KinKeeper

RESEARCH WHITE PAPER

Elder Fraud in the AI Era

How artificial intelligence changes the disguise and scale of fraud, and what families can do before money or access moves.

EVIDENCE CUTOFF

July 15, 2026

COMPANION COURSE

Elder Fraud & Scam Protection Playbook

WELLBEING PRIVACY MONEY IDENTITY

EXECUTIVE BRIEF

AI makes fraud more convincing. The basic playbook has not changed.

Families do not need to become AI experts to protect one another. They do need a plan for the moment when a call, message, or investment pitch creates urgency. Today's tools can produce a familiar voice, a plausible photo, and a polished personal story in minutes. That makes old warning signs, such as bad grammar or a voice that sounds slightly wrong, less dependable. It does not change the final step. The person behind the scam still needs someone to send money, share a code, reveal a password, or allow remote access.[1][3][6][7]

The practical takeaway

A strong response does not depend on spotting a deepfake. It adds time, a trusted contact, and a second channel before money or access moves.

WHAT AI CHANGES

The disguise gets better

Voice cloning can make an emergency call sound familiar. Generated images and video can give a false profile or investment pitch a face. Translation and writing tools can clean up awkward scripts. Public data can make the story feel personal. These changes weaken familiar clues and let one operation contact many more people with tailored messages.[1][3][6][7]

WHAT IT DOES NOT CHANGE

The decision still matters

Fraud still needs a decision that benefits the scammer. The request may be for a wire, gift card, cryptocurrency transfer, one-time code, password, or remote access. Pressure, authority, secrecy, and isolation still create the opening. A pause and an independently sourced contact method still take control of the evidence away from the person making the request.

Sources: FBI IC3 2025 [1]; FBI AI public service announcement [3]; FTC voice guidance [6]; investor alert [7].

WHAT THE EVIDENCE MEANS

The losses are serious. Age is not the explanation.

Reports from people age 60 and older show very large losses, including thousands of complaints above $100,000. That deserves a clear response, not a story that treats older adults as naturally gullible. FTC data show that older adults report losing money to fraud less often than younger adults. When a loss is reported, however, it is often larger. Exposure, available assets, irreversible payment methods, and isolation under pressure all matter. So does the fact that complaint systems capture only part of what happens.[1][2][4]

$7.748B

REPORTED LOSSES, AGE 60+

Adjusted losses reported to IC3 in 2025, up 59% from 2024.[1]

201,266

COMPLAINTS, AGE 60+

Complaints filed with IC3 in 2025, up 37% from 2024.[1]

12,444

LOSSES ABOVE $100K

Complainants age 60+ who reported losing more than $100,000.[1]

A useful family role

The goal is not to watch every move or take over. It is to be a safe second channel when an unexpected request creates pressure. Support should make it easier to pause and check, while the older adult stays part of the decision.

WHAT THIS PAPER RECOMMENDS

- Pause when an unexpected interaction asks for money, a code, a password, or access.
- Verify another way, using a number, app, or website you already trust.
- Share the request with someone you trust before acting, and without shame if something already happened.

Sources: FBI IC3 2025 [1]; FTC older-consumers report [2]; FTC high-loss imposter analysis [4].

SCOPE AND EVIDENCE

Three reporting systems show different parts of the problem

No single federal dataset counts all fraud. This paper keeps the systems separate and uses each for the question it can answer.

01

IC3

Cyber-enabled crime complaints

Counts complaints and adjusted reported losses submitted to the FBI. Its 60+ section is the newest detailed national view for 2025.[1]

02

FTC Sentinel

Consumer fraud reports

Compares reporting patterns by age and includes no-loss reports. It shows lower loss-reporting rates but higher median reported losses among older adults.[2]

03

FinCEN BSA

Financial-institution suspicion

Captures suspicious activity reported by banks and other financial institutions. The amounts are not the same as confirmed consumer losses.[5]

Language matters

In this paper, 'older adult' is the default. 'Elder fraud' and 'elder financial exploitation' are used when referring to established FBI, DOJ, FinCEN, or regulatory terminology. Financial exploitation can involve a stranger or a person the older adult knows.[5][13]

EVIDENCE DISCIPLINE

- Reported complaints are not a prevalence estimate; many events are never reported.
- Categories can overlap. Cryptocurrency and AI-related labels may describe how a crime was facilitated, not a separate crime type.
- Victims may not know whether AI was involved, so AI-related complaint counts are likely incomplete.

