

2026 Elder Financial Exploitation

Cooperative Credit Union Association

September 23, 2026

WIPFLI

Presenter



Stephanie Jennings, CRCM

Manager

WIPFLI

Fraud overview

Imposter scams

- 845,806 imposter scam reports
- \$3.5 billion lost to imposter scams in 2025
- Include people falsely claiming to be romantic interests, the gov't, a relative in distress, a well-known business, or a tech support expert.

Losses

- In 2025, people reported losing over \$15 billion to fraud.
- Over \$5 billion of losses reported were to investment-related scams.
- People aged 50 and older reported losing \$4.3 billion.

Top states

- Highest per capita rates of reported fraud: Florida, Alabama, Delaware, Nevada
- Highest overall financial losses: California (\$3.5 billion) and Texas, Florida, New York
- Lowest fraud rates: North Dakota

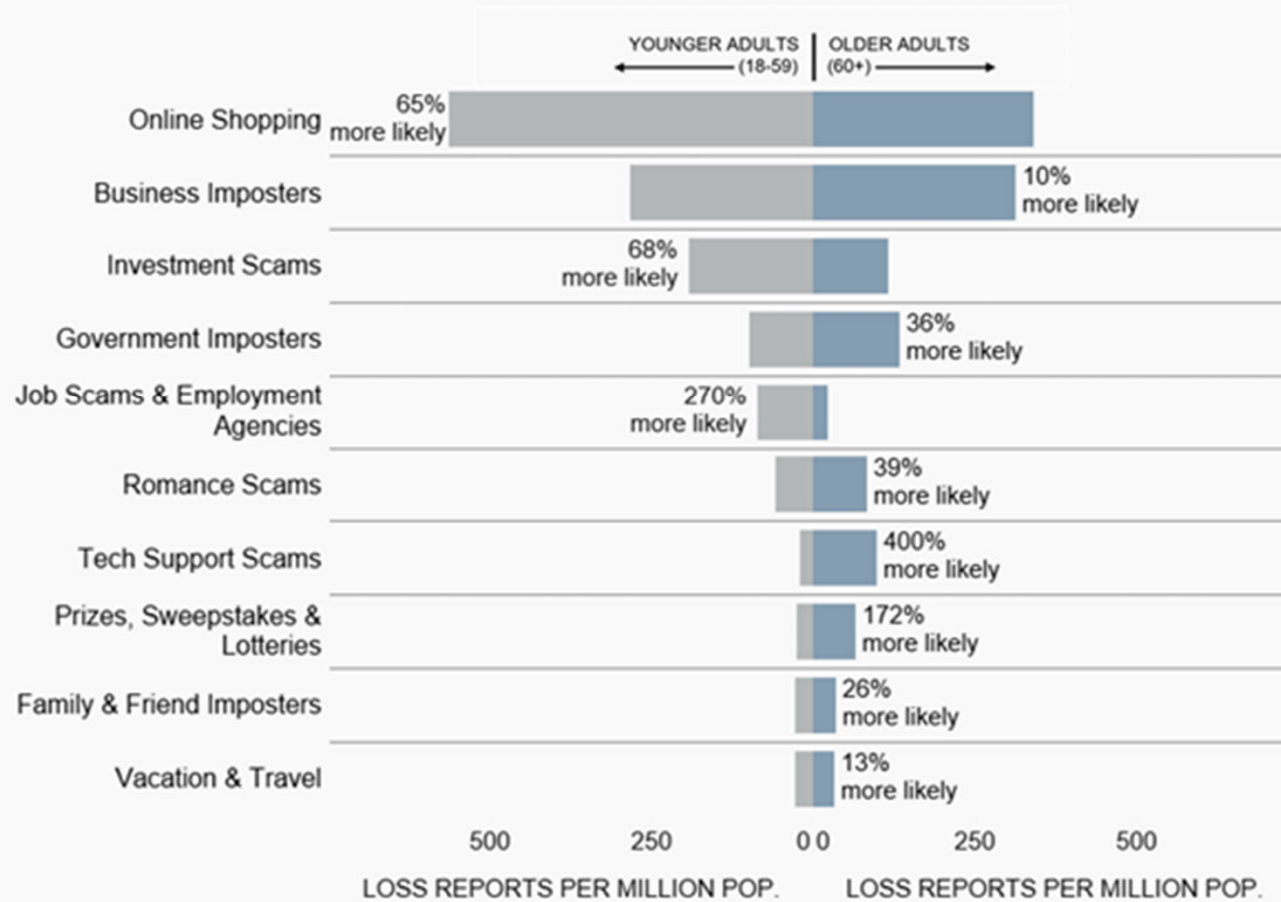
