Beware of the Rising Elder Financial Fraud Crisis

Every day, multinational criminal organizations are attacking Americans of all ages from many angles. No one is immune from this attack – if one approach doesn't work, they will try another, weaponizing human nature against us through fear, greed, or love to lower defenses. We are highlighting this rising risk for World Elder Abuse Awareness Day on June 15, 2026, because, unlike younger targets, older adults suffer more damage from these scams as they have more to lose and less time or ability to rebuild their hard-earned nest egg.

Financial fraud targeting adults over 60 has escalated into a national crisis with reported losses skyrocketing. According to the Federal Trade Commission (FTC), in 2024, older Americans reported losing a record $2.4 billion to scams, a fourfold increase since 2020. The FBI's Internet Crime Complaint Center (IC3) received over 200,000 complaints from this demographic in 2025, reflecting a staggering 37% jump in losses from 2024. Seniors lost the most of any age group – over $7.7 billion (a 59% increase from 2024), with the largest losses from investment scams accounting for $3.5 billion, and artificial intelligence (AI) related losses of $352 million.

Fraudsters increasingly target seniors because they often possess significant savings, home equity, and good credit. Social media has emerged as the most financially damaging contact method overall. In 2024, the North American Securities Administrators Association reported the top products and schemes involving senior victims were digital assets, romance investment scams, stocks and similar equities, social media fraud, and promissory notes.

Currently the most destructive, social media scams lure victims into fraudulent cryptocurrency platforms. Wisconsin seniors suffered over $26 million in cryptocurrency-related losses in 2024. An emerging tactic of scammers directs victims to deposit funds into cryptocurrency kiosks (also known as Bitcoin ATMs), which provide the near-instant, irreversible transfer of cash into cryptocurrency. The FBI reported $333 million in cryptocurrency kiosk scam losses in 2025.

Criminals are also leveraging generative AI for voice cloning and deepfakes. In modern "grandparent scams," AI can clone a grandchild's voice from a short audio sample to make a plea for emergency bail money appear authentic. Scammers also exploit trust by posing as government agencies (such as the IRS, FTC, or Medicare), tech support agents, or romantic interests. Tech support scams alone cost older Americans $159 million in 2024.

The good news is that regulators are leveraging technology to fight back against digital fraudsters, issuing alerts, shutting down scam websites, and partnering with blockchain and digital asset firms to trace and try to recover stolen funds. However, the best protection is always prevention. Proactive measures may include adding a trusted contact to investment accounts, establishing family code words to verify identities during urgent calls, and remaining alert to red flags of financial fraud, including the following warning signs:

- The first contact is an unsolicited text or through a social media platform (Instagram, LinkedIn, or dating applications);
- The scammer encourages moving to encrypted messaging services (WhatsApp, Telegram, or Signal);
- The scammer uses terms of endearment early in the relationship;
- The scammer encourages the victim to open a bank or cryptocurrency account;
- The scammer brags about their successful investments and offers coaching; and
- The scammer is never available to meet in person.

When facing pressure to turn over funds quickly, **pause, reflect, and protect** yourself by asking a trusted friend for their thoughts on the situation. If you have already sent money to the scammer, **report the scam** immediately.

In Wisconsin, a new law was recently passed that may help slow the extent of the losses. If a fraud victim uses a cryptocurrency kiosk, they should heed the posted warning, which is now required to be on the machine. There is now a $1,000 daily transaction limit on the machines, and consumers should avoid being convinced to try using multiple machines. If a consumer believes they have been scammed at a cryptocurrency kiosk, they need to report it to 1) the cryptocurrency kiosk operator and 2) a law enforcement agency (local law enforcement, the Wisconsin Department of Financial Institutions (DFI), or the Wisconsin Department of Justice) within 30 days of the transaction. The sooner the better because time is of the essence. Consumers who report the fraud to both the cryptocurrency kiosk operator and law enforcement within 30 days may be eligible to have lost funds refunded under the new law.

Reporting fraud also helps law enforcement detect patterns, build criminal cases, and protect others by helping agencies track emerging threats and issue public alerts. Survivors of financial scams should report the scam to the DFI's Division of Securities by calling (608) 266-2139 or emailing: DFIDLSecuritiesEnforcement@dfi.wisconsin.gov. The DFI can assist in gathering relevant information, tracing the cryptocurrency, and reporting it to law enforcement. Once a scam is reported to local law enforcement a case number is assigned. Financial scam victims should also file a complaint with the FBI's IC3, the FTC, and the Secret Service by emailing: CryptoFraud@SecretService.gov.

For more information, visit the Report Elder Abuse in Wisconsin website or call (833) 586-0107. Also, be sure to review the DFI's Avoiding Fraud Against Seniors webpage and the DFI's Investment Scam Tracker webpage to stay updated on the latest reported scams.