NELSON MULLINS

WHEN SILENCE IS COSTLY

Elder Financial Exploitation and Bank Liability

Dowse B. “Brad” Rustin IV
Chair, FinReg and FinTech Teams
Nelson Mullins
The Experience 2026 | September 29, 2026

The hour: from prevalence to prevention

01
The scale

02
How it happens

03
What the bank sees

04
Authority and liability

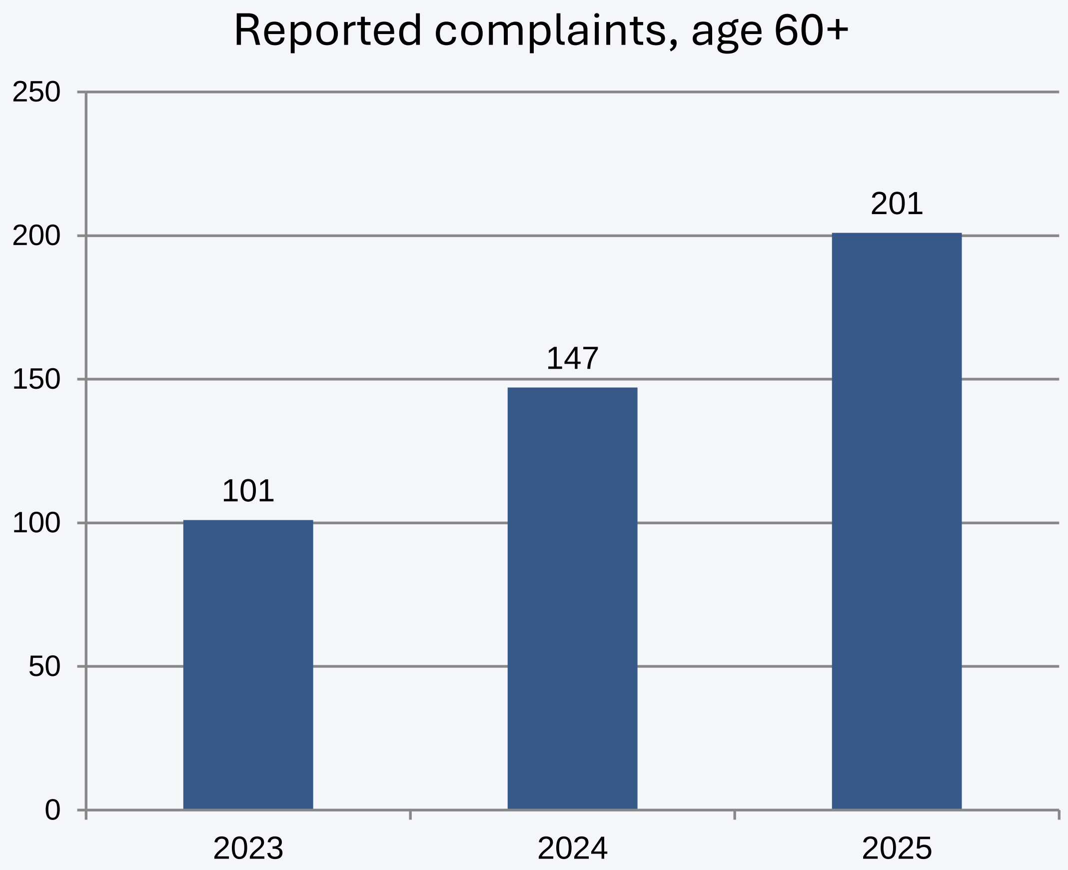
05
A defensible response

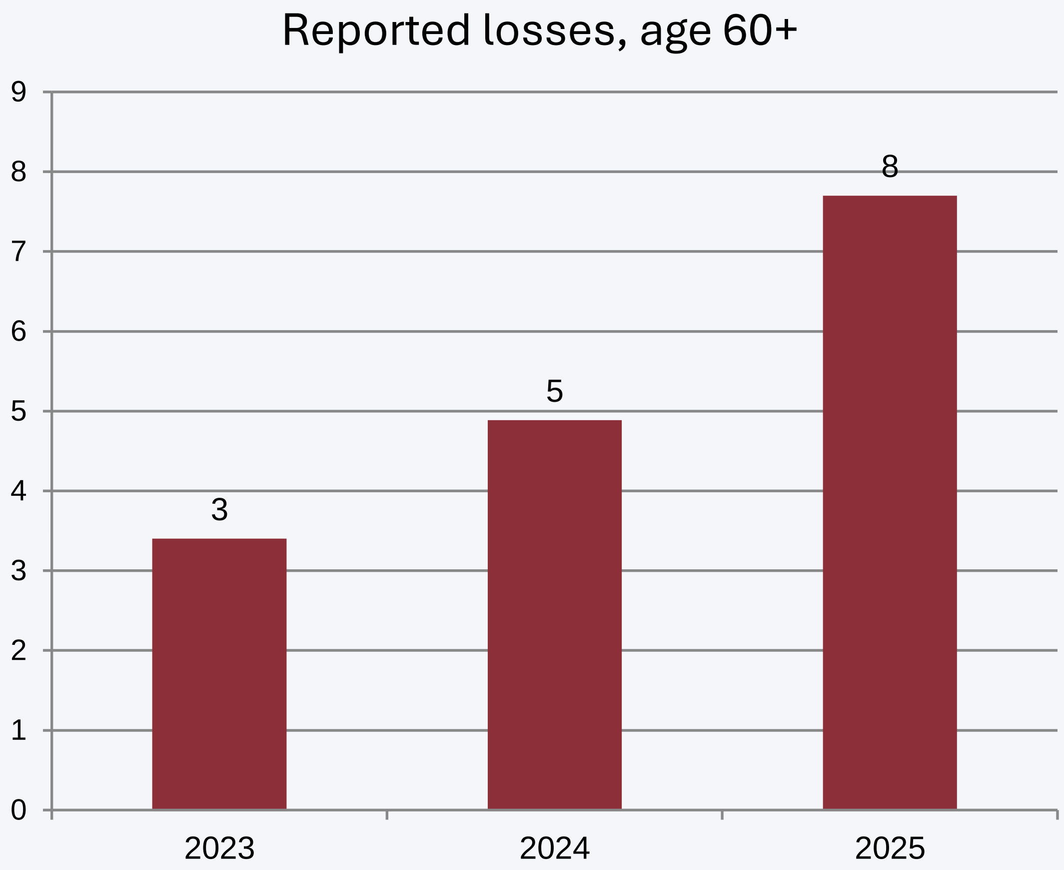
Elder fraud is now a balance-sheet event

201,000+	**$7.7B+**	**$38,000+**	**12,400+**
IC3 complaints from people 60+ in 2025	Reported IC3 losses by people 60+ in 2025	Average reported loss in 2025	Victims reporting losses of at least $100K

Reported data understates the operational problem: many victims never report, report late, or do not yet recognize the loss.

Losses are accelerating faster than complaint volume





FTC data tell the same story

4×

Increase in FTC-reported losses by older adults from 2020 to 2024

$2.4B

FTC reported losses by adults 60+ in 2024

$159M

Tech-support scam losses reported by older adults in 2024

Reported losses by fraud type, victims age 60+

Investment fraud is the costliest; call-center schemes drive the most complaints.

Total: more than $7.7 billion reported by 201,000+ victims age 60 and over.

Source: FBI Internet Crime Complaint Center (IC3), 2025 Elder Fraud Annual Report, top crime types by loss, complainants 60+.

What one year of SAR filings revealed

FinCEN analyzed BSA reports filed between June 2022 and June 2023.

155,415	$27B	15,993	80%
EFE-related filings in one year	In reported suspicious activity	Average monthly filings after the review period	Of activity was scam-related

