI, *Usage Policies* (most recent update October 29, 2025): explicit prohibitions on fraud, scams, impersonation, voice cloning
- Anthropic, *Acceptable Use Policy* (effective September 15, 2025); *Responsible Scaling Policy* v3.2 (effective April 29, 2026)
- Decrypt, *ChatGPT exposes pig-butchering scam*, December 2025 (referenced in Chapter 4)
- United Nations Office on Drugs and Crime, *Industry Accord Against Online Scams and Fraud*, Vienna Global Fraud Summit, March 2026
- Tech Transparency Project, *Meta Awash in Deepfake Scam Ads*, 2025; Center for Countering Digital Hate, scam-ads-targeting-seniors report
- *Wall Street Journal*, May 2025, on Meta automated-strike policy

CHAPTER 07

Chapter 7: The Legislative Landscape

> *"Last year alone, Americans lost over $16 billion to scams. That's a staggering amount of money that's been stolen from our families, our neighbors, and, disproportionately, our seniors". Sen. Kirsten Gillibrand (D-NY), December 2025, referring to total scam losses across all ages*

The Gap Between Words and Law

Elder fraud generates genuine bipartisan agreement. Protecting grandparents from criminals is, as a policy position, uncontroversial. Press conferences are held. Bills are introduced. Statements are issued.

This chapter maps that landscape, the bills in play, the laws on the books, and the remaining gap between legislative ambition and criminal reality.

Federal Legislation: What's Moving

The bills, hearings, and rule-makings catalogued in this chapter are happening with limited public visibility, itself a symptom of the fragmentation this report documents: a response so scattered across agencies, committees, and statehouses that even sustained activity never coheres into a story the public can follow and act on. The federal legislative landscape on elder fraud is active but fragmented, with multiple bills addressing different aspects of the same crisis. This chapter surveys representative measures, not a census: the field has grown too large for any one chapter to list in full, and the examples that follow are chosen to show the shape of the activity, and the seam that runs through it. The statuses below are snapshots as of early June 2026; bill status changes quickly, so verify current status against Congress.gov before relying on it.

Read together, these bills share a telling feature. Each is bipartisan, each is welcome, and each strengthens a different front: the supply chain abroad, a national strategy, state and local tools, platform advertising, transaction timing, and a first criminal line against AI impersonation. What none of them is designed to do is name who runs the day-to-day response, or how fast it must move. Keep that shared gap in view as the bills go by; it is the opening Chapter 9 is built to fill.

The SCAM Act (Scam Compound Accountability and Mobilization; S. 2950)

Status: Passed by the Senate, December 2025. Awaiting House consideration.

The Scam Compound Accountability and Mobilization (SCAM) Act, introduced by Sen. John Cornyn (R-TX) and Sen. Jeanne Shaheen (D-NH), addresses the international infrastructure behind elder fraud.

The bill targets the scam compounds, fortified facilities where trafficked workers are forced to conduct cyber fraud operations targeting Americans. Specifically, the SCAM Act would:

- Require the Secretary of State, in consultation with the Attorney General and Treasury Secretary, to submit a strategy to counter scam compounds
- Establish a six-year task force to implement the strategy and submit annual progress reports to Congress
- Authorize the President to impose IEEPA sanctions against foreign nationals who support or enable international scam compound operations
- Direct the DOJ to recommend mechanisms for financial redress to American scam victims
- Enhance capabilities of partner governments and law enforcement agencies to dismantle scam compounds

Co-sponsors include Sens. Rick Scott (R-FL), Tammy Duckworth (D-IL), Margaret Wood Hassan (D-NH), Tim Kaine (D-VA), James Lankford (R-OK), Pete Ricketts (R-NE), and Jacky Rosen (D-NV).

Sen. Rick Scott, chairman of the Senate Special Committee on Aging, said the act would particularly protect older adults. The legislation, he said, "is a critical step toward protecting our seniors and every American impacted by ensuring our law enforcement agencies have the resources they need to stop this abuse".

The National Strategy for Combating Scams Act (S. 3355)

Status: Introduced and referred to the Senate Judiciary Committee, December 4, 2025; in committee. House companion (H.R. 6425) introduced by Rep. Amo (D-RI).

Introduced by Sen. Kirsten Gillibrand (D-NY) with co-sponsors including Sens. Mark Kelly (D-AZ), Rick Scott (R-FL), and Ashley Moody (R-FL), this bill would:

- Require the FBI to develop a coordinated national strategy to combat scams
- **Standardize scam reporting** across federal agencies
- Incorporate input from victims, law enforcement, and the private sector

"Every year, scammers steal billions of dollars from Americans, harming families, especially seniors. But the federal government lacks a strategy to address the scope and speed of these schemes", said Sen. Mark Kelly. "This bipartisan bill will create a coordinated approach to crack down on fraud, better protect families and seniors, and hold scammers accountable".

The GUARD Act (S. 2544)

Status: Advanced out of Senate Judiciary Committee, February 5, 2026 (unanimous). Awaiting full Senate vote. House companion: H.R. 2978 (Reps. Nunn (R-IA), Gottheimer (D-NJ)).

The Guarding Unprotected Aging Retirees from Deception (GUARD) Act (S. 2544), led by Sen. Katie Britt (R-AL) and Sen. Kirsten Gillibrand (D-NY), with Sen. Rick Scott (R-FL) among the original cosponsors, and introduced July 30, 2025, takes a different approach: rather than creating new federal enforcement mechanisms, it empowers state and local law enforcement to fight elder fraud more effectively. (This is the elder-fraud GUARD Act; it is distinct from S. 3062, a separately introduced "GUARD Act" addressing AI chatbots and minors.)

The GUARD Act would:

- Expand how state and local law enforcement can use existing federal grant funds to investigate financial fraud
- Authorize greater federal assistance to state and local investigators using blockchain tracing tools
- Focus specifically on technology-enabled scams and "pig butchering" operations targeting older Americans

"This will help provide law enforcement the tools that they need to better help prevent the millions of dollars that we're seeing lost from fraud and cyber crimes in Alabama", said Alabama Securities Commission Director Amanda Senn.

The Safeguarding Consumers from Advertising Misconduct (SCAM) Act

Status: Introduced in House as H.R. 7548 (Rep. Dan Meuser, R-PA, with Rep. Lou Correa, D-CA), February 2026. Senate companion S. 3774 by Sens. Ruben Gallego (D-AZ) and Bernie Moreno (R-OH).

The FTC has identified social media as the leading contact method for elder fraud by total reported losses, with $561 million reported lost by adults 60 and over to social-media-initiated scams in 2024 alone. The SCAM Act would:

- **Ban paid scam ads** by holding platforms accountable when they profit from fraudulent or deceptive advertising
- Require real advertiser verification, including ID checks and impersonation safeguards
- Mandate fast action timelines for platforms to investigate reports and remove fraudulent ads
- Empower the FTC, states, and harmed consumers to enforce compliance

The bill has received endorsements from the American Bankers Association, the Consumer Federation of America, the Consumer Bankers Association, the Bank Policy Institute, and the National Consumers League.

"Social media companies making money from ads have a responsibility to make sure they're not fraudulent and put consumers first", said Rep. Correa.

Transaction Delay Legislation

Status: Introduced as S. 2840 on September 17, 2025 by Sen. Bill Hagerty (R-TN), with Sen. Ruben Gallego (D-AZ) as lead cosponsor; referred to the Senate Banking Committee. A related House bill, H.R. 2478 (Rep. Ann Wagner, R-MO, and colleagues), was introduced earlier, in March 2025, referred to House Financial Services, and reported in November 2025.

This bill would amend the Investment Company Act of 1940, the federal law governing mutual funds, to let a fund delay paying out when an investor cashes out shares (a redemption) if it reasonably suspects the financial exploitation of an older or vulnerable adult. The optional "cooling off" hold is designed to interrupt the urgency that scammers rely on. The CFP Board and financial industry groups have expressed support.

The AI Fraud Accountability Act (S. 3982)

Status: Introduced March 4, 2026 by Sen. Tim Sheehy (R-MT) and Sen. Lisa Blunt Rochester (D-DE). A bipartisan House companion, H.R. 7786, was introduced the same day by Reps. Vern Buchanan (R-FL) and Darren Soto (D-FL).

Congress has been alert to this threat since at least November 2023, when the Senate Special Committee on Aging, under Chairman Bob Casey (D-PA) and Ranking Member Mike Braun (R-IN), held a bipartisan hearing on scammers' use of AI voice clones and deepfakes, *Modern Scams: How Scammers Are Using Artificial Intelligence and How We Can Fight Back*, releasing that year's Fraud Book alongside it. Introduced over two years later, this is the first federal bill that would make AI-driven digital impersonation a standalone federal crime. It is not Congress's only response to the AI escalation documented in Chapter 4, the voice clones and deepfakes that now power the grandparent and impersonation scams hitting older Americans hardest: the Artificial Intelligence Scam Prevention Act (S. 3495), introduced December 16, 2025 by Sen. Amy Klobuchar (D-MN) and Sen. Shelley Moore Capito (R-WV), would prohibit replicating a person's voice or image, including with AI, with intent to defraud, enforcing that ban civilly through the FTC and routing consumer education through the senior-fraud advisory office Congress created in 2022. The AI Fraud Accountability Act would go further on the same conduct. The bill would:

- Make it a federal crime to use an AI-generated "digital impersonation" of a real person in interstate communications with intent to defraud
- Treat that same conduct as an unfair or deceptive act under the FTC Act, enforceable by the Federal Trade Commission
- Direct the FTC to identify the foreign countries most associated with digital-impersonation fraud and to pursue international cooperation
- Convene a NIST-led working group, with the DOJ, the FTC, industry, and technical experts, to develop best practices, while expressly preserving parody, satire, and journalism

Federal Legislation Tracker

The six bills above, summarized in one reference table:

Bill	Sponsors	Status (as of early June 2026)	Key Provisions
S. 2950, Scam Compound Accountability and Mobilization (SCAM) Act	Cornyn (R-TX), Shaheen (D-NH)	Passed Senate (Dec 2025), awaiting House	Counter scam compounds, IEEPA sanctions authority, 6-year task force, DOJ victim redress
S. 3355, National Strategy for Combating Scams Act	Gillibrand (D-NY), Kelly (D-AZ), Scott (R-FL), Moody (R-FL)	Introduced (Dec 2025); House companion introduced by Amo (D-RI)	Require FBI national scam strategy, standardize cross-agency scam reporting
S. 2544, GUARD Act	Britt (R-AL), Gillibrand (D-NY), Scott (R-FL); House companion H.R. 2978 (Nunn R-IA, Gottheimer D-NJ)	Advanced unanimously from Judiciary Committee (Feb 5, 2026)	Expand state/local use of federal grants for financial-fraud investigation; blockchain tracing tools
Safeguarding Consumers from Advertising Misconduct (SCAM) Act	House: Meuser (R-PA), Correa (D-CA); Senate: Gallego (D-AZ), Moreno (R-OH)	Introduced (Feb 2026)	Ban scam ads on platforms, require advertiser ID verification, mandate fast take-down timelines, FTC enforcement
S. 2840 / H.R. 2478 (investment-company redemption delay)	Hagerty (R-TN), Gallego (D-AZ); House: Wagner (R-MO) et al.	H.R. 2478 introduced Mar 2025 (reported Nov 2025); S. 2840 Sep 17, 2025	Amends Investment Company Act of 1940 to *permit* (not require) postponing fund-share redemptions when financial exploitation of a vulnerable adult is suspected
S. 3982, AI Fraud Accountability Act of 2026	Sheehy (R-MT), Blunt Rochester (D-DE); House companion H.R. 7786 (Buchanan R-FL, Soto D-FL)	Introduced and referred to Senate Commerce (Mar 4, 2026)	Make AI-generated "digital impersonation" used to defraud a federal crime; FTC civil enforcement; foreign-country identification; NIST best-practices working group

Source: Bill text and congressional press releases cited per bill above; corpus tracking through early June 2026.

