



INFORMATIONAL MESSAGE

UNCLASSIFIED

Preventing Financial Scams among Connecticut Seniors

The Connecticut Intelligence Center, a law enforcement partnership within the Connecticut Department of Emergency Services and Public Protection, is warning about a dramatic increase in financial scams targeting the elderly in Connecticut and the nation. The FBI's Internet Crime Complaint Center (IC3) received 859,532 complaints in 2024, with **losses reported at \$16.6 billion**, a 388% increase from 2023. In 2024 "false pretense" scams cost an estimated **\$31.9 million** to Connecticut victims, most of whom were 65 or older, according to the 2024 Crime in Connecticut Report.

Elder Fraud Scammers: Common Tactics and Techniques



Lottery and sweepstakes scam: You are told you have won a large prize but must pay a fee or taxes upfront to claim it. Legitimate lotteries do not require you to pay before you receive your winnings.

Grandparent scam: A caller, sometimes using AI to mimic a voice, claims to be a grandchild or other relative in an emergency and asks for immediate money. They often plead for secrecy, adding to the urgency.



Home repair scam: Involve unsolicited contractors who use high-pressure tactics to gain access to a home for unnecessary and shoddy work. Be wary of solicitations, never pay a large upfront amount, and always get multiple written estimates from licensed and insured contractors

What to watch out for

- High pressure, urgent timeline ("you must send money now").
- Request to pay with gift cards, wire transfer, prepaid cards, personal checks or cryptocurrency.
- Caller says you must not contact family or police.
- Caller ID spoofing (it may show a local number or government agency but is fake).
- Unwilling to meet in person or hesitation to identify themselves with official credentials.



What to do if you believe you are a victim

- Contact the local police to report the incident.
- Do not transfer money and do not give any payment information.
- Do not give any personal information or confirm/repeat social security numbers, birthdates, bank information or account numbers.
- Verify by calling the family member with a known number not one provided by the caller.
- If you have already made a payment contact your bank or the payment service immediately.

Where to go for help

- National Elder Fraud Hot Line- 1-833-372-8311
- Elder Fraud- Internet Crime Complaint Center (IC3) www.ic3.gov/Crimeinfo/ElderFraud
- Federal Trade Commission (FTC) <https://reportfraud.ftc.gov>
- File a Suspicious Activity Report with CTIC https://portal.ct.gov/demhs/homeland-security/suspicious-activity-reporting-form?language=en_US or download the “CT SAFE” application on your phone.

How Family Members and Caregivers Can Help

Warning signs of financial exploitation	Proactive Measures to Take
Sudden changes in bank accounts or banking practices, an unexplained withdrawal of large sums	Use direct deposit for regular income and set up automatic payments for bills to create a clear transaction record and minimize risk
The inclusion of additional names on an older adult’s bank signature card	Thoroughly check the references and credentials of any new caregiver/financial advisor before granting them access to personal information or finances
Unauthorized withdrawal of the older adult’s funds using their ATM card	Review activity in accounts. Set up alerts for large withdrawals or unusual activity
Provision of substandard care or bills left unpaid despite the availability of adequate financial resources	Consolidate accounts, close unused credit cards, and opt out of credit card solicitations
Discovery of a forged signature for financial transactions or for the titles of the older adult’s possessions	Use strong and unique passwords with a combination of numbers, letters and symbols
Sudden appearance of previously uninvolved relatives claiming their rights to an older adult’s property or possessions	Establish a durable power of attorney (POA) to appoint a trusted person to manage finances if needed
Unexplained sudden transfer of assets to a family member or someone outside the family	Use strong and unique passwords with a combination of numbers, letters and symbols
The provision of services that are not necessary, contactors asking for large sums of money upfront	Be wary of solicitation, estimates that seem unusually low, and ensure contractors are licensed and insured

Sources: FBI Internet Crime Complaint Center, Internet Crime Report, 2024; DESPP Crime Analysis Unit, Crime in Connecticut, 2024; AARP Fraud Scams-Fraud Helpline.