Banks filed the vast majority of these reports, which makes bank data the clearest picture we have.

Source: FinCEN, *Financial Trend Analysis on Elder Financial Exploitation*, June 2022 to June 2023 (April 2024).

The federal response, by the numbers

From the Department of Justice's 2025 Annual Report to Congress on elder fraud and abuse.

280+	600+	$2B+	1M+
Enforcement actions brought	Defendants charged, many extradited	Stolen or targeted for theft	Older Americans affected

DOJ has also held more than 1,000 awareness and training events, reaching nearly 15 million Americans.

Source: U.S. Department of Justice, *Annual Report to Congress on Activities to Combat Elder Fraud and Abuse* (October 2025).

Two faces of elder financial exploitation

FINANCIAL ABUSE—SOMEONE YOU KNOW

- Family members, caregivers, and trusted advisors are the most common perpetrators.
- Access is granted, not stolen—powers of attorney and joint accounts.
- Losses build gradually and look like ordinary account activity.
- Victims often stay silent to protect the relationship.

FINANCIAL FRAUD—A STRANGER

- Scammers reach victims by phone, text, email, social media, and dating sites.
- Built on manufactured trust or manufactured fear, then urgency.
- Funds leave by wire, cash, gift card, or crypto—fast and hard to recover.
- Victims are frequently coached to lie to bank staff.

Source: U.S. Department of Justice, Elder Justice Initiative - Financial Exploitation.

Scams and theft leave different fingerprints

ELDER SCAMS BY A STRANGER

- Roughly 80 percent of all reported activity.
- Account takeover is the most cited typology.
- Perpetrators avoid direct contact with staff.
- Methods are basic: phishing and reused passwords.
- Appendix A catalogs 15 prominent scam patterns.