Top 10 Fraud Categories - National

Rank	Category	# of Reports	% Reporting \$ Loss	Total \$ Loss	Median \$ Loss
1	Imposter Scams	845,806	22%	\$2,952M	\$800
2	Online Shopping and Negative Reviews	383,441	76%	\$432M	\$130
3	Business and Job Opportunities	126,217	36%	\$751M	\$2,250
4	Investment Related	118,960	79%	\$5,697M	\$9,196
5	Internet Services	118,261	28%	\$164M	\$300
6	Prizes, Sweepstakes and Lotteries	97,350	22%	\$351M	\$1,000
7	Telephone and Mobile Services	92,520	39%	\$56M	\$240
8	Health Care	78,763	51%	\$80M	\$283
9	Travel, Vacations and Timeshare Plans	58,347	67%	\$274M	\$922
10	Mortgage Foreclosure Relief and Debt Management	34,159	21%	\$82M	\$1,500

By Age

FIGURE 4: 2024 LOSS REPORTS BY AGE AND FRAUD TYPE

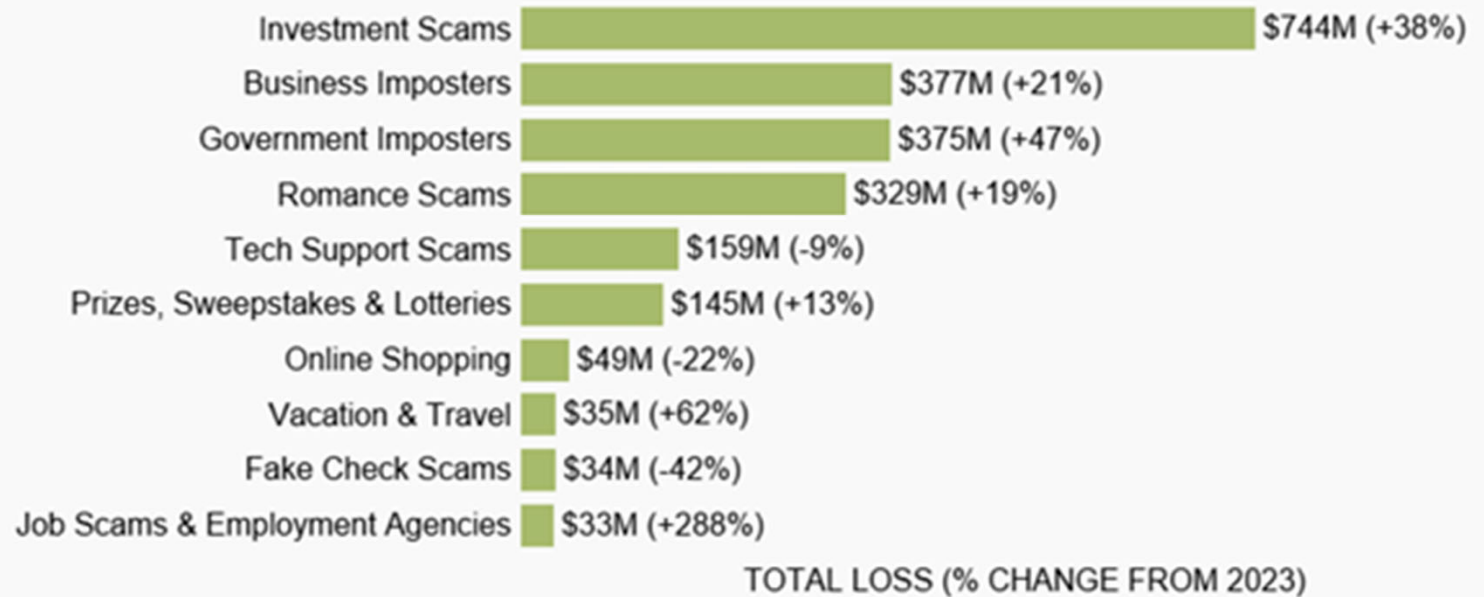
Losses to some types of fraud are more likely to be reported by younger adults, while others are more likely to be reported by older adults.