Also advancing. The six bills above are not the whole field. The Romance Scam Prevention Act (H.R. 2481, Rep. David Valadao (R-CA) with Reps. Pettersen (D-CO), Goldman (R-TX), and Suozzi (D-NY); S. 841, Sens. Marsha Blackburn (R-TN) and John Hickenlooper (D-CO)) passed the House by voice vote on June 23, 2025 and is on the Senate calendar; it would require dating platforms to warn, within 24 hours, any user who had received a message from an account banned for fraud. The Senior Security Act (H.R. 1469, Reps. Josh Gottheimer (D-NJ) and Ann Wagner (R-MO); Senate companion S. 4055,

Sens. Andy Kim (D-NJ), Susan Collins (R-ME), Kirsten Gillibrand (D-NY), and David McCormick (R-PA)) passed the House by voice vote on July 21, 2025 and would create a ten-year Senior Investor Taskforce at the SEC. The TRAPS Act (S. 2019, Sen. Mike Crapo (R-ID) with Sens. Warner (D-VA), Moran (R-KS), and Warnock (D-GA); H.R. 4936, Reps. Zach Nunn (R-IA) and Jim Himes (D-CT)) would convene a Treasury-led task force on payment scams spanning the CFPB, FCC, FTC, DOJ, and the banking regulators. And the Crypto ATM Fraud Prevention Act (S. 710, Sen. Dick Durbin (D-IL)), pending before the Senate Banking Committee since February 2025, would set federal kiosk fraud warnings, new-customer limits of $2,000 a day and $10,000 in total, refund rights for defrauded new customers, and Treasury registration: a federal floor under the state kiosk laws described below. Each strengthens a real front. And as with the six bills above, none of them names who runs the day-to-day response, or how fast it must move.

What's Already on the Books

The legislative push of 2025–2026 builds on several existing federal laws:

Law	Year	Key Provisions
Elder Abuse Prevention and Prosecution Act	2017	Required each U.S. Attorney's Office to designate an Elder Justice Coordinator; mandated DOJ/FTC elder-fraud data collection and annual reporting to Congress
Senior Safe Act (Title III, § 303 of Pub. L. 115-174)	2018	Gave trained financial-institution employees and their institutions immunity for good-faith, reasonable-care reporting of suspected senior financial exploitation to regulators, law enforcement, and adult protective services (12 U.S.C. § 3423); participation is voluntary, with no reporting mandate and no transaction-hold authority
Fraud and Scam Reduction Act	2022	Established the FTC's Office for the Prevention of Fraud Targeting Seniors and the Senior Scams Prevention Advisory Group; directed model senior-fraud education materials
Telemarketing Sales Rule Amendment	2024	Expanded FTC authority over telemarketing fraud, including tech support scams
FCC Declaratory Ruling FCC 24-17	2024	Confirmed that AI-generated and cloned voices count as "artificial" voices under the Telephone Consumer Protection Act, placing AI voice-clone robocalls squarely under existing consent and enforcement rules
FTC Impersonation Rule	2024	Made it illegal to impersonate government agencies and businesses; strengthened FTC enforcement tools

These laws provide a real foundation. The Senior Safe Act, for example, is the legal cover that lets trained bank staff report what they see without fear of liability for the employee or the institution, the predicate for the banking-sector response described later in this chapter, though it asks no one to answer that report within any particular window. And like the bills now moving, each strengthened a piece of the response without assigning anyone to run those pieces as a single system.

State Legislation

While Congress debates broad federal solutions, individual states have begun passing their own protections, creating a patchwork of laws that varies in scope and effectiveness.

Cryptocurrency ATM Regulation

The urgency of cryptocurrency regulation is underscored by the FBI's data. In 2025, total cryptocurrency fraud reached $11.4 billion across all ages from 181,565 complaints, the largest single loss aggregation IC3 tracks. (IC3 counts cryptocurrency as a cross-cutting descriptor, a payment and transaction tag spanning multiple crime types, rather than a standalone crime type; the highest-loss crime type by its own taxonomy was investment fraud at $8.65 billion across all ages.) Elder victims alone accounted for $4.35 billion in crypto losses. Complaints about cryptocurrency kiosks (ATMs) nearly doubled from 2023 to 2024, and losses continued to surge in 2025 (up 58% year-over-year), as scammers increasingly direct victims to convert cash to cryptocurrency at physical terminals. The elder impact is disproportionate: IC3 recorded 6,188 elder crypto kiosk complaints in 2025 totaling $257.5 million, accounting for 66% of all kiosk losses across all ages. Older adults are, by a wide margin, the most financially devastated demographic at the crypto ATM.

States have moved well beyond a few first steps. Lawmakers in nearly thirty states have introduced or passed crypto-kiosk rules in recent years, and the National Conference of State Legislatures counted at least forty states with cryptocurrency or digital-asset legislation introduced or pending in the 2025 session alone. In 2026, the first outright bans arrived. No two states have written quite the same rule; the tracker below shows the range, illustrative rather than exhaustive:

State	Measure	Status (as of early June 2026)	Daily cap (new customers)	Key feature
California	SB 401, Digital Financial Assets Law (2023)	In force (cap since Jan 1, 2024)	$1,000	Tightest cap surveyed; court-upheld; DFPI-enforced
Arizona	HB 2387 (2025)	In force since Sep 26, 2025	$2,000	Full refunds, including fees, for defrauded new customers
Illinois	SB 2319, Digital Asset Kiosks Act (2025)	In force since Aug 18, 2025	$2,500	Fee cap (greater of $5 or 18%); compliance and consumer-protection officers
Minnesota	Minn. Stat. § 53B.75 (2024), then SF 3868	Ban signed May 5, 2026; effective Aug 1, 2026	$2,000 (2024 law)	Regulate-then-ban; kiosks removed by Dec 31, 2026
Indiana	HEA 1116 (2026)	Ban in force since Mar 9, 2026	None (ban)	First statewide kiosk ban
Tennessee	HB 2505, Public Chapter 766 (2026)	Ban effective Jul 1, 2026	None (ban)	Second statewide ban; operation a Class A misdemeanor
Nebraska	LB609 (2025) + Grand Island Ordinance 10051	In force (statewide Sep 2025; municipal Nov 2025)	Warnings-based	Statewide kiosk fraud-warning law; first municipal signage ordinance
New Hampshire	SB 482	Enrolled; awaiting the Governor's signature	$2,000	48-hour hold on first transactions; 14-day refund window
Alaska	SB 249 (Sen. Cathy Tilton, R-Wasilla)	Passed both chambers; not yet law	$1,000	"Don't Mess with Grandma" bill; 10% fee cap; 90-day refunds

Sources: enacted texts and legislative records cited in the Data Sources block for this chapter; statuses as of early June 2026.

A few of these stories carry the chapter's larger point:

- **California** wrote the earliest and most court-tested rule. Sponsored by Sen. Monique Limón (D), enacted with companion AB 39 (Asm. Tim Grayson, D), and signed by Gov. Gavin Newsom (D) in October 2023, its $1,000 daily cap (Cal. Fin. Code § 3902) was upheld by a Los Angeles County court in August 2024; in October 2025, the state's Department of Financial Protection and Innovation announced a $675,000 consent order, including $105,000 in consumer restitution, against an operator whose over-limit kiosk customers were often over 60. California leads the nation in reported elder fraud losses (see Chapter 2).
- **Arizona** shows the bipartisan arc in one state: sponsored by Rep. David Marshall (R-Snowflake), signed by Gov. Katie Hobbs (D) on May 12, 2025, and in force since September 26, 2025. Announcing the protections, Attorney General Kris Mayes cited FBI estimates that Arizonans lost more than $177 million to cryptocurrency fraud in 2024, across roughly 600 kiosks statewide;

Arizona ranks fifth in the nation in reported elder fraud losses in the four tracked scam categories (see Chapter 2).

- **Minnesota** regulated first and then went further. Led by Sen. Amanda Hemmingsen-Jaeger (DFL) and Rep. Erin Koegel (DFL), the 2026 ban passed the Senate 57-10 and the House 127-7 before Gov. Tim Walz (D) signed it on May 5, 2026, following Indiana (signed by Gov. Mike Braun (R) on March 9, 2026) and Tennessee (approved by Gov. Bill Lee (R) in April 2026). The regulate-then-ban arc is instructive: where one rule fell short, states reached for a stronger rule of their own.
- **New Hampshire**, where reported elder fraud losses in the four tracked scam categories grew 2,247% over five years (the fastest five-year growth rate in the nation, off a small 2021 base; see Chapter 2), produced the strongest still-pending bill: sponsored by Sen. Tim McGough (R-Merrimack), SB 482 cleared the House 214-140 on April 23, 2026.
- **Grand Island, Nebraska** took the response to municipal scale: Ordinance No. 10051, approved by the City Council on November 4, 2025, requires fraud-warning signs on every kiosk within city limits, with $500-per-day fines, and the Grand Island Police Department, in partnership with AARP Nebraska, began on-site enforcement and business-education visits in December 2025.