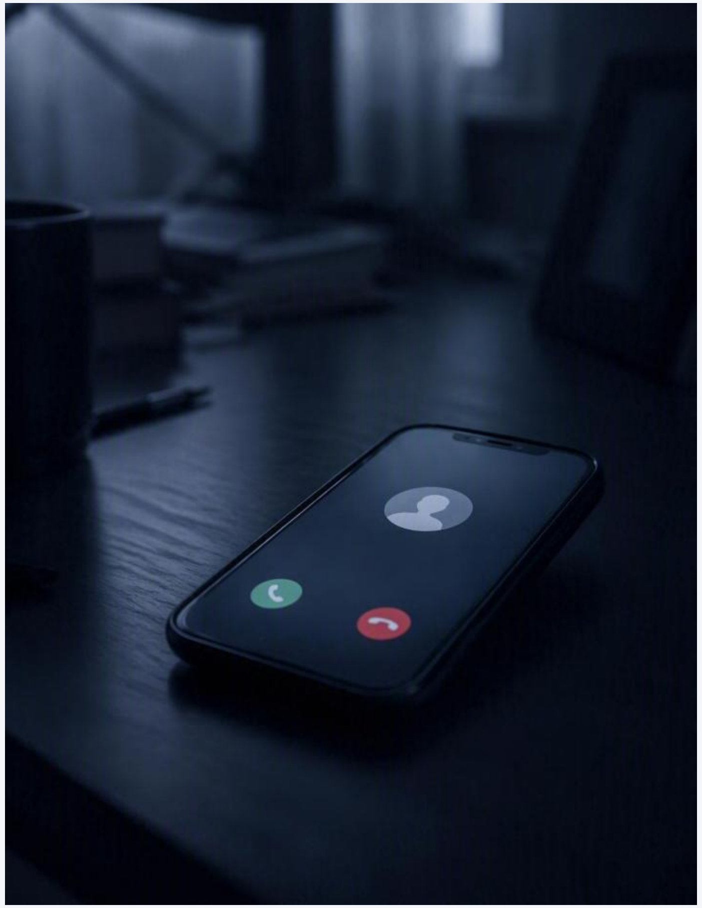
ELDER THEFT BY SOMEONE KNOWN

- Adult children are behind roughly 40 percent.
- Access comes by power of attorney or joint account.
- Activity blends into ordinary account history.
- Theft is widely undetected and underreported.
- Fewer filings does not mean fewer incidents.

Source: FinCEN, *Financial Trend Analysis on Elder Financial Exploitation* (April 2024).

Scam types DOJ and the FBI see most

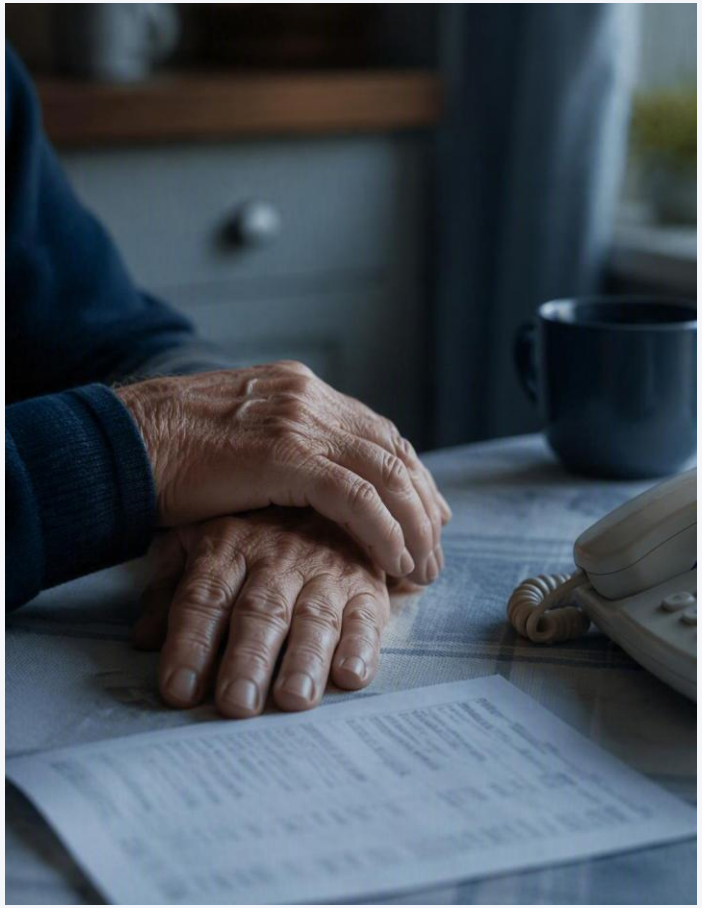
- Government impersonation—SSA, IRS, or FBI threatening arrest.
- Grandparent scams—a caller who needs bail money right now.
- Romance and confidence scams built over months.
- Tech support schemes—fake alerts and bogus refunds.
- Sweepstakes and lottery scams demanding fees up front.
- Payment by wire, cash courier, gift card, or crypto.