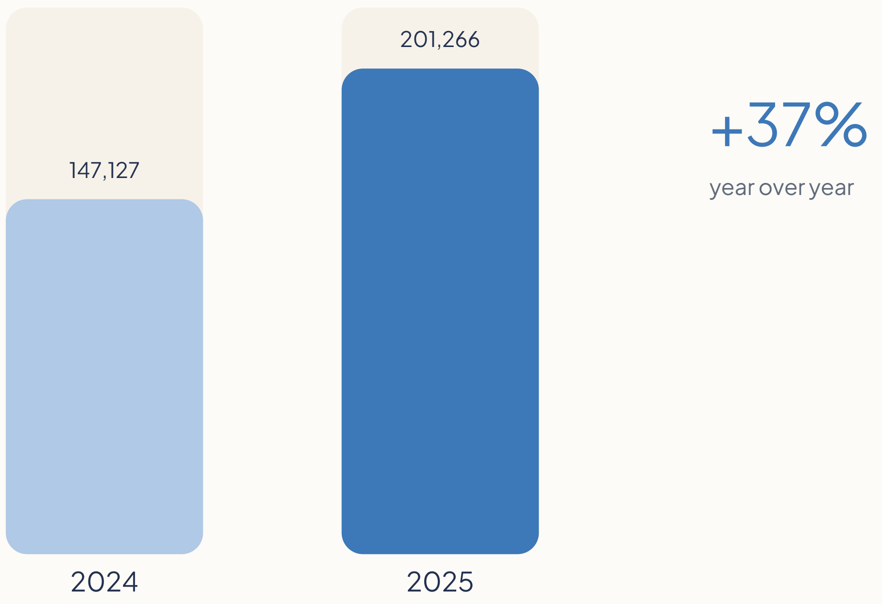
Sources: FTC older consumers report [2]; FinCEN EFE analysis [5]; DOJ Elder Justice Initiative [13].

01 - THE REPORTED SCALE

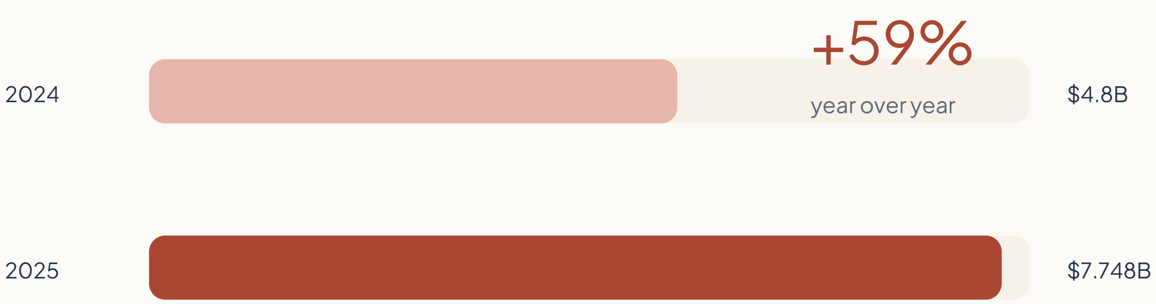
Reported losses grew faster than complaint volume

IC3 received 201,266 complaints from people age 60+ in 2025, 37% more than in 2024. Adjusted reported losses reached $7.748 billion, 59% more than the prior year.[1][19]

COMPLAINTS FILED BY PEOPLE AGE 60+



ADJUSTED REPORTED LOSSES



Why the gap matters

IC3 reports that 12,444 complainants age 60+ lost more than $100,000 in 2025.[1]

