

FINANCIAL ABUSE & FRAUD

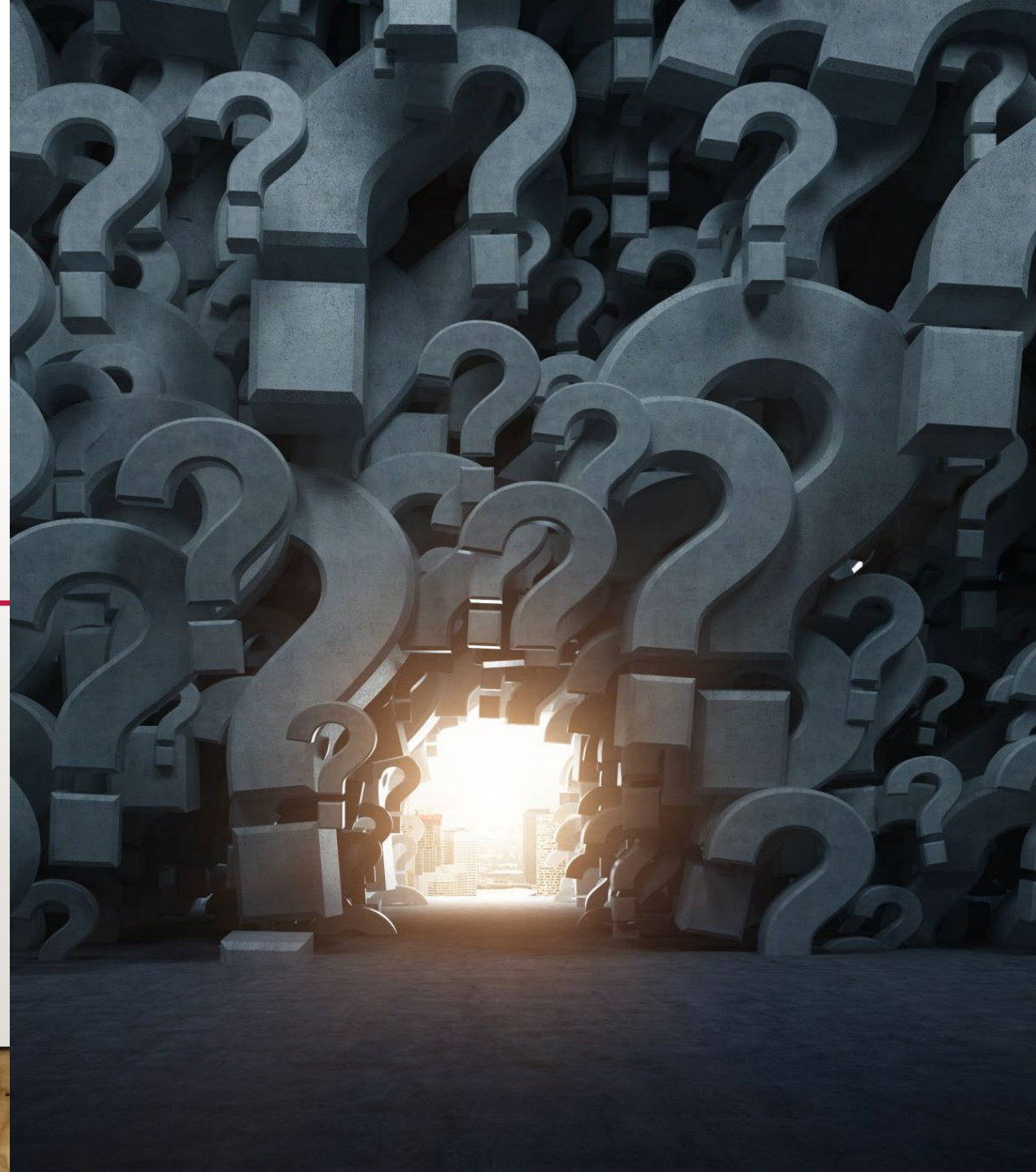
PRESENTED BY:

CINDY FLEITZ, BSA/COMPLIANCE OFFICER

JANAY CORDREY, BSA/COMPLIANCE SUPPORT SPECIALIST

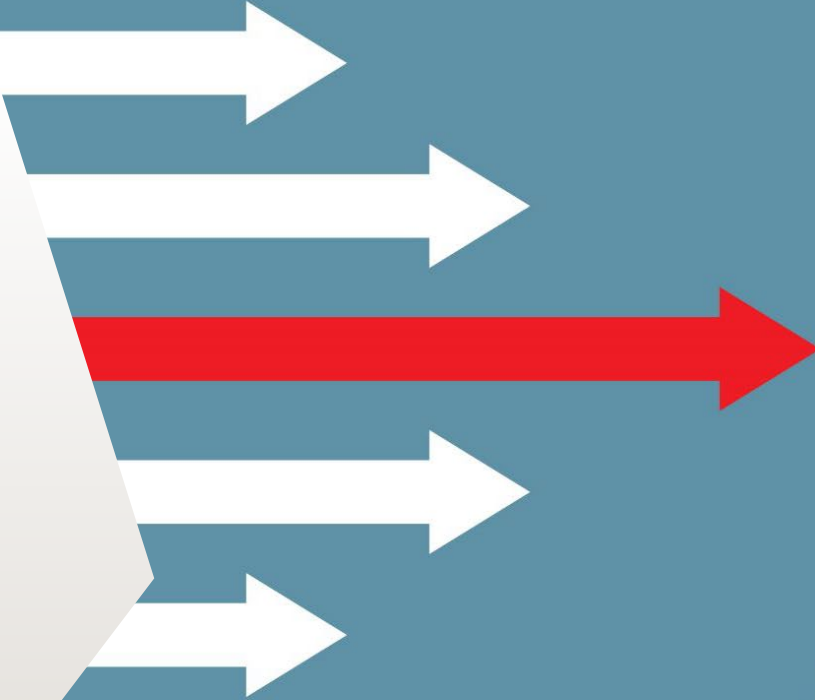
DENISE CICERO, DIRECTOR OF PAYMENT STRATEGIES

TAMMI FARMER, BRANCH MANAGER



OBJECTIVES

- Understand the different types of fraud
- Tips on how to protect yourself
- Different types of scams and what to look for
- Planning for the unexpected



TYPES OF FRAUD

Online account takeover

P2P Debit schemes

Spoofed caller ID

Fraudulent wires

Fake bank accounts

Fraud checks

Fraud Loans

Contractor/Home Improvement

Elder Financial Exploitation

- Romance Scams
- Investment Fraud
- Grandparent scams
- IRS Telephone scams
- Lottery & Sweepstakes Scams
- Phantom Debt collections Scam
- Signs of Charity Scam
- Identity Theft
- Medical Identity Theft
- Reverse Mortgages

ONLINE ACCOUNT TAKEOVER

Occurs when cybercriminals gain access to your accounts and use them to withdraw money, making purchases or extract information they can sell or use to access other accounts.

Potential targets include social media and email accounts, as well as those you use to shop or handle bank and credit transactions.



RED FLAGS

- Shut down online access to any accounts that show any visible signs of fraud
- Change username, password, security questions, and verify email and personal information
- Review your account for sudden online usage or enrollment
- Review your account for any file maintenance
 - Do these changes make sense?

-
- Fraudsters use malware to steal logins or automatically hack into accounts and transfer funds out.
 - Pretend to be fake support by using phishing messages or send fake receipts stating funds were sent to a persons account in error and asking for returns.



THINGS TO REMEMBER



Be skeptical



Double check with sender



Beware of texts and phone calls



Use enhanced authentication



Improve mobile security, with questions and multi-authentication tools

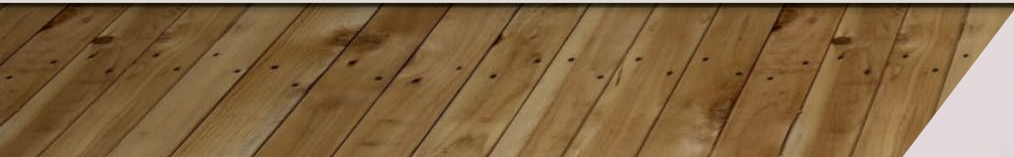


SPOOFED CALLER ID

- Most common is to fake phone numbers with voice over internet protocol (VoIP), in which they create an account that allows them to substitute their original number with any number they want. This means the scammer can target any phone number in their database.
- Some scammers will change the display name and caller ID so they can use almost anyone's phone number and name without the threat of call backs.

HELPFUL TIPS

- Don't pick up calls from unknown numbers.
- Install a spam blocker app
- Change phone numbers
- Don't be afraid to hang, look up, and call back



FRAUDULENT WIRES

- The act of fraud or attempt to commit fraud with the aid of some form of electronic communication (telephone or computer) and/or communication facility
 - Means of communication used distinguishes wire fraud from mail fraud.
- If you think you might be involved in a scam, stop the payment transaction and stop communicating with the person
- Ways we can help to stop this
 - We require a large amount to be completed in person
 - We verify all information on the account and ensure no recent changes have been made

FAKE BANK ACCOUNTS

- New account fraud occurs when a fraudster or money mule has successfully opened an account at a financial institution using their own identity, a stolen, or synthetic identity.
 - This means they have successfully enrolled for authentication, so the account appears legitimate
- These accounts will then be used to perform fraudulent transactions
- Mitigation steps
 - File a police report
 - Contact your credit union or bank right away
 - Pull a copy of your credit report from all three bureaus
 - Enroll in an identity theft solution
 - File any necessary disputes with bureaus, as well as place a credit freeze or fraud block with all.

FRAUD CHECKS



Using paper or digital checks to obtain money illegally. Includes:

- Someone writing fraud checks on their own
- Forging a check in someone else's' name
- Drafting a completely fake check
- Someone can steal your actual check or reproduces them and is able to cash, pulling funds right from your account.
- Forgery, illegally printing checks, and even thieves using chemicals to alter checks are all examples of fraud checks.