Source: DOJ Elder Justice Initiative, Senior Scam Alert.

How trusted access gets misused

- Power of attorney abuse—an agent spends the money on themselves.
- Names added to signature cards or accounts converted to joint ownership.
- Unauthorized use of the older adult’s ATM or debit card.
- Abrupt changes to a will, deed, trust, or beneficiary.
- Guardianship abuse, including fees for services never provided.
- Isolation of the older adult from family and advisors.



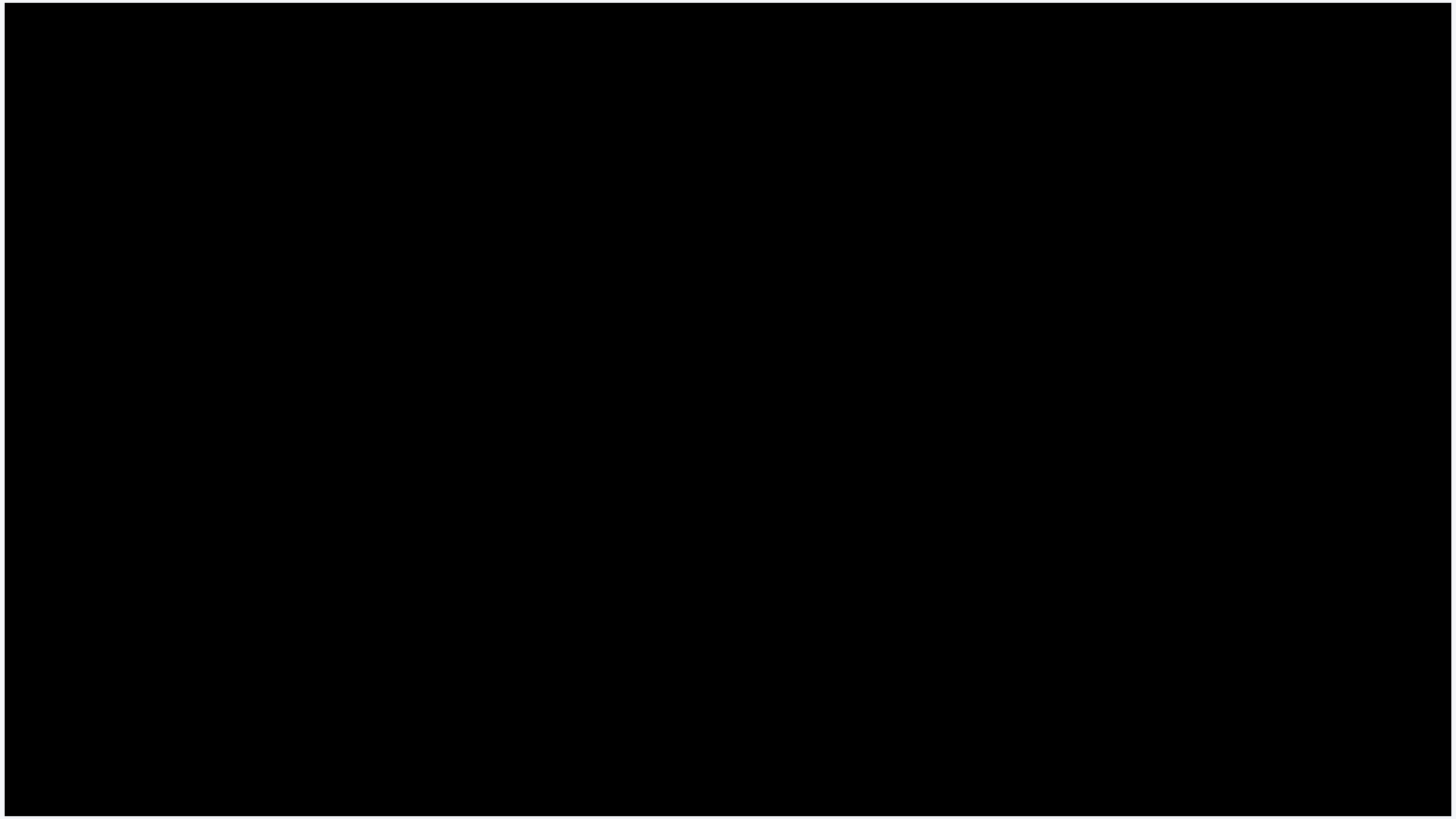
Source: DOJ Elder Justice Initiative, Spotting Financial Abuse.