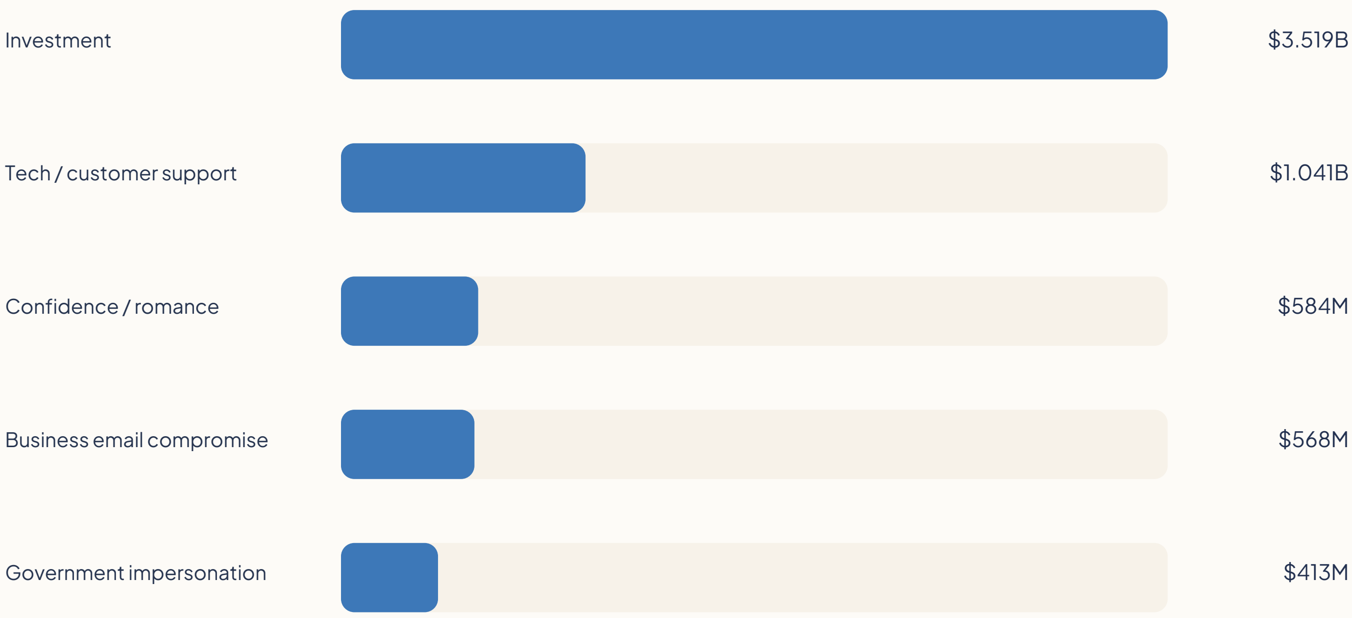
Sources: FBI IC3 2025 Annual Report [1] and 2024 Annual Report [19]. Figures are rounded where shown.

WHERE REPORTED LOSSES CONCENTRATE

Investment and support scams dominate the 60+ loss table

In 2025 IC3 complaints filed by people age 60+, investment complaints accounted for $3.519 billion in reported losses. Tech and customer support followed at $1.041 billion. Cryptocurrency was tracked separately as a descriptor and appeared in $4.347 billion of reported 60+ losses, so it should not be added to the categories below.[1]

2025 IC3 ADJUSTED LOSSES REPORTED BY PEOPLE AGE 60+



The AI signal is visible but incomplete

IC3 recorded 3,143 AI-related complaints from people age 60+ with $352.5 million in reported losses. Across all ages, IC3 recorded 22,364 AI-related complaints and $893.3 million in losses. Because complainants may not know whether AI was used, these figures should be read as identified AI references, not total AI-enabled fraud.[1]

Source: FBI IC3 2025 Annual Report [1]. Crime types and descriptors may overlap; amounts should not be summed across those systems.

A NECESSARY CORRECTION

This is not a story about older adults being easier to fool

FTC data show that older adults reported losing money to fraud at a lower rate than younger adults. When a loss was reported, however, the median loss was higher, especially for people age 80 and older.[2]

$900

MEDIAN REPORTED LOSS, AGE 60+

FTC Consumer Sentinel reports for 2024.[2]

$1,650

MEDIAN REPORTED LOSS, AGE 80+

Higher than any other age group in the FTC report.[2]

A BETTER RISK MODEL

Exposure

Scammers can reach anyone through calls, texts, email, social media, search ads, and pop-ups.

Irreversible rails

Cryptocurrency, cash, wires, and gold can turn one pressured decision into a hard-to-recover loss.[4]

Available assets

Retirement savings, home equity, and accumulated balances can make a successful event more costly.

Isolation under pressure

High-loss imposter scams often aim to keep the person on the phone and away from a second opinion.[4]

What follows from the evidence

A respectful defense adds time, independent verification, and trusted connection around high-risk actions. It does not remove independence from everyday decisions.