Cryptocurrency ATMs are a growing concern because they enable instant, irreversible, and effectively untraceable transfers. Scammers direct victims to "deposit cash at a Bitcoin ATM" as a modern equivalent of the gift card payment, with even less chance of recovery.

Writing AI Into State Fraud Law

States are also writing the AI escalation documented in Chapter 4 directly into their fraud statutes, a state counterpart to the federal AI bills above:

- **Texas (SB 2373):** Carried by Sen. Nathan Johnson (D-Dallas) and Rep. Giovanni Capriglione (R-Southlake) and passed without a dissenting vote in either chamber (Senate 31-0, House 138-0), the law was signed by Gov. Greg Abbott (R) on June 20, 2025 and took effect September 1, 2025. It is built for the modern scam fact pattern: knowingly using artificially generated media or phishing communications for financial exploitation is now both a civil cause of action and a graduated criminal offense (Penal Code § 32.56), rising to a first-degree felony when $150,000 or more is taken, with a $1,000-per-day civil penalty the Attorney General can seek and a confidential-identity procedure that shields victims in court. Texas reports the third-highest elder fraud losses in the nation in the four tracked scam categories (see Chapter 2).
- **Pennsylvania (SB 649, Act 35 of 2025):** Introduced by Sen. Tracy Pennycuick (R) with bipartisan co-sponsors including Sen. John Kane (D), it passed the Senate 50-0 and the House 199-3, and Gov. Josh Shapiro (D) signed it on July 7, 2025, effective that September. The act creates the offense of "digital forgery" (18 Pa.C.S. § 4101.1): making or using a forged digital likeness, an AI deepfake or cloned voice among them, is a first-degree misdemeanor, and a third-degree felony when done in a scheme to defraud, coerce, or steal. Pennsylvania ranks eighth in the nation in reported elder fraud losses in the four tracked scam categories (see Chapter 2).

State-Level Consumer Protections

- **Colorado (ASSET Act, HB26-1110):** Introduced February 2026 with a bipartisan sponsor team (Reps. Sean Camacho (D) and Jamie Jackson (D); Sens. Marc Catlin (R) and Jessie Danielson (D)) and passed both chambers (House March 9, Senate April 20, 2026). It targets financial exploitation of vulnerable adults at the teller window, authorizing banks and credit unions to delay suspicious transactions, alert a trusted contact, and report suspected exploitation with good-faith immunity. Gov. Jared Polis (D) signed it into law on May 26, 2026; it takes effect in August 2026.

Attorney General Initiatives

Beyond legislation, state attorneys general have increasingly used their existing authority to pursue elder fraud cases and launch awareness campaigns. Multiple state AG offices partnered with federal agencies, financial institutions, and local law enforcement to create elder fraud task forces, interagency bodies that coordinate investigation, prosecution, and victim services. Recent state-AG specialized units include Pennsylvania's Elder Exploitation Section (announced in late 2025), Arizona's Task Force Against Senior Abuse (TASA), and California's Division of Medi-Cal Fraud & Elder Abuse.

The state record is genuine and accelerating, and it is, by design, fifty different answers where a senior needs one. A national coordination layer would not replace these laws or preempt the states; it would give them a common channel to plug into, so a case that begins in one state does not stall at its border.

The Banking Sector Response

An emerging and potentially transformative development is the growing role of financial institutions in elder fraud prevention. In March 2026, KFF Health News reported on banks "becoming bulwarks against scams for vulnerable seniors", a shift driven by regulatory pressure.

Key developments include:

- **Transaction monitoring:** Major banks are deploying AI-powered systems to flag unusual transactions by senior account holders, large wire transfers, cryptocurrency purchases, or repeated gift card transactions
- **Teller training:** Banks are training front-line employees to recognize the signs that a customer may be acting under the influence of a scammer, scripts, nervousness, requests that the teller not ask questions
- **Voluntary transaction holds:** Some institutions have voluntarily implemented holds on suspicious transactions involving senior customers, allowing time for intervention
- **AI-powered behavioral monitoring:** Vendor-developed AI engines that score senior accounts against multi-indicator risk profiles (cognitive-decline patterns, repeated gift-card purchases, escalating transfers) have begun being deployed across community-bank software platforms

The banking sector's entry into elder fraud prevention is significant because banks are the last institutional touchpoint before stolen money leaves the system. If a bank can delay or block a fraudulent transfer, the scam can fail regardless of how sophisticated the social engineering that preceded it. But a teller's hold buys hours, not days, and without a coordinated 24-hour channel to escalate into, that window can close before anyone with recovery authority is even notified.

What the Landscape Leaves Unaddressed

The bills surveyed above represent a real surge in legislative attention to elder fraud, and each addresses a genuine dimension of a multi-dimensional problem. International compound operations, social-media advertising liability, blockchain tracing, transaction timing, federal/state strategy, a criminal line against AI impersonation, and behind them dating-platform warnings, investor protection, payment-scam coordination, and kiosk rules: these are necessary fronts, each advancing a real piece of the solution.

Read together, these bills leave one layer unaddressed: the operational connective tissue between them, the bridge between the public's need for simplicity and the government's need for efficiency. Each strengthens a real front; none names who runs the day-to-day response for the public, or how fast it must move. A single way in, a common protective message, and a shared 24-hour standard could let the work already underway function as one system, on authority the federal actors in Chapter 6 already hold. Chapter 9 takes up that gap.

Chapter 8 examines what these losses mean in human terms beyond the dollar figure, and Chapter 9 presents the Three Ones proposal.

Data Sources for Chapter 7:

- seniors.hcsk.org news corpus: 64 legislation/policy articles, August 2025–May 2026
- S. 2950, SCAM Act, Senate passage, December 2025 (McKnight's Senior Living report)
- S. 3355, National Strategy for Combating Scams Act: Sen. Kelly press release, "Kelly, Gillibrand, Scott, Moody Introduce Bipartisan Bill to Protect Seniors from Scammers", December 2025 (kelly.senate.gov, archived)
- GUARD Act, Yellowhammer News, February 2026
- Safeguarding Consumers from Advertising Misconduct (SCAM) Act, Correa.House.Gov press release, February 2026; ABA endorsement letter, February 2026
- Pennsylvania Attorney General, Elder Exploitation Section announcement, late 2025
- Arizona HB 2387, "cryptocurrency kiosk; license; fraud prevention" (Chapter 171, 2025; A.R.S. § 6-1236), approved by the Governor May 12, 2025, effective September 26, 2025 (azleg.gov, enacted chapter text)
- Arizona Attorney General (Kris Mayes), press release, "Attorney General Mayes Announces New Protections Against Bitcoin ATM Scams Going into Effect in Arizona", September 26, 2025
- California SB 401 and AB 39 (Chapters 871 and 792, Statutes of 2023), Cal. Fin. Code § 3902 (leginfo.legislature.ca.gov, chaptered text); California DFPI press releases on the kiosk-cap litigation (September 2024) and the October 30, 2025 consent order
- Illinois SB 2319, Digital Asset Kiosks Act, Public Act 104-0429, signed August 18, 2025 (ilga.gov, enacted text; IDFPR release)
- Minnesota Stat. § 53B.75 (2024) and 2026 Session Laws, Chapter 65 (SF 3868), signed May 5, 2026 (revisor.mn.gov, statute and chaptered text)
- Indiana House Enrolled Act 1116 (2026), IC 28-8-7, signed March 9, 2026 (iga.in.gov); Tennessee Public Chapter 766 (2026), HB 2505, approved April 2026, effective July 1, 2026 (Tennessee Secretary of State, enrolled act)
- Texas SB 2373 (Acts 2025, 89th Leg., Ch. 1154; Civ. Prac. & Rem. Code ch. 100B; Penal Code § 32.56), signed June 20, 2025, effective September 1, 2025 (capitol.texas.gov, enrolled text and bill analysis)
- Pennsylvania SB 649, Act 35 of 2025 (18 Pa.C.S. § 4101.1, digital forgery), signed July 7, 2025 (palegis.us, enacted text)
- Colorado HB26-1110, ASSET Act, signed May 26, 2026 (leg.colorado.gov status history and enrolled act)
- New Hampshire General Court, SB 482-FN docket (House passage 214-140, April 23, 2026; enrolled June 4, 2026; awaiting the Governor's signature as of early June 2026)
- State legislation counts: National Conference of State Legislatures, "Cryptocurrency, Digital or Virtual Currency and Digital Assets 2025 Legislation" (ncsl.org: "at least 40 states have introduced or pending legislation"); Duane Morris Government Strategies, state crypto-kiosk tracker, April 28, 2026 (statecapitallobbyist.com: "lawmakers in nearly 30 states have introduced or passed crypto kiosk regulations")
- Union Leader, "NH seniors targeted by crypto ATM scams", March 2026