The bank sees the transaction. The scammer controls the story.

- Scammer creates urgency, authority, and secrecy.
- Victim rehearses an explanation before reaching the bank.
- Questions from bank staff are reframed as obstruction.
- Escalation can deepen the victim’s commitment to the scam.

Hearing it from the victim

Why the voice on the phone outranks the teller, the family, and the police.



Source: Federal Bureau of Investigation, public awareness material on elder fraud.

The credibility inversion

Why might a customer trust the scammer over the bank?

CONTINUITY

The scammer has spent hours or weeks building a narrative.

SECRECY

The victim has been told not to trust family, police, or the bank.

COMMITMENT

Prior payments make admitting error psychologically costly.

IDENTITY

The victim sees the transaction as proof of competence or loyalty.

A real-world illustration: warning itself can look suspicious

An FBI agent identified a likely victim in her 70s. The victim ignored two calls, answered a third with suspicion, hung up, and blocked the agent. The agent eventually reached her at work and persuaded her that she had already sent more than $500,000.

Operational implication: a customer's confidence may reflect successful grooming, not informed consent.

The harm runs past the dollars

- Shame, anxiety, and depression follow the financial loss.
- Life savings and home equity are often gone before anyone intervenes.
- Victims can feel complicit in their own victimization.

Sources: DOJ Elder Justice Initiative; DOJ Office for Victims of Crime.

Most of it never reaches anyone

- Only a fraction of incidents are ever reported.
- When a relative is the abuser, reporting means accusing a family member.
- DOJ is clear that no one is ever to blame for being victimized.

Sources: DOJ Elder Justice Initiative; DOJ Office for Victims of Crime.

Red flags in the account record

01 Unusual account activity—large, frequent or unexplained withdrawals.

02 A switch to a more complicated account the customer does not need or understand.

03 Withdrawals or transfers the customer cannot explain.

04 Sudden non-sufficient funds activity or unpaid bills.

05 Closing CDs or accounts without regard to penalties.

06 Uncharacteristic attempts to wire large sums of money.

07 Suspicious signatures on checks or outright forgery.

08 Checks written as "loans" or "gifts."

09 Bank statements no longer going to the customer's home.

10 New powers of attorney the older person does not understand.

11 Altered wills and trusts.

Source: American Bankers Association Foundation, "*14 Red Flags for Elder Financial Abuse*"; behavioral items regrouped.

WARNING SIGNS

The DOJ’s top warning signs of abuse for family members

- Sudden changes in bank accounts or banking practices.
- An unexplained withdrawal of a large sum by someone accompanying the older adult.
- Additional names appearing on a bank signature card.
- Unauthorized withdrawals using the older adult’s ATM card.
- Abrupt changes in a will or other financial documents.
- Unexplained disappearance of funds or valuable possessions.
- Substandard care or unpaid bills despite available resources.
- Sudden transfer of assets to a family member or someone outside the family.

Source: U.S. Department of Justice, Elder Justice Initiative - Red Flags of Elder Abuse.

BEHAVIORAL RED FLAGS

What the customer’s conduct reveals

- A caregiver or other individual shows excessive interest in the older customer’s finances or assets.
- The companion will not allow the customer to speak independently or refuses to leave the customer’s side.
- The customer shows unusual fear of, or submissiveness toward, a caregiver.
- The customer expresses fear of eviction or nursing home placement if money is not given to a caretaker.
- The bank cannot speak directly with the customer despite repeated attempts to reach them.
- A new caretaker, relative, or friend suddenly transacts for the customer without proper documentation.
- The customer appears coached, providing rehearsed explanations or answers arriving by phone.
- Urgency and secrecy: the customer resists questions or asks that family not be told.

Sources: ABA Foundation, *Know the Signs*; DOJ Elder Justice Initiative; 2024 Interagency Statement on Elder Financial Exploitation.

What frontline staff see

- First-ever or atypical wire
- New overseas beneficiary
- Customer coached by phone
- Inconsistent purpose
- Urgency or secrecy
- Sudden liquidation or credit

The bank’s approach to stopping abuse must be *practical*, not *prescriptive*

The 2024 interagency statement provides examples of risk-management practices for identifying, preventing, and responding to elder financial exploitation. It expressly states that it does not create new compliance standards, regulatory requirements, or supervisory expectations.

- Employee training and escalation.
- Transaction holds or delays, where lawful.
- Trusted-contact programs.
- SAR filing and law-enforcement coordination.
- Information sharing consistent with privacy law.

Mandatory in some states, permissive in others

Whether a bank must report, or merely may report, depends entirely on the state.