Sources: FTC older consumers report [2]; FTC high-loss imposter Data Spotlight [4].

02

What AI changes

AI can make a false story faster to produce and easier to believe. It cannot complete the fraud on its own. Money, a code, a password, or access still has to move through a real channel.

Sources: FBI IC3 2025 [1]; FBI generative AI public service announcement [3].

WHAT CHANGED

Four capabilities make old fraud easier to scale

The FBI describes AI-generated text, images, audio, and video as tools that can increase believability while reducing the time and effort required to create deceptive content.[3]

01

Polish

Fluent language, cleaner formatting, and faster translation remove familiar warning signs such as awkward grammar.

02

Personalization

Public data and stolen information can be woven into a tailored story, profile, or message.

03

Synthetic presence

Cloned audio, generated images, and deepfake video can imitate family members, officials, or advisers.

04

Scale and persistence

One operation can maintain many distinct conversations, vary scripts, and produce new content quickly.

What did not change

The scam still needs a decision that benefits the fraudster: send money, reveal a one-time code, enter credentials, install remote-access software, or keep the request secret.

Sources: FBI IC3 generative AI PSA [3]; FTC family emergency guidance [6]; SEC/NASAA/FINRA investor alert [7].

WHERE AI ENTERS

AI makes the first contact more convincing

It helps to separate the parts AI can improve from the moments when a household or institution can still interrupt what is happening.

1 **Reach**
Call, text, email, ad, social message
AI CAN AMPLIFY

2 **Credibility**
Polish, personal facts, cloned voice, fake profile
AI CAN AMPLIFY

3 **Pressure**
Urgency, authority, fear, secrecy
AI CAN AMPLIFY

4 **Isolation**
Stay on the line; do not tell anyone

5 **Transfer**
Money, code, credential, remote access

6 **Recovery scam**
A second promise to get the money back
AI CAN AMPLIFY

The intervention points

Pause interrupts pressure. Verify another way breaks the sender's control of the channel. Share breaks isolation before transfer.

Synthesis based on FBI AI mechanisms [1][3], FTC high-loss imposter patterns [4], and FTC family emergency guidance [6].

SPOTLIGHT

A familiar voice is no longer proof of identity

The FBI and FTC both warn that a short audio sample can be used to create a convincing imitation of a loved one. In 2025, IC3 recorded more than $5 million in losses to distress scams with a reported AI nexus.[1][6]

FICTIONAL CALL

Family emergency

Unknown number

"Please do not call Mom. I need money for bail right now."

DO NOT TEST THE VOICE

- End the call, even when the story feels urgent.
- Call the person on a number you already know.
- If they do not answer, contact another family member.
- Use a private family phrase that is not posted online.

Why this works

Independent verification works whether the voice was cloned, the caller was a skilled impersonator, or the emergency was genuine. The response does not depend on identifying the technology.

DEEPFAKE INVESTMENT RISK

AI-generated video and audio can also imitate celebrities, executives, government officials, or investment professionals. Regulators recommend checking registration and contacting the real organization through independently sourced information before moving money or securities.[7][18]

Sources: FBI IC3 2025 [1]; FTC voice-cloning guidance [6]; SEC/NASAA/FINRA alert [7]; Investor.gov [18].

THE KEY BEHAVIORAL SHIFT

Do not make AI detection the consumer's job

You do not have to decide whether a message, image, or voice was made with AI. You only have to notice when an unexpected interaction asks you to act before you can verify.

CLUES THAT ARE GETTING WEAKER	RULES THAT STILL HOLD
X Bad grammar	+ Unexpected pressure
X An unfamiliar accent	+ A request for secrecy
X A profile that looks artificial	+ A demand for codes or remote access
X A voice that sounds slightly wrong	+ Instructions to move money to protect it
X A message with one factual mistake	+ A refusal to let you verify independently

A strong standing rule

No legitimate bank, government agency, or company needs you to move money to a new account, cryptocurrency kiosk, courier, or pile of gold to keep it safe.[4][14][17]

Sources: FTC high-loss imposter Data Spotlight [4]; FTC 2025 imposter data [14]; FTC consumer alert [17].

03

Defense by design

The goal is not constant suspicion. It is a small set of household and institutional defaults that add time, a trusted channel, and another person around high-risk actions.