- KFF Health News, "Banks Are Becoming Bulwarks Against Scams for Vulnerable Seniors", March 10, 2026
- Carefull, GreyMatter AI behavioral-monitoring engine launch, Business Wire release, October 27, 2025 (anchors the community-bank AI-monitoring development noted above)
- FTC, *Protecting Older Consumers 2024-2025* (P144400, December 2025), Figure 6, "2024 Top Contact Methods Ranked by Losses (Ages 60 and Over)" (social media ranked first; $561 million)
- Alaska SB 249 (HCS CSSB 249(L&C)), Sen. Cathy Tilton (R-Wasilla): Senate 20-0 (May 12, 2026), House 40-0 (May 19, 2026), Senate concurrence 20-0 (May 20, 2026); awaiting transmittal to the Governor as of early June 2026 (akleg.gov bill action history)
- govinfo.gov bill texts and status records, for S. 2950, S. 3355, H.R. 7548 / S. 3774, S. 2840 / H.R. 2478 (H. Rept. 119-361, November 4, 2025), and S. 3982 / H.R. 7786
- AARP Nebraska, "Protecting Consumers from Cryptocurrency Kiosk Scams"
- Nebraska Legislature, LB609, the Controllable Electronic Record Fraud Prevention Act, approved by the Governor March 11, 2025 (nebraskalegislature.gov, enacted slip law)
- Elder Abuse Prevention and Prosecution Act of 2017, Pub. L. 115-70, enacted October 18, 2017 (govinfo.gov, enacted text)
- Fraud and Scam Reduction Act, Division Q, Title I of Pub. L. 117-103 (2022), comprising the Stop Senior Scams Act and the Seniors Fraud Prevention Act of 2022 (govinfo.gov, enacted text)
- FBI IC3, *2025 Internet Crime Report*, 2026 (cryptocurrency complaint data, kiosk complaints)
- FTC Impersonation Rule, 16 CFR Part 461 (89 FR 15017, effective April 1, 2024); FTC Telemarketing Sales Rule amendment covering inbound technical-support calls, 16 CFR Part 310 (89 FR 99069, effective January 9, 2025) (federalregister.gov)
- S. 3982, AI Fraud Accountability Act of 2026: Congress.gov bill page (introduced and referred to the Senate Committee on Commerce, Science, and Transportation, March 4, 2026); sponsor press releases (Sen. Blunt Rochester, Rep. Buchanan), March 2026
- U.S. Senate Special Committee on Aging, hearing, *Modern Scams: How Scammers Are Using Artificial Intelligence and How We Can Fight Back*, November 16, 2023 (S. Hrg. 118-179; Chairman Casey, Ranking Member Braun; the annual Fraud Book was released at the hearing); official transcript via govinfo.gov
- S. 3495, Artificial Intelligence Scam Prevention Act, introduced December 16, 2025 (Klobuchar, Capito); govinfo.gov bill text and status record
- Romance Scam Prevention Act: H.R. 2481 (House-passed by voice vote, June 23, 2025) and S. 841 (S. Rept. 119-58; Senate Calendar No. 145, September 2, 2025); govinfo.gov bill texts and status records
- Senior Security Act: H.R. 1469 (House-passed by voice vote, July 21, 2025) and S. 4055 (introduced March 11, 2026); govinfo.gov bill texts and status records
- TRAPS Act, S. 2019 (introduced June 10, 2025) and H.R. 4936 (introduced August 8, 2025); govinfo.gov bill texts and status records
- S. 710, Crypto ATM Fraud Prevention Act of 2025, introduced February 25, 2025 (Durbin); govinfo.gov bill text and status record

- Senior Safe Act, Title III, § 303 of Pub. L. 115-174 (2018), codified at 12 U.S.C. § 3423 (govinfo.gov, enacted text)
- FCC, Declaratory Ruling FCC 24-17, CG Docket No. 23-362, adopted February 2, 2024 (docs.fcc.gov)

CHAPTER 08

Chapter 8: Beyond the Dollar

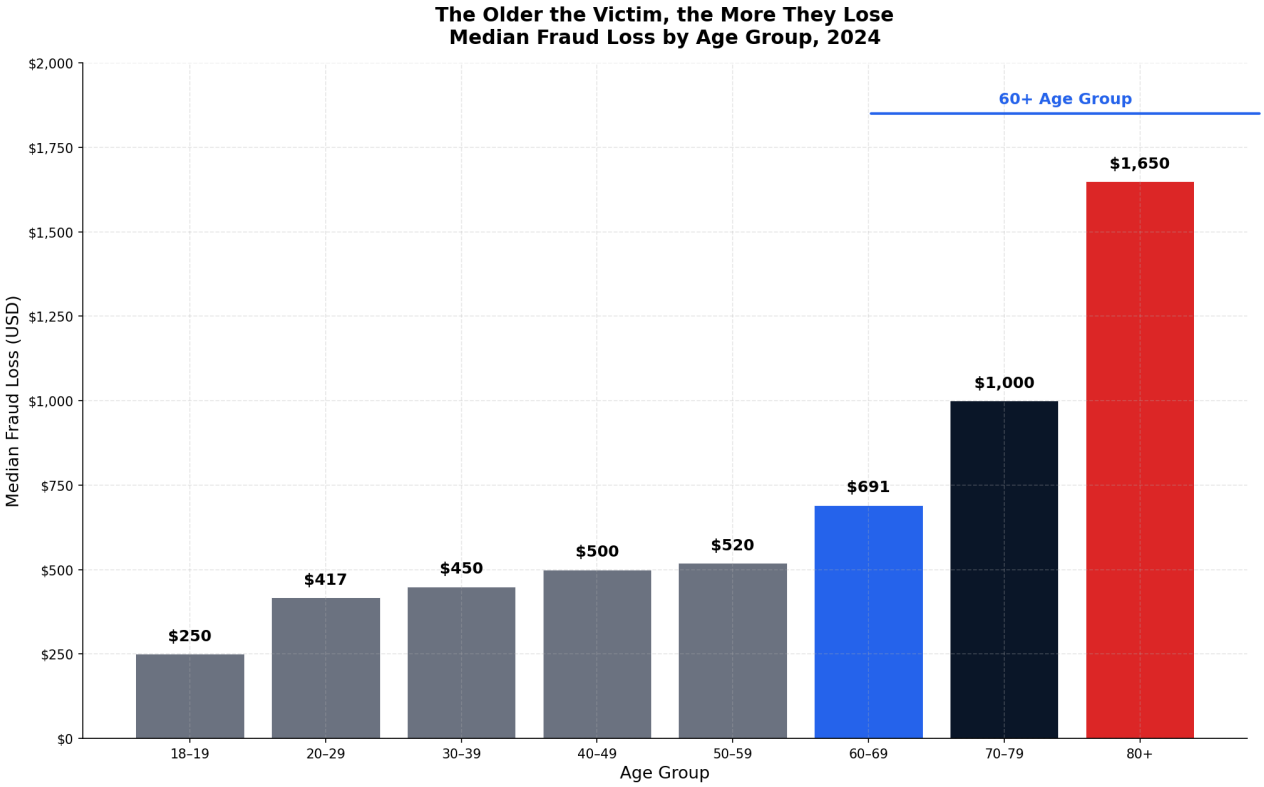
> *"Losing the money is devastating. Losing the love and the life I thought I was gonna have, that was more than I could handle, and I cried for days".*
>
> **SOURCE:** *Pennsylvania romance scam victim, testifying before the state House Democratic Policy Committee, February 2026*

What the Numbers Don't Count

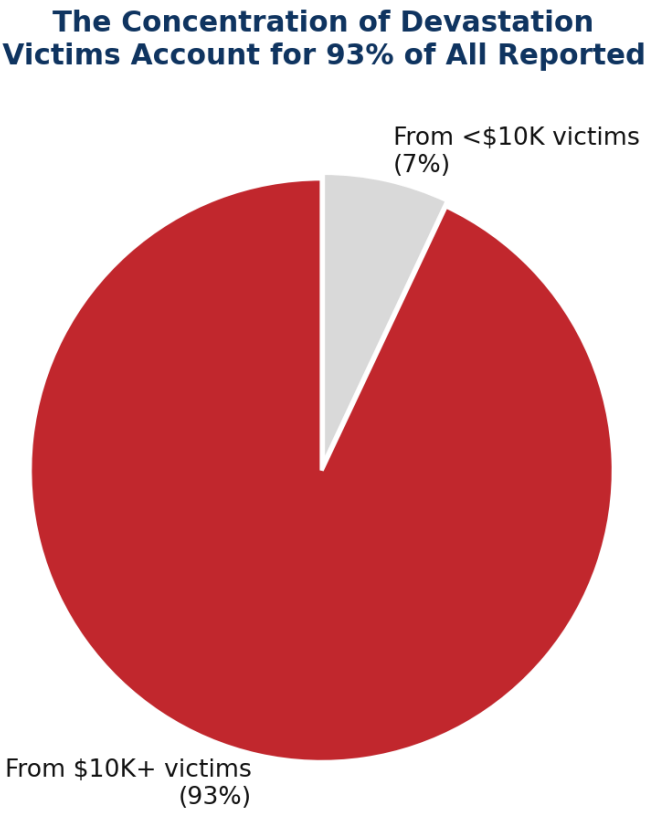
This report has, by necessity, measured elder fraud in dollars and percentages.

The numbers are essential for understanding the scale of the crisis. They reveal little about what it does to a human being. Elder fraud destroys more than money. It destroys trust, in institutions, in technology, in other people, in oneself. It destroys independence. It destroys relationships. It destroys the inheritance they meant to leave their children.

This chapter attempts to document what no data table can capture: the human cost of elder fraud, told through the voices of those who have experienced it.



Median fraud loss by age group, 2024. Source: FTC Consumer Sentinel Network / Protecting Older Consumers 2024–2025; medians by age group.



Source: FTC Consumer Sentinel Network, 2024. All ages.

The concentration of loss: 13 percent of victims (those losing $10,000 or more) account for 93 percent of all reported losses. Source: FTC Consumer Sentinel Network, 2024; all ages.

The Anatomy of a Victim's Experience

Stage 1: The Hook

Every fraud begins with a moment of trust. The victim is not at fault and was not careless; they are responding to a situation that has been carefully engineered to appear legitimate.

A **widow in Pennsylvania**, isolated during COVID-19, accepted a Facebook friend request from a man calling himself Tony. "He had studied my profile on Facebook and he knew a great deal about me", she told state legislators in February 2026 testimony. "Every single night he called and would ask, 'How was your day, honey?' No one had asked me that since my husband had passed away".

A **retired nurse in Maryland** received a call appearing to come from her local police chief. She checked the name online, it matched. She was transferred to someone claiming to be an FBI agent. "I grew up in a culture that had respect for government officials and law enforcement", she explained in subsequent advocacy.

A **hairstylist** who was saving to open her own business received a spoofed call that appeared to come from her bank, with the caller ID matching the number on the back of her card. She was told a hacker was trying to steal $20,000 of her savings. "I'm just trying to hurry up and make sure they can't get that money", she said. By the time she realized the call itself was the fraud, her $20,000 was gone.

A **Pennsylvania man** called the Senate Aging Committee's fraud hotline to report that he had cashed out his entire 401(k) and deposited all funds into what he believed was a high-yield savings account. The investment company's website has since vanished. He was left with no money and no retirement.

In every case, the victim responded rationally to the information available to them. The irony of elder fraud is that the victims who lose the most money are often the most conscientious, people who verify caller identities, who research claims, who try to do the right thing. Scammers exploit due diligence as readily as they exploit trust.

Stage 2: The Escalation

Once trust is established, the financial extraction follows a predictable pattern of escalation. Small requests become large demands. Each compliance makes the next request harder to refuse.

The Pennsylvania widow's scammer started with $50 gift cards. By the end, she had given away her financial security. The Maryland retired nurse withdrew nearly $600,000 over months, dropping cash at a designated courthouse locker, believing she was helping the FBI take down a fraud ring.