MANDATORY REPORTING

- Some states name financial institution staff as mandated reporters outright.
- Other state obligations reach bank employees plus supervisory, compliance, and legal staff.
- Other states make every person a mandated reporter, which sweeps in bank staff.
- The duty usually runs to APS, and in some states, to a financial regulator, as well.
- Failing to report can carry its own penalty.
- You should carefully review the mandatory reporting laws in your states.

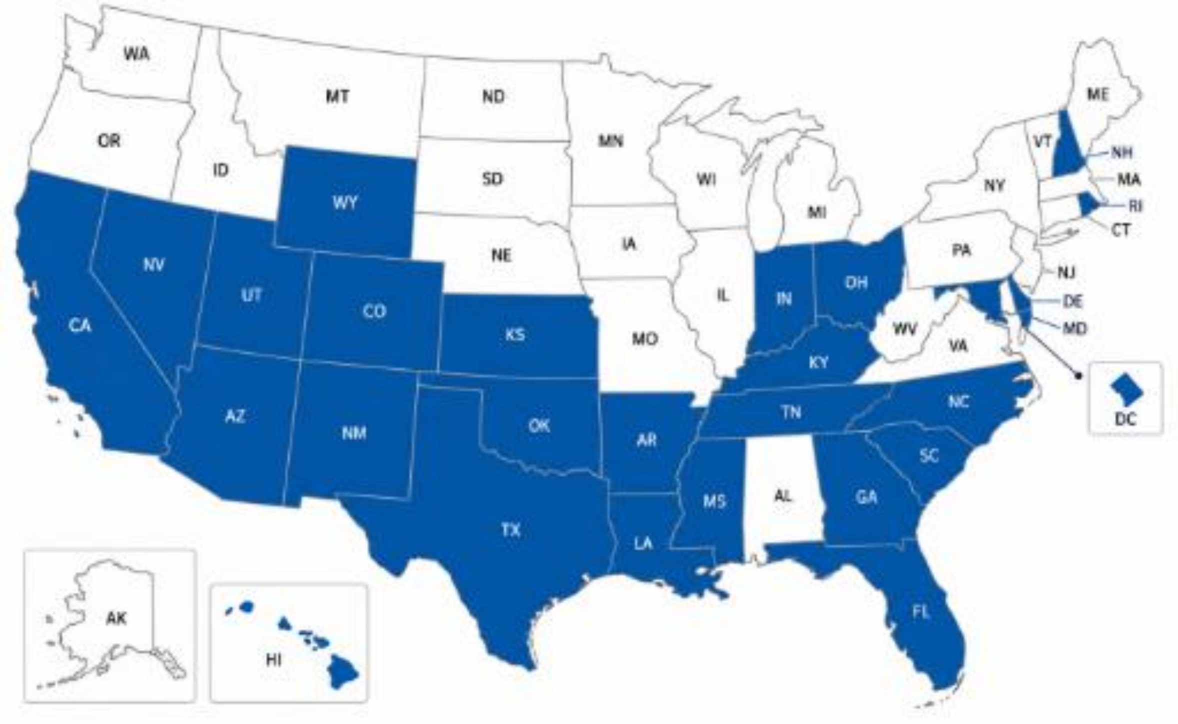
PERMISSIVE REPORTING

- Many states authorize a report but do not require one.
- Permissive statutes normally pair the option with good-faith immunity.
- Several states add a transaction hold, commonly for up to 15 days.
- A permissive statute protects the report, not the decision to do nothing.

Sources: ABA Commission on Law and Aging, bank reporting of suspected elder financial exploitation; CFPB 2019 Advisory Update, Appendix A; state-by-state reporting summaries.

Where reporting is mandatory

- Scope varies: some statutes name bank employees directly, others reach only securities professionals.
- Reports generally run to Adult Protective Services, and in several states, to a financial regulator as well.
- More recently, states have passed legislation allowing a bank to “delay” or “pause” a transaction; however, this generally requires mandatory reporting. For example, Alabama and Virginia have implemented this structure.
- Confirm your own state before relying on this map.



Source: CFPB, *Reporting of Suspected Elder Financial Exploitation by Financial Institutions* (July 2019), Appendix A. Counts and coverage are as of April 2019; several states have amended their statutes since. Map is illustrative only.

Privacy law is not a reason to stay silent

- Eight agencies signed it: FRB, CFTC, CFPB, FDIC, FTC, NCUA, OCC, and SEC.
- Reporting suspected abuse to the authorities does not generally violate GLBA privacy.
- Specific GLBA exceptions permit sharing without complying with notice and opt-out requirements.
- OCC Bulletin 2013-21 applied the guidance to national banks and federal savings associations.
- FinCEN advisories in 2011 and 2022 address SAR filing and new typologies.
- The 2024 interagency statement adds practices, not new regulatory requirements.