Framework companion: KinKeeper Elder Fraud & Scam Protection Playbook [15].

A THREE-MOVE RESPONSE

Pause. Verify another way. Share.

The response is intentionally simple enough to use under pressure and broad enough to work across calls, texts, email, physical mail, social media, and AI-generated content.[3][6][15]

01

Pause

Stop the interaction. Pressure is the cue to slow down, not proof that the request is real.

IN THE MOMENT

Do not click, reply, read a code, install software, or send money.

02

Verify another way

Leave the channel the sender controls. Use a saved number, official app, trusted statement, or website you type yourself.

IN THE MOMENT

Do not use a callback number, link, QR code, or search ad supplied by the interaction.

03

Share

Bring in a trusted person before a high-risk action. A calm second person breaks secrecy and sees the story from outside the pressure.

IN THE MOMENT

For a loved one, lead with thanks and help, not shame.

Why 'another way' matters

Asking the same caller to prove who they are keeps verification inside the attacker's channel. Independent verification changes who controls the evidence.

Sources: FBI generative AI PSA [3]; FTC family emergency guidance [6]; KinKeeper companion course [15].

BEFORE PRESSURE ARRIVES

A one-time household setup can protect everyday independence

Good fraud defense lives in defaults. Set these up during a calm moment, with the older adult making the choices.

1. **Choose a trusted check-in person**
   Decide who to contact before sending money, codes, or account access in response to an unexpected request.

2. **Create a private family phrase**
   Use something memorable that is not a birthday, pet name, or detail posted online.[3][7]

3. **Save official contact routes**
   Store bank, card, brokerage, and key family numbers. Use statements or official apps, not inbound links.

4. **Turn on account alerts**
   Enable alerts for transfers, withdrawals, password changes, new payees, and new devices where available.

5. **Adopt a two-person rule**
   For an unexpected request above a household-selected threshold, pause until a second trusted person reviews it.

6. **Name the non-negotiables**
   No one-time codes, remote access, safe-account transfers, gift cards, crypto kiosks, or couriers in response to surprise contact.

Optional bank support

Ask the bank, credit union, or brokerage what trusted-contact, notification, transaction-hold, and exploitation-response options it offers. A trusted contact does not automatically gain authority over the account.[8][9]

Sources: FBI AI PSA [3]; SEC/NASAA/FINRA investor alert [7]; CFPB [8]; interagency statement [9].

CONNECTION WITHOUT TAKEOVER

The best family role is a safe second channel

Scammers benefit when people feel embarrassed or fear losing control. Family systems should make it easier to ask for a second opinion while keeping the older adult at the center of the decision.

1. **Thank the pause**

   Say: 'Good call checking. Let's look at it together.'

2. **Verify with, not for**

   Open the official app or call a known number together whenever possible.

3. **Separate support from surveillance**

   Agree in advance which alerts are helpful and who sees them.

4. **Act before lecturing**

   If money or access moved, contact the provider first. Review warning signs later.

5. **Never shame**

   Anyone can be targeted. Shame reduces future disclosure and helps recovery scammers.

When the concern is a known person

Elder financial exploitation also includes theft or misuse by relatives, caregivers, fiduciaries, or other trusted people. If that is suspected, use local Adult Protective Services, law enforcement, and legal resources rather than confronting the suspected person alone.[5][13]

Sources: FinCEN elder financial exploitation analysis [5]; CFPB resources [8]; DOJ Elder Justice Initiative [13].

FOR INSTITUTIONS AND COMMUNITIES

Design for interruption, dignity, and a fast response

Financial institutions, senior-serving organizations, libraries, and caregiver programs can reduce the burden on individuals by building independent verification and human connection into the environment.

01

Detect patterns, not age

Monitor unusual transfers, new payees, account takeover signals, abrupt behavior changes, and high-risk payment rails. Do not treat age alone as proof of incapacity.

02

Offer trusted-contact options

Make designation clear, revocable, and separate from transactional authority. Explain when contact may occur.[8][9]

03

Add proportionate friction

Use callbacks, holds, escalation, or a second review for unusual high-risk transactions while preserving normal access.

04

Prepare the response path

Train staff on escalation, suspicious activity reporting, Adult Protective Services, law enforcement, and victim-centered communication.[5][9]

The system is already seeing the signals

FinCEN identified 155,415 elder-financial-exploitation-related BSA filings covering roughly $27 billion in suspicious activity over one year. About 80% of the filings involved elder scams and about 20% involved elder theft.[5]

Sources: FinCEN [5]; CFPB [8]; interagency statement on elder financial exploitation [9].