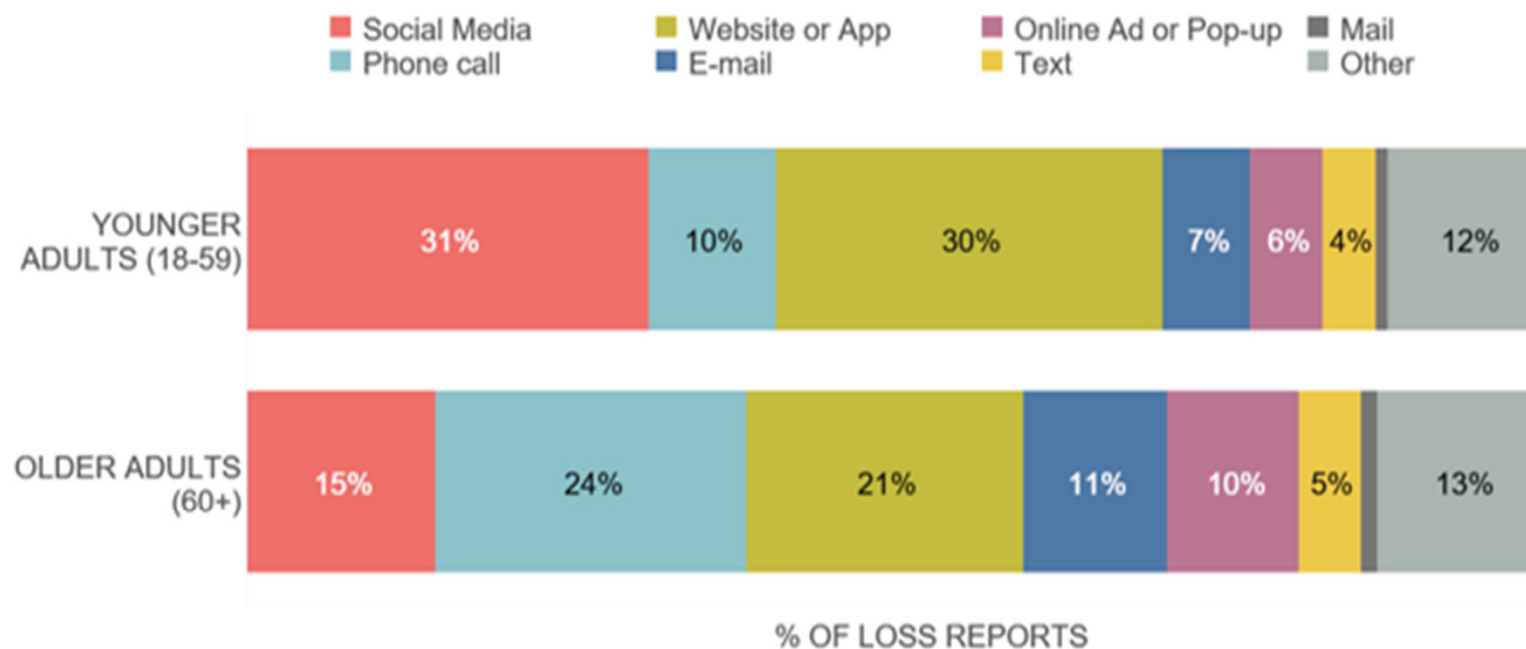
By Age

FIGURE 5: 2024 TOP FRAUD TYPES BY TOTAL DOLLARS LOST (AGES 60 AND OVER)

Reports suggest that some fraud types are far more costly to older adults in aggregate than others, and losses to a number of fraud types increased from 2023 to 2024.