Sources: Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults (2013); OCC Bulletin 2013-21; Interagency Statement on Elder Financial Exploitation (2024).

The Senior Safe Act trades training for immunity

Section 303 of the 2018 Economic Growth, Regulatory Relief, and Consumer Protection Act.

WHAT IMMUNITY COVERS:

- Protection from liability in civil or administrative proceedings for reports from supervisors, compliance officers, legal officers, or BSA officers.
- Applies to disclosing suspected exploitation to a covered agency.
- Covers the institution and its eligible employees.
- Immunity turns on the customer being 65 or older, not ECOA's age threshold of 62.
- The report must be made in good faith and with reasonable care.
- No agency received rulemaking or enforcement authority.

WHAT THE TRAINING MUST DO:

- Teach staff to identify and report suspected exploitation.
- Cover the common signs of exploitation of a senior citizen.
- Explain internal escalation and reporting to authorities.
- Address customer privacy and confidentiality.
- Be appropriate to the attendee's job responsibilities.
- Be documented, because the record is what proves eligibility.

Sources: Senior Safe Act, Pub. L. 115-174 § 303; SEC, NASAA, and FINRA Senior Safe Act Fact Sheet; ABA compliance guide.

Reporting and records: silence leaves its own trail

72%

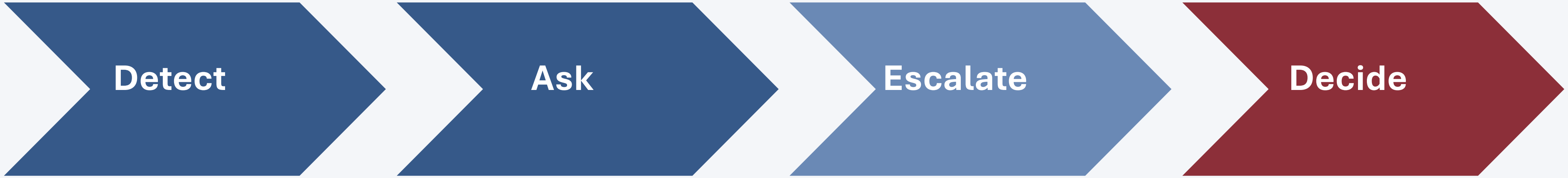
Share of elder-exploitation BSA filings made by banks in FinCEN analysis

- Create a contemporaneous chronology.
- Preserve unusual customer explanations verbatim.
- Record who escalated, who decided, and why.
- Avoid conclusory labels unsupported by facts.
- Coordinate SAR, APS, and law-enforcement pathways.

The bank’s liability rarely comes down to one law

State reporting duties	State transaction-hold authority	Privacy exceptions	UCC, Reg E payment rules
Contract terms	Negligence / aiding theories	UDAAP risk	Regulatory criticism

The moment of intervention: autonomy versus protection



- Separate capacity from persuasion.
- Do not treat authorization as the end of the inquiry.
- Document facts, statements, escalation, and rationale.
- Use legal authority precisely; avoid improvising holds.

A defensible escalation playbook

1	**Pause the script**	Move from routine service to structured inquiry.
2	**Test the narrative**	Use open-ended questions and repeat-back.
3	**Break contact**	Ask the customer to end the outside call.
4	**Add trusted voices**	Involve a supervisor, the fraud team, a trusted contact, APS or law enforcement.
5	**Document and decide**	Apply policy and legal authority; document the rationale.

What good customer language sounds like

AVOID

- "You are being scammed."
  Labels the customer as a dupe and triggers shame.
- "We cannot let you do this."
  Frames the bank as an obstacle to their autonomy.
- "If you insist, it is your loss."
  Ends the conversation and forfeits the relationship.
- "Are you sure? This is obviously a fraud."
  Direct challenge; the customer may withdraw or move the money elsewhere.
- "You should have known better."
  Blame silences the customer and deters future reporting.

USE

- "We see patterns like this when someone is being pressured."
  Names the scheme, not the customer.
- "Let's slow this down and verify independently."
  Buys time without refusing the request.
- "Our concern is protecting your choice before the money is irreversible."
  Puts autonomy at the center.
- "Try telling them no to the next request and see how they react."
  Let the customer test the relationship themselves.
- "Who else do you trust that we could bring into this?"
  Opens the door to a trusted contact or family member.

Sources: ICBA, *What to Say to Customers When They Are Being Scammed* (Dec. 2024); AARP BankSafe frontline training; FINRA trusted contact guidance (Rules 2165, 4512); CFTC, *How to Identify and Talk About Elder Fraud*.

Trusted contacts create a second channel of trust

Customer → **Bank** → **Trusted contact**

Advance consent lets the institution alert a designated person when a suspicious situation cannot be resolved directly with the customer.