RESPONSE

Act quickly, preserve evidence, and avoid the second scam

A fast, calm response may limit damage. Recovery depends on how the money or access moved, so start with the financial or technology provider involved.[10]

1. **Contact the provider now**

   Call the bank, card issuer, wire service, payment app, brokerage, gift-card issuer, mobile carrier, or delivery service. Ask whether the transaction, transfer, package, or account change can be stopped or reversed.

2. **Secure exposed access**

   Change exposed passwords, contact the phone carrier after a SIM takeover, remove remote-access software, run a security scan, and review accounts for changes.

3. **Preserve the record**

   Save messages, envelopes, receipts, phone numbers, transaction IDs, wallet addresses, account details, and the timeline. Do not keep engaging with the scammer.

4. **Report through the right channels**

   Use ReportFraud.ftc.gov and IC3.gov. Use IdentityTheft.gov when personal information was misused. The National Elder Fraud Hotline is 833-372-8311.[10][11][12]

5. **Watch for recovery fraud**

   Scammers may impersonate law firms, agencies, or recovery specialists and ask for upfront money. Independently verify any offer to recover funds.[1]

If there is an immediate threat of physical harm, call 911. For suspected abuse or exploitation by a known person, contact local Adult Protective Services or law enforcement.[13]

Sources: FTC recovery guidance [10]; IdentityTheft.gov [11]; FBI elder fraud program [12]; DOJ [13].

COMPANION COURSE

Practice the decisions before pressure arrives

KinKeeper's free Elder Fraud & Scam Protection Playbook uses realistic, fictional scenarios to practice the same response across texts, email, physical mail, AI-enabled calls, relationship scams, money requests, and recovery.[15]

Chapters 1 and 6	Pressure and personalization	Practice recognizing urgency, authority, secrecy, and personal details that are not proof.
Chapters 2 and 3	Texts, email, and mail	Choose an independent route for bank alerts, delivery fees, government notices, and donations.
Chapters 4 and 5	AI voices and access	Respond to a familiar-sounding emergency, one-time-code requests, and remote-access demands.
Chapters 8 and 9	Connection and recovery	Help without shame and act quickly when money or access has already moved.
Chapter 10	Household plan	Choose concrete actions for a trusted person, family phrase, saved numbers, alerts, and reporting.

KinKeeper

The Elder Fraud & Scam Protection Playbook

Free. Private by default. No sign-up required.

kinkeeper.com/playbooks/elder-fraud-scam-protection/

The Playbook and KinKeeper fraud tools are educational and alerting resources. They cannot prevent or guarantee protection from scams.

Companion: KinKeeper Elder Fraud & Scam Protection Playbook [15].

METHODOLOGY

How this paper was researched

1

Evidence window

Sources were reviewed through July 15, 2026. The newest complete federal reporting period available was 2025 for FBI IC3 data and 2024 for the FTC older-consumer annual report.

2

Source selection

Primary federal sources were preferred: FBI IC3, FTC Consumer Sentinel, FinCEN BSA analysis, CFPB, DOJ, and joint securities-regulator guidance. KinKeeper material was used only for the companion framework and course mapping.

3

Data treatment

IC3, FTC, and FinCEN figures were kept separate because they measure different reporting channels and concepts. Dollar amounts were rounded only where the source itself used rounded values.

4

Editorial review

Claims were checked against the source ledger. High-volatility facts, reporting routes, and product availability are scheduled for quarterly review.

LIMITATIONS

- Complaint systems substantially undercount fraud and are influenced by awareness, access, reporting behavior, and contributor practices.
- Reported loss is not the same as verified adjudicated loss, and suspicious activity is not the same as confirmed victim loss.
- AI involvement is difficult for complainants to observe. Identified AI-related complaints are not a complete count of AI-enabled fraud.
- The category 'age 60+' covers a large and diverse population. It should not be treated as one risk profile.
- This paper is educational, not legal, investment, financial, cybersecurity, or law-enforcement advice.

Next scheduled review

October 15, 2026, or earlier if the FBI, FTC, reporting routes, or KinKeeper product availability materially changes.