2021 FRAUD CONTACT METHODS BY AGE AND SHARE OF LOSS REPORTS



Figures are based on fraud reports to the FTC's Consumer Sentinel Network that indicated a dollar loss, including reports provided by data contributors. Reports without age and contact method data are excluded from percentage calculations.

Elder Financial Exploitation

- Defined as an illegal or improper use of an older adult's funds, property, or assets; includes physical, emotional, or financial abuse.
- While EFE has state-specific statutes, an older adult is considered a person 60 years or older.
- Statutes may include individuals who do not have the capacity to act on their own, due to a disability, as part of the defined group.
- Combined losses reported by older adults who lost more than \$100,000 increased from \$55 million in 2020 to \$445 million in 2024.

FIN-2022-A022 Behavioral Red Flags

- Unusual changes in account contact information, such as updated emails or phone numbers.
- Customer with a known cognitive impairment has unusual account activity.
- Customer who seems fearful or submissive and unable to answer basic questions about account activity; one who seems to be taking direction from a third party, or one who is fearful or submissive to their caretaker.
- A caregiver or family member who shows excessive interest in the customer's assets, does not allow the customer to speak for themselves, and is reluctant to leave the customer's side.
- A customer who mentions an online friend or romantic partner and wants to send money to join them in a business venture.

FIN-2022-A022 Behavioral Red Flags

- A customer who is agitated or frenzied about the need to send money immediately to an “emergency” of a loved one, but the money is sent to an unconnected third party.
- A new caretaker, friend, or relative who suddenly begins conducting financial transactions on behalf of the older person without proper documentation (such as a POA).
- Your staff is unable to contact or speak directly to the customer.
- Dormant accounts with large balances begin to show constant WDs or CDs are closed without regard for penalties.
- A customer purchases large numbers of gift cards or inquires about buying cryptocurrency.
- Attempts to wire large sums of money or receives large wires (money mules).

Elder financial exploitation

- Elder scams
 - Scams involving the transfer of money to a stranger or imposter for a promised benefit or good that the older adult did not receive
 - **The scammers operate outside of the U.S. and contact their victims using a fake persona through robocalls, text messages, social media, or dating apps**
 - **To establish trust, they impersonate government officials, law enforcement agencies, technical and customer support representatives, social media connections, family, friends, and even well-known media personalities**
 - **Scammers request payments via wire transfers at MSBs, purchasing gift cards, money orders, and even Bitcoin**
 - **Victims may also be used as money mules, who transfer illicit funds scammed from other victims at the direction of the scammer**