What this means for a bank’s playbook

- Map reporting duties in every state where you take deposits.
- Know whether your state authorizes a disbursement hold, and exactly how long it lasts.
- File a SAR when exploitation is suspected and, where appropriate or required, report to APS and law enforcement.
- Expedite records and SAR supporting documentation when investigators ask.
- Collect trusted contacts at account opening so a second channel exists before a crisis.
- Train to the Senior Safe Act standard and retain attendance records.

Sources: CFPB 2016 Recommendations and 2019 Advisory Update; Interagency Statement on Elder Financial Exploitation (2024).

How to file and train

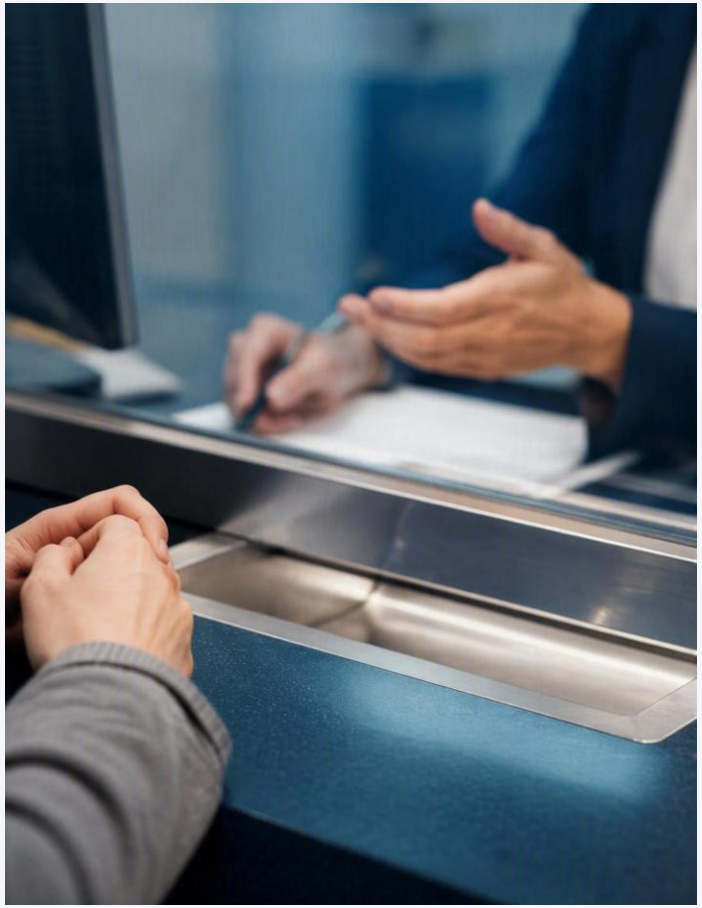
- Report suspected exploitation to all appropriate federal, state, and local authorities.
- File a SAR with FinCEN and use the term “elder financial exploitation” in the narrative.
- Never name the victim as the subject of the SAR.
- Train tellers and customer service staff first, because they see the behavior first.
- Pair staff training with customer education, such as ABA’s Safe Banking for Seniors.
- Keep current on FinCEN typologies, which the 2022 advisory materially expanded.

Sources: American Bankers Association, *Elder Financial Exploitation resources and SAR filing guidance*; ABA Foundation, *Safe Banking for Seniors*.

What we tell older adults to do

Practical steps to share with every community audience.

- Government agencies never call to threaten arrest or demand payment.
- Never wire money, send cash, or buy gift cards at a caller’s direction.
- Never give out Social Security numbers, passwords, or account access.
- Hang up and call back using a number you independently verify.
- Choose a power of attorney carefully and build in oversight.
- Stay connected—isolation is what perpetrators look for.



Source: DOJ Elder Justice Initiative, prevention and public outreach guidance.

Three questions for every institution

1. Can frontline staff recognize persuasion, not just incapacity?

2. Can the institution lawfully slow the transaction?

3. Can the file explain the decision six months later?

When silence is costly

The customer may authorize the payment.
The scammer may control the decision.
The bank must recognize the difference.

Questions and discussion

DISCLAIMER

About This Presentation

- The material provided herein is general and is not intended to be legal advice.
- Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules, and regulations, and other legal issues unique to your circumstances.
- Receipt of this material does not establish an attorney-client relationship.
- Nelson Mullins is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case or engagement is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements or marketing materials.

NELSON MULLINS

QUESTIONS OR FOLLOW UP?

Thank You

Dowse B. ("Brad") Rustin IV, CRCM, ACAMS

Chair, Financial Regulatory Practice

Nelson Mullins Riley & Scarborough LLP

Brad.Rustin@nelsonmullins.com

202.689.2320 (Washington, DC)

864.373.2320 (Greenville, SC)

NELSON MULLINS