FREE INTERACTIVE COURSE

Practice the moves before pressure arrives

The Elder Fraud & Scam Protection Playbook turns this paper's guidance into realistic, fictional practice. Learners work through modern scam scenarios and build a response they can use without having to identify the technology behind the message.

FREE INTERACTIVE COURSE

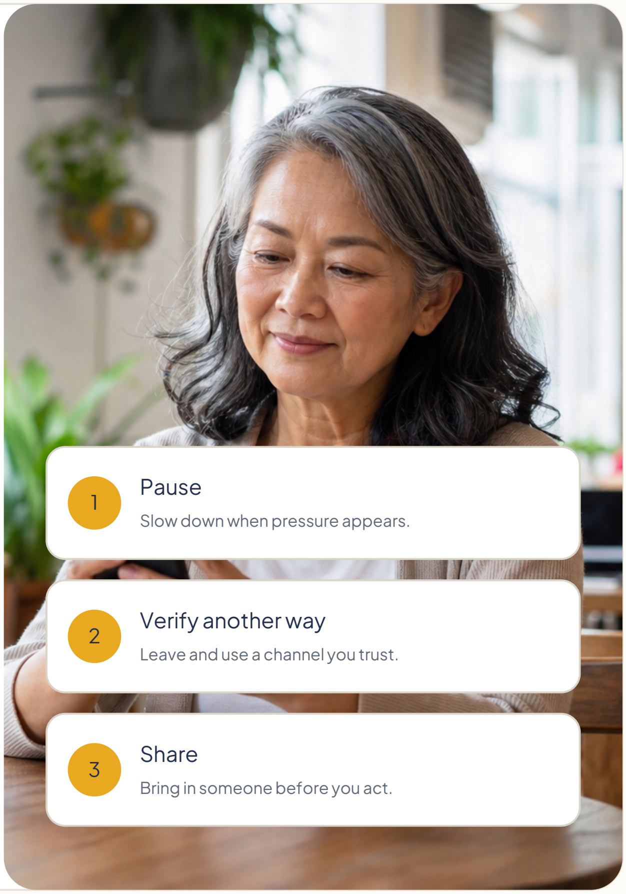
The Elder Fraud & Scam Protection Playbook

Practice recognizing scams across texts, email, physical mail, calls, and relationships, then choose habits you can use right away.

- 25-30 minutes
- 10 chapters
- No sign-up
- Private by default

Open the free course

kinkeeper.com/playbooks/elder-fraud-scam-protection/



Practice, not a test

Fictional scenarios teach repeatable decisions. The course does not create a vulnerability score.

For you or a loved one

Choose the perspective that fits. Progress and answers stay in the learner's browser.

Free and easy to share

No account is required. Organizations can also embed the responsive course.

REFERENCES

Sources 1 of 2

[1] Federal Bureau of Investigation, Internet Crime Complaint Center. *2025 IC3 Annual Report*. 2026. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf. Accessed 2026-07-15. Primary source for 2025 complaint, loss, age, crime-type, cryptocurrency, and AI-related complaint data.

[2] Federal Trade Commission. *Protecting Older Consumers 2024-2025*. December 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf. Accessed 2026-07-15. Primary source for Consumer Sentinel reporting patterns, age comparisons, median reported losses, and reporting limitations.

[3] Federal Bureau of Investigation, Internet Crime Complaint Center. *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*. December 3, 2024. https://www.ic3.gov/PSA/2024/PSA241203. Accessed 2026-07-15. Primary source for AI-enabled text, image, audio, and video fraud mechanisms and consumer guidance.

[4] Federal Trade Commission. *False alarm, real scam: how scammers are stealing older adults' life savings*. August 7, 2025. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings. Accessed 2026-07-15. Primary source for high-loss imposter scam patterns, contact methods, payment methods, and population-normalized reporting comparisons.

[5] Financial Crimes Enforcement Network. *FinCEN Issues Analysis on Elder Financial Exploitation*. April 18, 2024. https://www.fincen.gov/news/news-releases/fincen-issues-analysis-elder-financial-exploitation. Accessed 2026-07-15. Primary source for Bank Secrecy Act reporting, $27 billion in suspicious activity, and the distinction between elder scams and elder theft.

[6] Federal Trade Commission. *Scammers use AI to enhance their family emergency schemes*. March 20, 2023. https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes. Accessed 2026-07-15. Primary consumer guidance on voice cloning and independent verification.