Common Scams

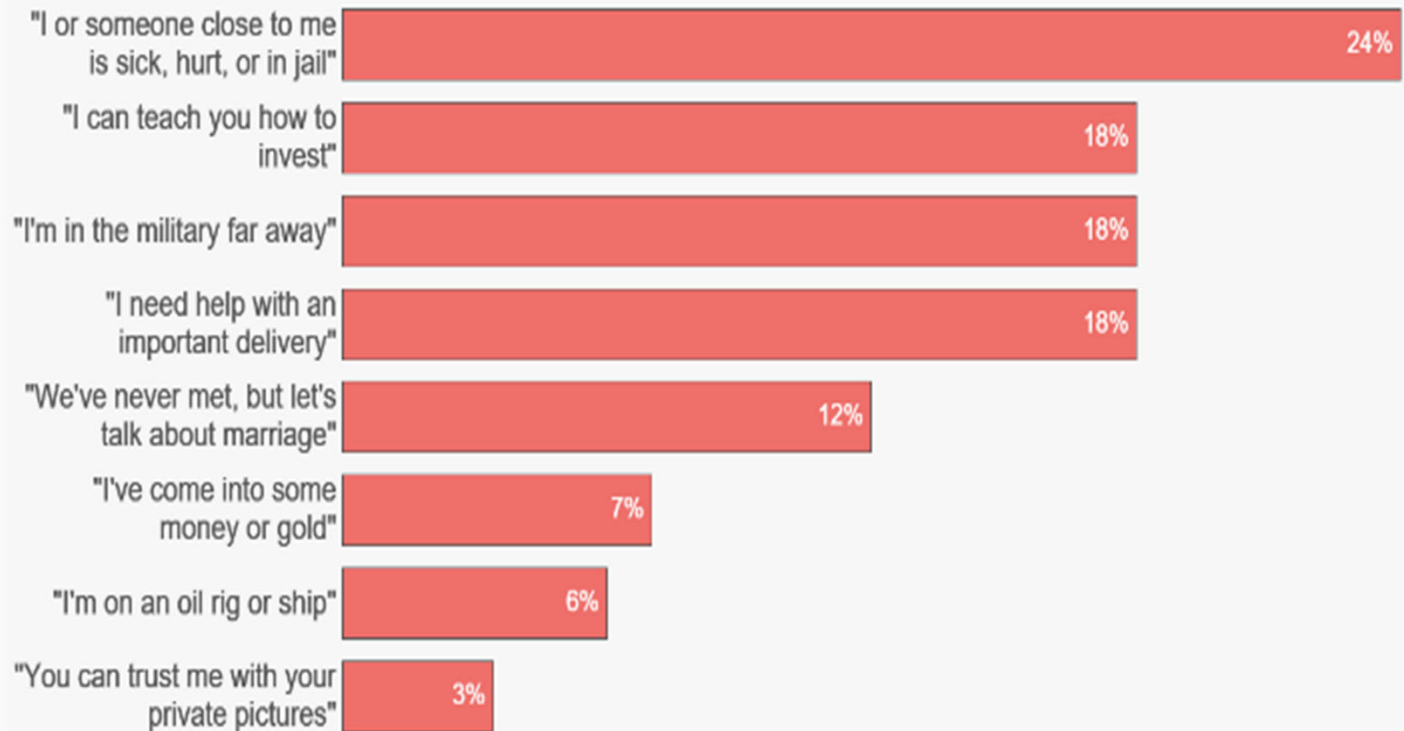
- Romance scam
 - Fraudsters pose as interested romantic partners through dating websites to capitalize on their elderly victims' desire to find companions.
- Tech support scam
 - Perpetrators pose as tech support representatives and offer to “fix” non-existent computer issues. They gain remote access to victims' devices, which includes sensitive information.
- Grandparent scam
 - Scammers pose as a relative (child or grandchild), claiming to be in immediate financial need.

Common Scams

- Government impersonation
 - Perpetrators pose as government employees (IRS) and threaten to arrest or prosecute victims unless they agree to provide funds or other payments.
- Sweepstakes/charity/lottery scams
 - Fraudsters claim to work for legitimate charitable organizations, or they claim their targets have won a foreign lottery or sweepstakes, where they can collect their winnings for a “fee”.
- Home repair
 - Scammers appear in person and charge homeowners in advance for home improvement services that they never provide.

Numbers by the LIES

Romance Scammers: Their Favorite Lies by the Numbers



Figures are based on 8,070 2022 romance scam reports that indicated a dollar loss and included a narrative of at least 2,000 characters in length. Lies were identified using keyword analysis of the narratives.

Imposter scams

- Imposter fraud
 - An imposter is a person who pretends to be someone else
 - Imposters may pretend to be someone you know:
 - **A family member**
 - **A friend**
 - **A person you feel like you know but have not met in person**
 - **A company you do business with – maybe your electric company**
 - **A company that can fix your computer**
 - **A company that gives out prizes**
 - **A charity that asks for donations**
 - Imposters might try to get you to pay them by asking you to buy a gift card or wire money



Imposter scams

- Examples

- They are calling (or email) from a tech support company about a problem on your computer. They ask you to pay for their services with a gift card.
- You owe money to the IRS or another government agency
- You just won a prize, but you have to pay fees to get the prize
- A friend is in trouble and needs your help
- You got a check for too much money, and you need to send back the extra
- Someone calls to say you inherited money, but first you have to wire money for the taxes
- You see an ad promising you a credit card. But first you have to wire money to pay to apply

Imposter scams

- How to identify and prevent imposter scams
 - Customers tell you they were solicited “out of the blue”
 - The transaction needs to be rushed; the customer insists on getting it done quickly
 - The customer may be afraid of the consequences if they don’t pay
 - Similar “stories” are found on internet searches that were deemed to be fraud
 - The customer needs additional account information to give to someone else, including passwords, PINs, or account history