In Collin County, Texas, the Sheriff's cyber unit documented more than 200 victims over age 65 who collectively lost their retirement funds to gold bar scams, a variant in which seniors are convinced to convert their savings to physical gold and hand it to couriers. As of early 2026, Collin County alone has reported more than $7 million in confirmed losses, part of a statewide gold-bar scheme exceeding $55 million, and law enforcement has documented similar gold-bar courier schemes in coordinated multi-state operations targeting jewelry-store laundering networks in Texas, Georgia, and Florida. One Illinois courier was intercepted by law enforcement in March 2024 carrying 16 gold bars worth over $1 million, collected from victims over two days.

The escalation stage is where even strong prevention programs have the hardest time breaking through. By the time a victim has made their second or third payment, they are psychologically committed. It is the scam's design, not any lack of effort, that makes intervention so difficult here. Admitting fraud at this point means admitting that earlier payments were also lost, a cognitive cost that many victims cannot bear until the scammer disappears.

Stage 3: The Discovery

The moment of discovery, when the victim realizes they have been scammed, is, by many accounts, more devastating than the financial loss itself.

A **Montgomery County resident** who lost $10,000 to a government impersonation scam described the aftermath as feeling that her sense of self had been wiped away in an instant.

An **Ohio woman** called the Senate Aging Committee's fraud hotline to report a romance scam that had lasted two years and cost her $40,000. Two years of daily contact, of trust, of what she believed was love, followed by the realization that none of it was real.

The Pennsylvania widow described the moment more starkly: "Once I realized I was being scammed, my heart shattered".

Discovery typically comes through one of three channels:

- The scammer asks for an amount the victim cannot produce, forcing them to seek help and exposing the fraud
- A family member, bank teller, or friend notices the financial behavior and intervenes
- Law enforcement or a government agency contacts the victim

In too many cases, discovery comes too late, after the victim's savings are gone and the scammer has disappeared.

Stage 4: The Aftermath

The aftermath of elder fraud extends far beyond the immediate financial loss.

Financial devastation. For seniors on fixed incomes, the loss of retirement savings is often permanent. There is no second career to rebuild the nest egg. Social Security provides a floor, but for victims who lost five or six figures, the gap between that floor and their former standard of living is a daily reminder of what happened. Recovery is far less likely once the money has moved, which is why reporting within hours matters most: in 2025 the FBI's Recovery Asset Team froze about half the money at risk in the elder-fraud cases reported fast enough to act, but reached only a few hundred of the 201,266 elder-fraud complaints filed. The four-stage recovery process the Consumer Financial Protection Bureau identifies (identification → reporting → investigation → return) has no automatic handoff between stages, and most cases fall out of the pipeline before the return of funds.

Shame and silence. A mass-market-fraud study cited by the FTC found that only 4.8 percent of fraud victims said they reported the incident to a government entity or the Better Business Bureau, though the frauds it covered generally involved low losses; the FTC's own data show reporting rises with the amount lost (about 2.0 percent for losses under $1,000 versus 6.7 percent for losses over $1,000). Among those who do report, the path is often humiliating. When the Pennsylvania widow called for help, she was told: "Why are you calling here? There's no crime here. You willingly gave him that money".

"You have no idea how much courage it takes to make those phone calls", she later told state legislators.

Family rupture. Scams strain family relationships in both directions. Adult children sometimes respond to a parent's victimization with anger rather than support, "How could you be so foolish?", compounding the victim's shame. In other cases, family members discover that a parent has borrowed

from them under false pretenses (the scammer told the victim to keep the situation secret), creating a breach of trust that mirrors the original fraud.

Loss of independence. For seniors who prize self-sufficiency, the combination of financial loss and family intervention can feel like the end of independence. Adult children may take control of finances, move a parent to supervised living, or restrict technology access, well-intentioned responses that can feel like punishment for having been victimized.

Physical and mental health consequences. The stress of fraud victimization has documented health effects. Depression, anxiety, insomnia, and social withdrawal are commonly reported. Federal data documents the most severe end of this spectrum: in 2025, the FBI's Operation Level Up made 38 suicide-intervention referrals for victims of cryptocurrency investment fraud, a single program, in a single year, at a single federal agency. The true number of fraud-linked suicidal crises is unknown and almost certainly higher.

> *If you or someone you love is in crisis, the 988 Suicide & Crisis Lifeline is available 24 hours a day, free and confidential, by call or text. Call or text 988 from any phone in the United States.*

Voices

"A Higher Good"

The Maryland retired nurse spent months withdrawing her life savings, nearly $600,000, and dropping it at a courthouse locker, believing she was helping the FBI take down a fentanyl ring. She was a nurse. She was, by every measure, a functioning, intelligent, capable adult.

"I thought I was going to do a higher good by helping the FBI take down a fentanyl ring that was money laundering, supposedly with my Social Security number", she said.

An Elderly Widow

In the San Diego prosecution of a $65 million fraud ring, prosecutors described one victim as an elderly San Diego woman who was "repeatedly defrauded until she'd lost her life savings".

The Collin County Retirees

In Collin County, Texas, the Sheriff's cyber unit has documented a pattern that repeats itself across the country: retirees who followed every instruction, who cooperated with what they believed were government agents, and who converted their retirement accounts to gold bars that were collected by couriers at their front doors.

The Psychological Machinery of Exploitation

Understanding why intelligent, experienced adults fall victim to fraud requires understanding the psychological techniques that scammers employ. These are not random. They are systematic, tested, and refined through millions of interactions.

There is also a structural reason the usual defenses are down. The cognitive defenses many older adults built over a working lifetime, the simulated-phishing tests, the security training, the learned instinct to distrust an out-of-the-blue request, were scaffolded by an employer's apparatus: an IT department, monitoring tools, role separation, someone to call. Retirement quietly removes that scaffolding. At home there is no IT team, no phishing-test program, no 24/7 monitoring, and scammers know it. The techniques described below land on a person who, through no fault of their own, has lost the institutional backstop that once caught these attempts at work.

Authority Compliance

The Milgram experiments demonstrated in the 1960s that ordinary people will comply with harmful instructions from perceived authority figures. Elder fraud exploits this tendency directly. Government impersonation scams, which grew +638 percent over five years (second only to investment), work precisely because victims believe they are speaking to the FBI, the IRS, or their local police.

For Americans who came of age in an era of greater institutional trust, the instinct to comply with authority is deeply ingrained. This is not a weakness. It is a social virtue that scammers have learned to weaponize.

Veterans face a particularly cruel application of this lever. Scammers impersonate the VA to insist a benefits "overpayment" must be repaid, or pose as paid "claims" helpers, turning a lifetime of earned trust in the institution that serves them into the very mechanism of the theft.

Isolation and Secrecy

Many scams in our corpus includes an instruction to keep the interaction secret: "Don't tell your family", "This is a confidential government investigation", "If you tell anyone, the criminals will know".

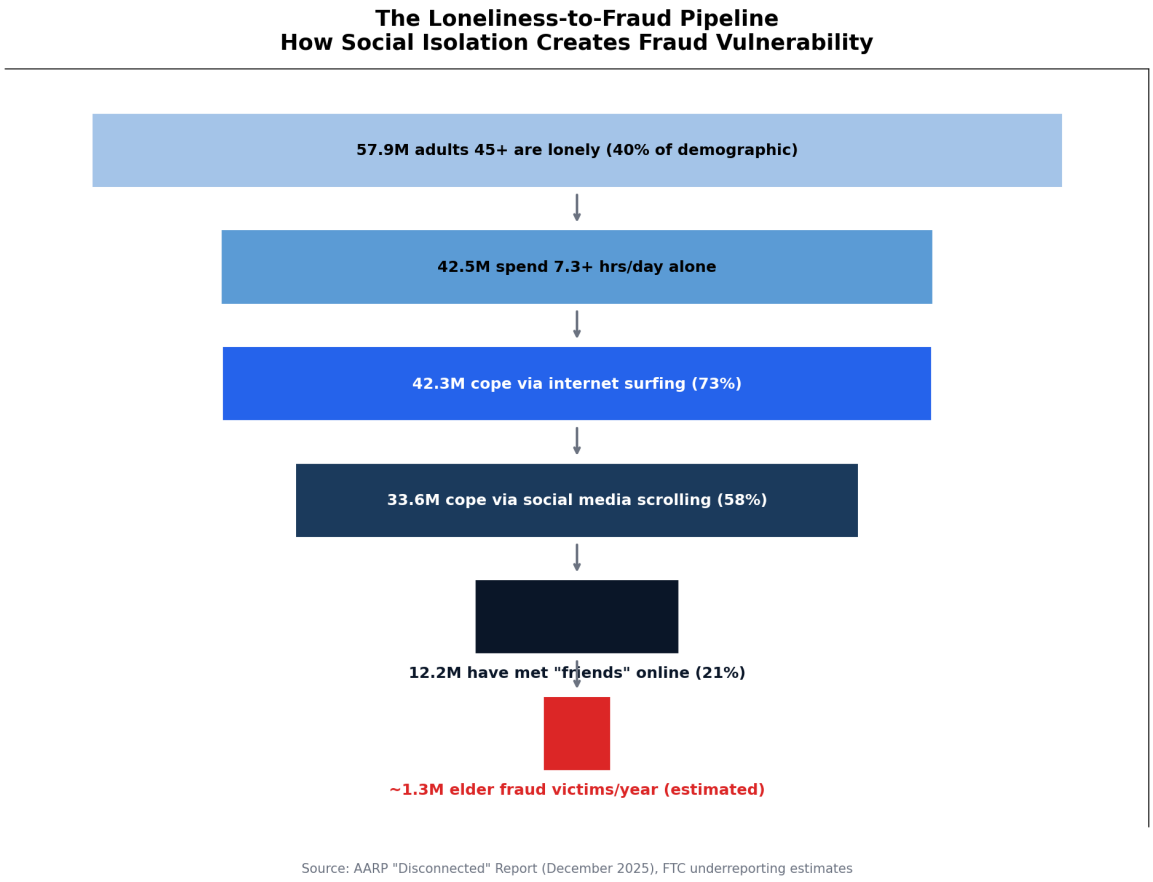
This instruction serves a critical function: it removes the victim from their social safety net. A victim who tells their daughter about a suspicious phone call will probably be talked out of sending money. A victim who has been sworn to secrecy has no one to consult.

The scale of this vulnerability is documented in two converging bodies of evidence. The U.S. Surgeon General's 2023 Advisory *Our Epidemic of Loneliness and Isolation* established loneliness as a public-health crisis. Federal Census data (Current Population Survey, 2023) confirms that approximately 28 percent of Americans age 65 and over live alone (about 16 million people), the highest rate among any age group.