[7] SEC Office of Investor Education and Advocacy, NASAA, and FINRA. *Artificial Intelligence (AI) and Investment Fraud: Investor Alert*. January 25, 2024. https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud. Accessed 2026-07-15. Primary regulatory guidance on AI-themed investment fraud, deepfake endorsements, registration checks, and family verification phrases.

[8] Consumer Financial Protection Bureau. *Protecting Older Adults from Fraud and Financial Exploitation*. Updated March 10, 2026. https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/protecting-against-fraud/. Accessed 2026-07-15. Primary guidance for trusted contacts, banks, caregivers, and community organizations.

[9] Federal financial regulatory agencies. *Interagency Statement on Elder Financial Exploitation*. December 4, 2024. https://files.consumerfinance.gov/f/documents/cfpb_interagency-statement-on-elder-financial-exploitation_2024-12.pdf. Accessed 2026-07-15. Primary guidance for financial-institution governance, trusted contacts, holds, monitoring, and reporting.

[10] Federal Trade Commission. *What To Do if You Were Scammed*. Current consumer guidance. https://consumer.ftc.gov/articles/what-do-if-you-were-scammed. Accessed 2026-07-15. Primary recovery guidance by payment type, credential exposure, and device access.

REFERENCES

Sources 2 of 2

[11] Federal Trade Commission. *IdentityTheft.gov*. Current federal service. https://www.identitytheft.gov/. Accessed 2026-07-15. Federal identity-theft reporting and recovery-plan service.

[12] Federal Bureau of Investigation, Internet Crime Complaint Center. *Elder Fraud*. Current program page. https://www.ic3.gov/crimeinfo/elderfraud. Accessed 2026-07-15. Official definition, reporting route, and National Elder Fraud Hotline details.

[13] U.S. Department of Justice, Elder Justice Initiative. *Financial Exploitation*. Current program page. https://www.justice.gov/elderjustice/financial-exploitation. Accessed 2026-07-15. Official distinction between financial abuse by known people and financial fraud by strangers, plus help resources.

[14] Federal Trade Commission. *FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025*. June 2026. https://www.ftc.gov/news-events/news/press-releases/2026/06/ftc-data-show-people-reported-losing-3-point-5-billion-imposter-scams-2025. Accessed 2026-07-15. Current all-age context for imposter scam losses and business and government impersonation.

[15] KinKeeper. *The Elder Fraud & Scam Protection Playbook*. July 2026. https://www.kinkeeper.com/playbooks/elder-fraud-scam-protection/. Accessed 2026-07-15. Companion course and source of the Pause, Verify another way, Share learning model. Not used as external evidence.

[16] Plaid. *The New Identity Crisis: Rethinking Fraud in the AI Era*. February 2026. https://downloads.ctfassets.net/ss5kfr270og3/1K5FPXZynsEf7qdj8u3TxJ/05ade5f5c164d72f1b3daa63dbe9e674/Rethinking_Fraud_in_the_AI_Era.pdf. Accessed 2026-07-15. Design and format reference supplied by the user. Not used as evidence for KinKeeper claims.

[17] Federal Trade Commission. *How to handle unexpected calls that claim your money is at risk*. January 2026. https://consumer.ftc.gov/consumer-alerts/2026/01/how-handle-unexpected-calls-claim-your-money-risk. Accessed 2026-07-15. Current guidance on independent contact information and fraudulent search advertisements.

[18] Investor.gov. *Relationship Investment Scams - Protect Yourself*. Current investor guidance. https://www.investor.gov/protect-your-investments/fraud/types-fraud/relationship-investment-scam. Accessed 2026-07-15. Primary guidance on relationship investment fraud, fake trading evidence, and AI-generated media.

[19] Federal Bureau of Investigation, Internet Crime Complaint Center. *2024 IC3 Annual Report*. April 2025. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. Accessed 2026-07-15. Primary comparison source for 2024 complaints and losses reported by people age 60+.

KinKeeper

KinKeeper helps families coordinate daily wellbeing check-ins and protection across Privacy, Money, and Identity. The Kin Circle receives outcomes, summaries, and alerts while the person at the center keeps their independence.

Two 15 Foundry, LLC dba KinKeeper | kinkeeper.com | Research edition 1.0