Fake charity and donation scams

- Charity fraud schemes seek donations for organizations that do little or no work – instead, the money goes to the fake charity's creator
- Especially prevalent after high-profile disasters such as floods, cyclones, earthquakes, and bushfires
 - Preying on emotions, generosity, and human kindness
 - Fraud actors may combine with imposter scams to impersonate government authorities or disaster support associations
- Charity fraud can be in the form of emails, social media, crowdfunding, cold calls
- Fake websites that look similar to real charities (slightly changed web address)

Money mule scams

- Money mule scams on the rise!
 - Growth in transnational criminal organizations targeting consumers, businesses, government funds:
 - **Romance scams, lottery fraud, government imposter fraud, technical support fraud, person-in-need scams**
 - **Business email compromise/CEO fraud**
 - **Unemployment insurance fraud/PPP**
 - Begin as victims of scams, particularly romance fraud and lottery scams
 - Job posts on online boards, social media – promised easy money for little effort
 - Recruited by fraudsters to facilitate the scheme
- Money mules often receive a commission for their service, or they might provide assistance because they believe they have a trusting relationship

Top AI Scams (2025-2026)

- AI Voice Cloning (“Vishing”)
 - Scammers use as little as three seconds of audio, gathered from social media or voicemails. Used to clone a loved one’s voice to pretend they are in an emergency (arrested, kidnapped, in an accident) to demand immediate money.
- Deepfake Video Calls
 - Use of real-time AI to look and sound like a trusted person (CEO, manager, family member) during a video call to trick the victim into transferring funds or revealing personal information.
- AI-powered “Pig Butchering.”
 - AI-driven “experts” and chatbots used to build rapport over weeks/months.

Top AI Scams (2025-2026)

- Hyper-Personalized Phishing
 - AI allows scammers to bypass spam filters and write professional, flawless phishing emails and texts (smishing) that reference recent personal or professional activities, making them appear incredibly legitimate.
- Fake Job Recruitment & Deepfake Interviews
 - Fake job postings to steal data, or in some cases, use deepfake technology to conduct interviews, land remote IT jobs, and then use AI to perform the work while stealing data.
- AI-Enhanced Romance Scams
 - Scammers create “perfect match” fake profiles using AI-generated photos and voice notes to build emotional connections on dating apps before asking for money.

Top AI Scams (2025-2026)

- Fake “Live” Chatbots
 - Scammers set up AI-driven customer service bots that look like legitimate bank or company portals to steal login credentials or personal information.

Warning signs & Prevention Methods

Urgency & Emotion

- Scammers tend to always create a sense of panic or extreme urgency.

Verify independently

- If a “loved one” calls for money, hang up and call them back at a trusted number.

Family code words

- Create a secret phrase with family members.

Unusual payment methods

- Red flags if asked to pay via crypto, gift cards, or wire transfers.

The “Uncanny Valley”

- Look for strange inconsistencies; unnatural mouth movements or slight robotic tones.

Limit social footprint

- Watch the amount of voice and video content posted on social media. It can be used for cloning purposes.

Common Questions

- Can you refuse to honor a wire request if you feel the customer is a victim of a scam?
 - Yes!
- Can you close the account if the customer repeatedly tries to conduct transactions related to scams?
 - Yes!
- Who can you contact to report your concerns?
 - Law enforcement, FinCEN, Adult Protective Services, local elder abuse support organizations
- When should a SAR be filed?
 - SARs should be filed in accordance with general SAR filing guidelines. It's important to remember that activity is not REQUIRED to fall within SAR filing thresholds.

Common Questions

- What is the best way to detect and prevent EFE?
 - Keep your customers informed on current fraud trends and scams.
 - Automated Surveillance Monitoring (ASM) systems
 - Train your staff! Frontline staff (tellers, account-opening staff) are among your best resources.
 - **Train staff on how to identify potential red flags.**
 - **Ensure staff are aware of whom to report any potential red flags to (BSA and/or fraud departments, branch management, etc.)**

Stephanie Jennings, CRCM

Manager

Stephanie.jennings@wipfli.com

815 484 5631

wipfli.com

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable standards, Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.

WIPFLI

Wipfli LLP. All rights reserved.