AARP's December 2025 research report *Disconnected: The Escalating Challenge of Loneliness Among Adults 45-Plus* measured 40 percent of U.S. adults aged 45 and over as lonely, approximately 57.9

million Americans in the broad midlife-and-older population whose isolation heightens fraud vulnerability. Lonely adults in that survey spent an average of 7.3 hours per day alone. Fifteen percent of adults 45 and over reported no close friends at all, rising to 25 percent among those who are lonely.

When they cope with loneliness, they overwhelmingly turn to the channels where scammers are waiting: 73 percent favor internet surfing and 58 percent turn to social media scrolling. In 2024, social media was the single largest source of elder fraud losses reported to the FTC ($561 million for adults 60 and over).



The loneliness-to-fraud pathway: how social isolation among adults 45 and over can heighten fraud exposure. Source: AARP Disconnected (December 2025) and FTC underreporting estimates.

Romance scammers explicitly target isolated individuals. The Pennsylvania widow's story begins with a COVID-era Facebook friend request. The Maryland nurse's begins with someone living alone. The scammer's first question is always some version of: *Are you alone? Is anyone with you?*

The Sunk Cost Trap

Once a victim has made initial payments, the psychological pressure to continue becomes enormous. Admitting fraud means admitting that previous payments are lost. Continuing the relationship preserves the possibility, however slim, that the investment will pay off, the lover will arrive, the government investigation will conclude.

This is why many victims escalate their losses over weeks or months, even as warning signs accumulate. The scammer knows this. The escalation pattern, small request, medium request, large request, is designed to build a ladder of sunk costs that the victim cannot psychologically step off.

Shame as a Silencing Mechanism

The shame that victims feel after discovery serves the criminal enterprise even after the scam is complete. Victims who feel ashamed do not report. Victims who do not report are invisible in the data. Invisible victims cannot inform prevention efforts, cannot warn their communities, and cannot hold anyone accountable.

The president of the Pennsylvania Alliance for Retired Americans, testifying alongside the Pennsylvania widow at the February 2026 hearing, put it simply: "Education alone cannot solve a problem that is operating at industrial scales".

Chapter 9 presents the Three Ones.

Data Sources for Chapter 8:

- FBI IC3, *2025 Internet Crime Report* / *Elder Fraud Report 2025* (headline 60+ figures: $7.748B, 201,266 complaints, +59%; Operation Level Up suicide-intervention referrals; +638% government-impersonation growth is a state-aggregated 2021–2025 HCSK derivation, not a figure printed in the FBI report)
- U.S. Senate Special Committee on Aging, *Age of Fraud*, 2025 (Chicago hair-stylist case, Pennsylvania 401K victim, Ohio romance victim)
- Consumer Financial Protection Bureau, *Recovering from Elder Financial Exploitation: A Framework for Policy and Research*, September 2022 (four-stage recovery framework)
- Yuksel Aydin (HCSK founder), "Boomers are getting scammed for billions online", *The Hill*, June 14, 2025
- U.S. Surgeon General, *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, 2023, federal framing of loneliness as a public-health crisis
- AARP Research, *Disconnected: The Escalating Challenge of Loneliness Among Adults 45-Plus*, December 2025 (w/ Ipsos Public Affairs)
- U.S. Census Bureau, American Community Survey, living-alone statistics for Americans 65+
- Federal Trade Commission, *Protecting Older Consumers 2024-2025*, December 2025, fraud reporting rate research; median fraud loss by age group (2024)
- Keystone Newsroom, "Targeted and alone: Why Pennsylvania seniors are losing millions", February 27, 2026
- The Baltimore Banner, "Once scammed, these Montgomery County women now work to prevent other seniors", April 9, 2026
- San Diego Union-Tribune, $65 million fraud ring prosecution, August 29, 2025
- Tampa Free Press, "Fake Feds and Real Gold: Illinois courier admits role in Missouri $6M elder fraud ring", November 29, 2025
- CBS News Texas, "More elderly victims identified in North Texas gold-smelting fraud ring", January 31, 2026, and Collin County Sheriff cyber-unit profile, February 28, 2026 (200+ victims over 65; $7M+ in Collin County; $55M+ statewide per Times of India / Yahoo, January 30 / February 23, 2026)

CHAPTER 09

Chapter 9: The Proposal: The Three Ones

> *America has the people, the agencies, the laws, and the data. What it lacks is a single front door, a single message, and a single clock. The missing piece is coordination and simplification.*

The first eight chapters of this study documented the landscape, the problem. This chapter proposes a way forward.

The proposal is a simple framework, three coordinated changes that take the federal and state infrastructure America already has and could help it function as a single system instead of complex ones.

We call it the Three Ones:

- **One Front Door**, a single way in by phone or web: a single national elder-fraud hotline (the **One Number**) and a single federal online entry point (the **One URL**)
- **One Message**, a single behaviorally-grounded protective frame: *Think First, Verify Always*
- **One Day**, a 24-hour coordinated response standard from first report to multi-agency activation

What the Three Ones does not do

- *It does not create a new federal agency.*
- *It does not replace the FBI, FTC, DOJ, CFPB, FinCEN, SSA OIG, HHS OIG, USPIS, USSS, state attorneys general, Adult Protective Services, or banks.*
- *It does not require victims to repeat their story to different offices. One report activates the coordinated response.*
- *It does not dictate which phone line or which website becomes the One Number or the One URL. That designation belongs to officials; the obvious candidates already exist.*

What it would create is a single front door, a common protective message, and a 24-hour coordination standard.

9.1 The Three Findings

Before proposing unification, we have to name the fragmentation. The American response to elder fraud is fragmented across three dimensions, each documented in earlier chapters and each addressed by one of the Three Ones.

No single front door: scattered by phone and on the web (1. One Front Door)

Many actors maintain elder-fraud programs. Each has its own reporting or intake channel, its own data system, its own awareness materials, and its own institutional priorities. Plus state attorneys general across the 50 states, DC and Puerto Rico's Secretary of Justice, Adult Protective Services agencies in every state, a distributed network of state Senior Medicare Patrols (SMP), State Health Insurance Assistance Programs (SHIP), and hundreds of private banks, credit unions, payment processors, and platforms making case-by-case decisions about whether to intervene when a senior customer appears to be in the middle of a scam.

A senior or caregiver searching online for "report a scam" or "report elder fraud" does not land in a single, recognizable destination.

And the maze does its damage at the worst possible moment. Someone who has just been scammed is already confused, frightened, and often ashamed; a fragmented front door adds noise exactly when clarity matters most. Asking for help at all takes courage, and a hard-to-find front door is a barrier to it, one whose cost is not the victim's alone. Every report that is deterred or delayed is also a chance not taken to stop that scammer from reaching the next person. An easy, obvious way in is not a convenience; it is often the difference between a report that happens and one that never does.

Phone and web are two faces of the same gap, and both call for the same fix: designation of a single, recognizable, existing front door as the default first stop: one number to call and one website to visit.

Inconsistent protective messaging, the wrong threat model (2. One Message)

This fragmentation is the one consumers actually see, and it is among the most damaging. The protective messaging that federal agencies, banks, and nonprofits direct at older Americans is largely borrowed from cybersecurity and therefore mismatched to the threat:

- *Use strong passwords.* The right call against credential theft, but no help against a romance scam, in which the victim willingly sends money.
- *Don't click suspicious links.* The right call against phishing, but no help against a phone-based grandparent scam.
- *Update your antivirus.* The right call against malware, but no help against any social-engineering scam, which is most of them.
- *Use two-factor authentication.* The right call against account takeover, but no help against extortion, romance scams, or government-impersonation scams.

Each of these is correct guidance for some threat. Together they constitute a protective frame that does not match the dominant threat. Elder fraud in 2025 is overwhelmingly manipulation-based, not technical-exploit-based. A romance-scam victim with a 32-character password and hardware 2FA still loses her life savings if the scammer earns her trust over six months and then asks for the money. The password hygiene is irrelevant to the threat model.

What protective frames *do* fit the threat? Several existing campaign taglines come closer:

- The *Stop. Think. Connect.* campaign
- AARP's *Pause. Reflect. Protect.*
- San Diego DA's *Stop. Hang Up. Tell Someone.*
- Secret Service's *Guard Personal Information, Monitor Communication, Slow Down, Verify, Use Caution*
- FINRA Foundation's *Ask and Check*

Speed mismatch, money moves faster than the federal response (3. One Day)

Money moves faster than the federal response can follow it. A fraudulent wire can sometimes be frozen, but only if it is reported almost immediately, and cryptocurrency, once converted and moved across multiple blockchains, is almost unrecoverable within hours. Most elder-fraud reports never reach a federal channel that quickly. By the time a senior who was scammed on a Friday evening reaches a federal intake on Monday morning, the operational recovery window may have closed.

9.2 One Front Door: One Number to Call, One Website to Visit

The proposal

Designate a single national front door for elder-fraud reporting, reachable two ways, by phone and on the web, and route every report from it to the agency whose mandate fits. A senior or caregiver in distress should have one number to call and one website to visit.

A single front door means one report does the work that ten separate intakes do today:

- The senior or caregiver reports once, by phone or on the web.
- The intake triages the case and issues auto-referrals to the appropriate agencies
- With consent, a family member is notified.
- A single case number follows the case across agencies.

This is a coordination protocol. The hotline should answer 24 hours a day, 7 days a week; the website should display the number prominently, surface the One Message at the head of its guidance, and trigger the One Day response workflow on submission. The two channels reinforce each other: call it or click it, the same coordinated response follows.

A working precedent. The federal government has already built one for veterans. In August 2024 it launched VSAFE (vsafe.gov; 1-833-38V-SAFE / 1-833-388-7233), a single number and website for

reporting fraud, scams, and predatory practices, with an explicit "no wrong door" design: one contact is routed to the correct federal agency, combining resources from the CFPB, FTC, SSA, IRS, FCC, OMB, and the Departments of Defense, Education, and State. The intake channel and the interagency routing already exist. VSAFE shows a single front door is feasible; the Three Ones would extend one front door for everyone, the same coordinated way in for every older American.

9.3 One Message, "Think First, Verify Always"

Agencies are converging on the same two behaviors that defeat manipulation: engage your own judgment before acting, then confirm through a channel you choose rather than the one that contacted you. The U.S. Secret Service's public guidance, for instance, lists *Slow Down* and *Verify* among its protective steps. What has been missing is a single, tested way to carry them: agencies state them differently, at different lengths, and usually inside longer checklists, so no one version takes hold. *Think First, Verify Always* is what this study adds: a deliberate two-part structure that pairs a trigger to engage judgment with a standing instruction to verify, short enough to repeat, and tested in a controlled trial (below).

The proposal

Adopt "Think First, Verify Always" as the unified consumer-protection message frame for elder fraud.

The two core actions.

1. **Think First.** Engage independent human reasoning before relying on AI assistance, automated systems, or any party who initiated the contact. Slow down long enough to ask: *Am I being rushed? Am I being told to act in secret? Am I being asked to move money or share a code?* If the answer to any is yes, the pressure is the warning.
2. **Verify Always.** Cross-check critical information through independent sources before taking action. The channel that contacted you is potentially compromised; only an independent channel you choose is trustworthy. Call the agency from a number on a paper bill. Log in to your bank by typing the URL yourself. Reach a family member on a number you stored months ago.

Why this phrase, why this structure

Both clauses address documented behavioral failure modes in elder fraud:

Think First addresses the urgency-and-emotion trap. Daniel Kahneman's *Thinking, Fast and Slow* (Farrar, Straus & Giroux, 2011) documents how System 1 thinking, fast, intuitive, emotionally-driven, overrides System 2 thinking, slow, analytical, skeptical, when a person is placed under time pressure and emotional load. Every scam category in this report, from grandparent scams to phantom-hacker schemes to fake-FBI calls, exploits this. The instruction *think first* gives the listener a short, two-word behavioral prompt to shift modes before responding. It is a prompt that interrupts the automatic response.

Verify Always addresses the channel-trust trap. Scammers gain credibility through the channel they contact the victim on: a real-looking caller ID, a believable email address, a video call with a deepfake. The protective rule must be that the channel that contacted you is potentially compromised; only an independent channel you choose is trustworthy. *Verify always*, call the agency on a number from a known document, log in to your bank by typing the URL yourself, ask your grandchild on a number you stored months ago, gives the listener a universal procedure that works regardless of which scam category they are facing.

How it works against the documented scam landscape

Scam type	"Think First" application	"Verify Always" application
Grandparent scam	*Slow down. A familiar voice is no longer proof, and panic is the script.*	Hang up; call your grandchild back on the number you've had for months
Romance scam	*Someone who loves me doesn't need my money to prove it.*	Before sending anything, show the messages to one person you trust
Tech support scam	*Real tech companies don't call you about a virus.*	Look up the company's number yourself, from your receipt or its official site, and call that
Government impersonation	*Real agencies send letters; they don't threaten arrest by phone.*	Call back on a number from the agency's official .gov website or your latest letter, never the one that called you
Investment scam	*Guaranteed returns don't exist.*	Check the seller and the offer at Investor.gov, the SEC's free database, or on FINRA's free BrokerCheck
Crypto-ATM payment demand	*No real business or agency takes payment at a Bitcoin ATM.*	Slow down; talk to your bank before turning cash into cryptocurrency

In a single randomized controlled trial (n = 151), a three-minute micro-lesson of the "Think First, Verify Always" protocol produced a statistically significant improvement in scenario-based task performance: trained participants scored 65.3 percent versus 57.4 percent for the control group, an absolute gain of about 7.9 percentage points (Aydin, 2025, arXiv:2508.03714; MIT Sloan Management Review, Summer 2026).

A single message is also the only kind that can be repeated. Memory is built by repetition, and a protective habit takes hold only when the same words are heard again and again, from the bank teller, the evening news, the grandchild, the Medicare flyer, until they surface on their own at the moment of pressure. Ten competing taglines cannot do that; one can. A unified frame is what allows the message to be said often enough, in enough places, to lodge in memory before it is needed.

9.4 One Day, the 24-Hour Coordinated Response Standard

The proposal

When a senior reports a suspected scam to the **One Number** or via the **One URL**, a federal–state–banking–family-protective response is coordinated within 24 hours. Each actor's role is pre-defined; the coordination would be automatic by design.

Why 24 hours

Money moves fast. The FBI's Recovery Asset Team can freeze a fraudulent wire, but only when a victim reports it to their bank and IC3 as quickly as possible; the odds of a freeze fall once the money begins moving between institutions. Cryptocurrency moves faster: once converted to a foreign exchange and moved across multiple blockchains, recovery becomes almost impossible within hours. The current federal response timeline, measured in days for federal handoffs, weeks for state agency follow-up, and months for any investigative coordination, operates on a fundamentally slower clock than the threat.

A final word

This report has documented an annual reported loss of $7.748 billion (FBI IC3 2025), a five-year growth rate of approximately +360 percent.

The Three Ones is not a complete solution. It does not address the underlying drivers, demographic aging, online migration of social and financial life, the asymmetric speed of cryptocurrency, the AI escalation. Those are longer problems with longer answers.

What the Three Ones would do is eliminate one of the variables that should not be a problem from the victim's perspective: a senior who is being defrauded at 11:30 p.m. on a Saturday should have a number to call (One Number) and a website to find (One URL). Caregivers should know the protective phrase they want their parents to remember (One Message). The federal–state–banking response should arrive within hours.

It requires the institutional choice to function as a single coordinated response.

Data sources for Chapter 9:

- Consumer Financial Protection Bureau, *Recovering from Elder Financial Exploitation: A Framework for Policy and Research*, September 2022 (four-stage recovery framework)
- Consumer Financial Protection Bureau, *Interagency Statement on Elder Financial Exploitation*, December 2024 (Trusted Contact framework)
- Federal Trade Commission, *Protecting Older Consumers 2024-2025 Report*, December 2025 (Scams Against Older Adults Advisory Group fraud-prevention messaging principles; Sentinel data on impersonation and urgency tactics)

- FinCEN Alert FIN-2023-Alert005, *Pig Butchering*, September 2023 (cross-border money-flow and bank-detection indicators)
- FinCEN Alert FIN-2024-Alert005, *Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities*, December 2024 (FinCEN-impersonation, BOI, and MSB scams)
- SSA Office of Inspector General, *Quarterly Scam Reports Issues 2–18* (July 2021 – September 2025; for SSA imposter trend documentation)
- U.S. Senate Special Committee on Aging, *Fraud Books 2021, 2023, 2025*
- U.S. Secret Service, *Public Advisory: Tips to Prevent Elder Fraud*, April 2026
- Daniel Kahneman, *Thinking, Fast and Slow* (Farrar, Straus & Giroux, 2011), behavioral basis for "Think First"
- Yuksel Aydin, *A Three-Minute Protocol to Reduce AI Manipulation Risk*, MIT Sloan Management Review Research Snapshot, Summer 2026 Edition (https://sloanreview.mit.edu/article/a-three-minute-protocol-to-reduce-ai-manipulation-risk/);*"Think First, Verify Always": Training Humans to Face AI Risks*, arXiv:2508.03714, 2025, preprint reporting the n = 151 randomized controlled trial
- FBI IC3, *2025 Internet Crime Report*, 2026 (overall 2025 figures: $7.748B, 201,266 complaints, 60+ chapter; Recovery Asset Team and Operation Level Up data)
- U.S. Department of Justice, *EAPPA Annual Report to Congress*, 2025

Appendices

Appendix A: About HCSK Inc.

Mission

This is a nonprofit initiative. HCSK Inc.'s chartered purpose, as registered in Delaware, is Human-Empowered AI Cybersecurity & Protecting Seniors From AI Scams. In service of that purpose, HCSK Inc. publishes the seniors.hcsk.org resource library, with the goal of being a reliable, freely accessible online reference on online scams targeting older adults, with particular focus on AI-enabled fraud. The organization's editorial work combines federal primary-source data with plain-language, guidance for older adults, their families, caregivers, and community partners.

Founder

HCSK Inc. was founded and is directed by Yuksel Aydin, whose background spans cybersecurity and artificial intelligence.

Published work and press mentions

HCSK Inc.'s founder has published on elder fraud in national outlets, and the seniors.hcsk.org work has been featured or referenced by others (representative selection, not exhaustive).

Bylined work by HCSK's founder:

Outlet	Article
The Hill	*Boomers are getting scammed for billions online, how to break the cycle* (opinion, June 14, 2025)
ISC2 (the cybersecurity professional association)	*Protecting Seniors from Online Scams: How Cybersecurity Professionals Can Help* (Insights, October 22, 2025)
MIT Sloan Management Review	*A Three-Minute Protocol to Reduce AI Manipulation Risk* (Research Snapshot, Summer 2026; grounded in the author's arXiv:2508.03714)

Press mentions:

Outlet	Feature
WIFR (Rockford, IL)	*Rockford-area agencies give tips to protect seniors*
WSMV (Nashville, TN)	*Senior scams are "escalating rapidly" in these 3 major Tennessee cities*
Hoodline (Memphis, TN)	*Scammers bleed Tennessee seniors dry in Nashville, Memphis, and Knoxville*

Contact

- **General:** contact@hcsk.org
- **Press inquiries:** press@hcsk.org

Appendix B: Glossary of Key Terms

An A-Z reference for the technical terms, acronyms, agencies, and programs used in this report.

Term	Definition
Account takeover (ATO)	Fraud in which criminals gain control of a victim's financial accounts and drain them, often using stolen login credentials or a SIM swap
ACL	Administration for Community Living, the HHS agency that funds aging-services programs including the Senior Medicare Patrol, SHIP, and the Eldercare Locator
APS	Adult Protective Services, the state or county agency legally designated to receive and investigate reports of abuse, neglect, and financial exploitation of older and vulnerable adults; reachable nationwide via the Eldercare Locator
Bank Secrecy Act (BSA)	The federal anti-money-laundering law under which financial institutions file Suspicious Activity Reports (SARs) with FinCEN
BEC	Business email compromise, a scam in which criminals impersonate a company, executive, or vendor by email to redirect payments or wire transfers
Blockchain analytics / tracing	Following cryptocurrency transactions across public ledgers to locate stolen funds and block transfers to wallets linked to fraud; required by several state kiosk laws
CAGR	Compound Annual Growth Rate, the average annual growth rate over a multi-year period
CFPB	Consumer Financial Protection Bureau, the federal consumer-finance regulator; co-led the December 2024 Interagency Statement on elder financial exploitation
Civil forfeiture	A legal action through which the government takes ownership of money or property tied to crime, used in large cryptocurrency-fraud seizures; forfeited funds can be returned to victims through remission
Cryptocurrency kiosk (crypto ATM, Bitcoin ATM)	A physical machine that converts cash to cryptocurrency on the spot; scammers direct victims to deposit cash at kiosks because transfers are instant and often unrecoverable

Term	Definition
Cryptocurrency wallet	A digital address or app that holds cryptocurrency; stolen funds are moved through multiple wallets to frustrate tracing and recovery
Deepfake	AI-generated video or audio that convincingly impersonates a real person
Descriptor (IC3)	In FBI IC3 data, a cross-cutting tag (such as Cryptocurrency or AI Related) that can attach to many crime types; descriptor totals span categories and are not standalone crime types
Digital arrest	Scam variant where victims are told they are under "digital arrest" via video call and forbidden from disconnecting
Digital impersonation	Using an AI-generated likeness or voice of a person to deceive; pending federal legislation would make digital impersonation used to defraud a standalone federal crime
EAPPA	Elder Abuse Prevention and Prosecution Act of 2017, the federal law that created DOJ Elder Justice Coordinators in every U.S. Attorney's Office and required annual elder-fraud reporting to Congress
Elder Justice Task Force	A multi-agency task force, such as the FBI San Diego Elder Justice Task Force, that combines federal, state, and local personnel to investigate and prosecute elder fraud
Eldercare Locator	A free national service of the Administration for Community Living (1-800-677-1116) that connects callers to local aging services, including Adult Protective Services
Engrossed / enrolled	Legislative-status terms: a bill is engrossed when it passes one chamber in final form, and enrolled when both chambers have agreed on identical text and it awaits the executive's signature
FFKC	Financial Fraud Kill Chain, FBI's process for freezing stolen funds through rapid coordination with financial institutions
FinCEN	Financial Crimes Enforcement Network, U.S. Treasury bureau that collects and analyzes Suspicious Activity Reports (SARs) from financial institutions
FINRA / FINRA Foundation	The Financial Industry Regulatory Authority, the self-regulatory body for broker-dealers (its Rule 4512 created the Trusted Contact framework), and its investor-education foundation, author of the *Ask and Check* campaign
Gold-bar courier scam	A government-impersonation variant in which victims are told to convert savings into gold bars or cash and hand them to a courier sent to their door
Grandparent scam	A scam in which the caller poses as the victim's grandchild in an urgent crisis, increasingly using an AI-cloned voice, and demands emergency money in secret
IC3	Internet Crime Complaint Center, operated by the FBI
IEEPA	International Emergency Economic Powers Act, federal law authorizing economic sanctions against foreign threats
Mandated reporter	A professional (such as certain social workers and clinicians) whom state law requires to report suspected elder abuse or financial exploitation

Term	Definition
Money mule	A person who transfers stolen money between accounts on behalf of criminals, often unknowingly
National Elder Fraud Hotline	The DOJ-funded hotline (1-833-FRAUD-11) that helps people 60 and over report fraud and routes reports to the appropriate agencies
NIST	National Institute of Standards and Technology, the federal standards agency tapped by pending AI-fraud legislation to convene best-practices working groups
OIG	Office of Inspector General, an agency's independent watchdog; the SSA OIG and HHS OIG investigate government-impersonation and health-program fraud against seniors
Operation Chakra	Joint CBI-FBI operation against transnational elder-fraud schemes targeting American victims
Operation Level Up	FBI program (with the U.S. Secret Service) launched January 2024 to proactively identify and notify victims of cryptocurrency investment fraud before their losses escalate
P2P payment	Peer-to-peer payment service (Zelle, Venmo, Cash App) that enables instant, often irrevocable person-to-person transfers
Pension poaching	A scheme targeting veterans in which advisers promise higher benefits by moving assets into high-fee products, harvesting fees rather than helping
Phantom Hacker	Multi-stage scam combining tech support fraud, bank impersonation, and government impersonation in sequence
Phishing	Fraudulent emails, texts, or messages impersonating a trusted organization to steal credentials, codes, or money
Pig butchering (*sha zhu pan*)	Investment scam technique where the victim is "fattened" through a fake relationship before being "slaughtered" through fraudulent investments
Recovery Asset Team (RAT)	The FBI team that works with banks to freeze fraudulently transferred funds before they disperse; it froze about half the reported money in the 60+ cases that reached it in time in 2025 (see FFKC)
Recovery scam	Fraud targeting previous scam victims with false promises to recover stolen funds; the victim is defrauded a second time. Documented as a growing tactic in the FBI IC3 2025 report
Remission	The DOJ process that returns forfeited criminal proceeds to identified victims
Robocall	An automated call delivering a recorded or AI-generated message at scale; AI voice-cloned robocalls fall under the Telephone Consumer Protection Act's "artificial voice" rules (FCC 24-17)
Romance-baited investment scam	A hybrid scam that begins as an online romance and steers the victim into fake investments, typically cryptocurrency (see pig butchering)
SAR	Suspicious Activity Report, filing by a financial institution reporting transactions that may involve money laundering, fraud, or other criminal activity

Term	Definition
Scam Center Strike Force	Federal coordination unit led by the U.S. Attorney's Office (District of Columbia), with the DOJ Criminal Division, FBI, and U.S. Secret Service, formed to disrupt cryptocurrency investment-fraud scam compounds operating in Southeast Asia (FBI IC3 2025 report, p.19)
Scam compound	Fortified facility where trafficked workers conduct large-scale cyber fraud operations
Sentinel Network	FTC's Consumer Sentinel Network, a database of consumer fraud reports
Sextortion	Threatening to release intimate or AI-fabricated images unless the victim pays
SHIP	State Health Insurance Assistance Program, ACL-funded counseling that helps Medicare beneficiaries, including spotting and avoiding Medicare fraud
SIM swap	Tricking a phone carrier into moving a victim's number to a criminal's device, intercepting the text codes that protect accounts
SMP	Senior Medicare Patrol, ACL-funded volunteer programs in every state that help Medicare beneficiaries prevent, detect, and report health-care fraud
Social engineering	Manipulating a person through trust, fear, or urgency into sending money or revealing information; the mechanism behind most elder fraud, no hacking required
Spoofing	Faking caller ID, an email address, or a website so a scam contact appears to come from a trusted person or institution
System 1 / System 2	Daniel Kahneman's terms for fast, intuitive thinking (System 1) versus slow, analytical thinking (System 2); scams trigger System 1 under pressure, and "Think First" prompts the shift to System 2
Transaction hold	A bank's temporary pause on a suspicious transfer, buying time to check for fraud before money leaves the account; several states authorize such holds for suspected elder exploitation
Transnational Elder Fraud Strike Force	DOJ/FBI initiative coordinating with foreign law enforcement to investigate and extradite perpetrators of cross-border elder fraud schemes
Trusted Contact	A person a bank or broker-dealer customer names in advance, whom the institution may contact if it suspects financial exploitation; the contact receives no account access or transactional authority (FINRA Rule 4512 trusted-contact provisions; CFPB-led December 2024 Interagency Statement)
USPIS	U.S. Postal Inspection Service, the law-enforcement arm of the Postal Service, which investigates mail-based fraud including check theft and courier pickups
USSS	U.S. Secret Service, whose financial-crimes mandate covers elder fraud through its Cyber Fraud Task Forces and major cryptocurrency seizures
Voice cloning	AI technology that creates a synthetic replica of a person's voice from a short audio sample

Term	Definition
VSAFE	The federal government's single fraud-reporting number and website for veterans, service members, and their families (vsafe.gov; 1-833-38V-SAFE), launched August 2024 with a "no wrong door" design that routes one report to the correct federal agency

Appendix C: Methodology

This report and its companion timeline, *Ten Months in Two Columns*, rest on the same federal primary sources, documented in each chapter's Data Sources block and in the archive at seniors.hcsk.org/data-sources/, plus one original dataset: a monitored corpus of news and official public-source coverage. This appendix documents how that corpus was built and how the companion timeline's examples were selected.

The news corpus (Chapter 5)

From August 2025 through May 2026, we maintained daily monitoring of U.S. coverage of elder fraud and senior-targeted scams, spanning news reporting and official public sources. The monitoring produced 1,910 collected items.

- **Scope.** U.S.-focused coverage of fraud and scams affecting older adults: victim cases, agency and law-enforcement warnings, enforcement actions and court outcomes, legislation, and awareness efforts.
- **Sources.** The 1,910 items came from approximately 1,000 distinct sources, drawn disproportionately from local and state newsrooms rather than national aggregators.
- **Coding.** Each item was categorized by scam type, theme, geography (state where identifiable), and response track (enforcement, courts, legislation, awareness), coded against the article text and tagged to its dominant category where it spanned several.
- **What it is, and is not.** The corpus is a record of what was *reported*, not an independent adjudication of each case, and not a census of all elder-fraud incidents. It measures media attention and its distribution (analyzed in Chapter 5); it does not supply the loss and victim figures, which rest on federal complaint data. Names have been anonymized.

The companion timeline (*Ten Months in Two Columns*)

The companion pairs, for each of ten months, reported scam activity (left) with the enforcement, court, legislative, and awareness response (right). Its entries are selected, source-attributed examples drawn from the same monitored corpus and the project's held source archive; the timeline is illustrative, not an exhaustive inventory of either column. Each month was assembled under a fixed editorial filter:

- One dominant scam of the month, in plain language, drawn from the month's heaviest coverage.

- Several threat items: a tactic or agency warning, plus senior-victim cases across different states, with a seasonal pattern where one applied.
- A response drawn from up to four tracks. Enforcement, court, and awareness items are attributed to the reporting outlet; every legislative item traces to a held primary source in the Congress and state-legislation archives and carries its point-in-time status (enacted, pending, or failed), verified as of early June 2026.
- People are anonymized throughout, defendants and victims alike, and items are presented as reported by the cited outlet.

Because both the corpus and the timeline present curated, attributed examples rather than complete inventories, individual figures within them should be read as reported by their cited sources, while this report's load-bearing loss, victim, and growth figures rest on the federal complaint data documented in each chapter's Data Sources block and verified against the federal source archive.

THE THREE ONES

One Front Door

one national phone/web entry point

One Message

a single prevention message, "Think First, Verify Always"

One Day

24-hour coordination from agencies to family supports

★ ★ ★ ★ ★

seniors.hcsk.org

Stolen Trust: America's Elder Fraud Landscape.
Special Study · seniors.hcsk.org/special-study-2026/

V.1 · JUNE 2026

Photography: Unsplash and Pexels contributors.
Charts and maps: HCSK, from federal data (FBI IC3, FTC, FinCEN, DOJ, U.S. Census Bureau), state, and news sources as cited.