If you are a victim, Contact your creditors immediately and follow up/keep an eye on your statements

FRAUD LOANS



- Many lending agencies require small amounts of information in their lending application process, making it easy for identity thieves to use your stolen information to get a quick loan.
- With enough stolen details, fraudsters can open a legitimate car, home or business loan
- If you are a victim
 - Gather your documents to present to authorities
 - Contact local law enforcement
 - Place fraud alert with all three credit bureaus
 - Enroll in an identity theft solution
 - Talk with family and friends to keep others informed

TYPES OF LOAN SCHEMES

Fraud wire instructions-

- **Mainly for real estate closings.**
- **Fraudsters will search for upcoming closings, send fake emails to the credit union or purchaser with “updated wire instructions”**
- **Emails will look similar to legitimate emails**

Identity theft/Synthetic Fraud

- **Fraudsters take stolen information- anything from social security number to name and address to banking information- to obtain a loan**

Loan Stacking

- **Opening lending is a preferred channel**
- **Auto-decisioning result in faster processing**
- **Uses window of opportunity between loan approval and funding to apply for loans**

Predatory loan applications

- **These usually advertise attractive offers, even zero percent rates for a limited time with no due diligence check**





ELDER FINANCIAL EXPLOITATION WHAT IS IT?

- Fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual that uses the resources of an older person for personal benefit, profit or gain
- Actions that result in depriving an older person of rightful access to, or use of benefits, resources, belongings or assets
- Anyone can be a victim of Financial Exploitation. Elder financial exploitation crosses all social, educational, and economic boundaries

ELDER EXPLOITATION

WHY ARE OLDER ADULTS AT RISK?

- Have regular income and accumulated assets
- Be trusting and polite
- Be lonely and socially isolated
- Be vulnerable due to grief from a loss
- Be reluctant to report exploitation by a family member, caregiver, or someone they depend on
- Be dependent on support from a family member or caregiver to remain independent
- Be receiving care from a person with financial or other issues
- Fear of retaliation by the exploiter
- May be unfamiliar with managing financial matters
- Can be dependent on a family member or other person who may pressure them for money



EXAMPLES OF FINANCIAL EXPLOITATION

- By an agent under a Power of Attorney or person in another fiduciary relationship
- Investment fraud and scams Theft of money or property by family members, caregivers, or in home helpers
- Lottery and sweepstakes scams
- Grandparent/imposter scam
- Romance or charity scams
- Telemarketer, mail offer of salesperson scams
- Telephone, computer and internet scams
- Identity theft
- Reverse mortgage funding
- Contractor fraud and home improvement scams

WHO ARE ABUSERS OF FINANCIAL EXPLOITATION?

Family members and caregivers

Friends, neighbors, and acquaintances

Agents under power of attorney

Financial advisers

Telephone and mail scammers

Internet scammers

Home repair contractors

Medicare scammers

Romance scammers

WHY DON'T OLDER ADULTS REPORT EXPLOITATION?

Shame and embarrassment

Loyalty to family member or caregiver

Fear of retaliation or not being believed

Dependance on the abuser

Denial

Self-blame

Lack of awareness

ROMANCE SCAMS

- When a new love interest says they love you, but they just want your money
- To do this, they may;
 - Assume a false identity
 - Take time to build your trust
 - Ask for money under false pretenses
 - Can be online or in person
 - Claim they need money for emergency surgery or medical bills
 - Ask for help in paying unexpected customs fees or gambling debts
 - Request money for travel expenses so they can visit you
 - Ask for gift cards and wire transfers
 - Contact you through social media, dating apps, websites, text messages, or email

ROMANCE SCAMS WARNING SIGNS

- Overly complimentary and flirtatious
- Shower you with attention
- Want you to keep your relationship secret
- Show unusual interest in your finances
- Try hard to get you to share financial information

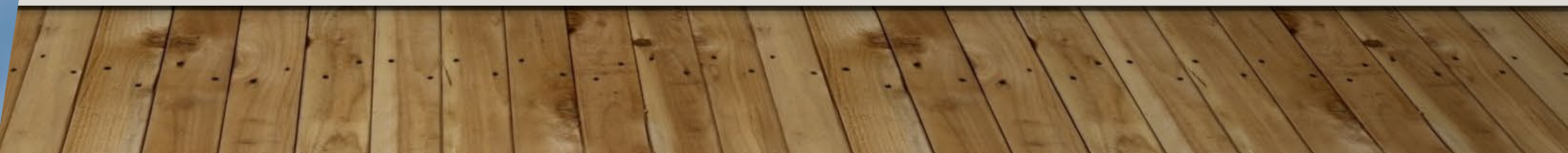
INVESTMENT FRAUD TYPES

- Misleading senior certifications/designations
- Ponzi schemes
- Unscrupulous financial advisers
- Affinity fraud
- Internet fraud- aka “dot-con”
- Inappropriate or fraudulent annuities





POINTERS FOR INVESTING

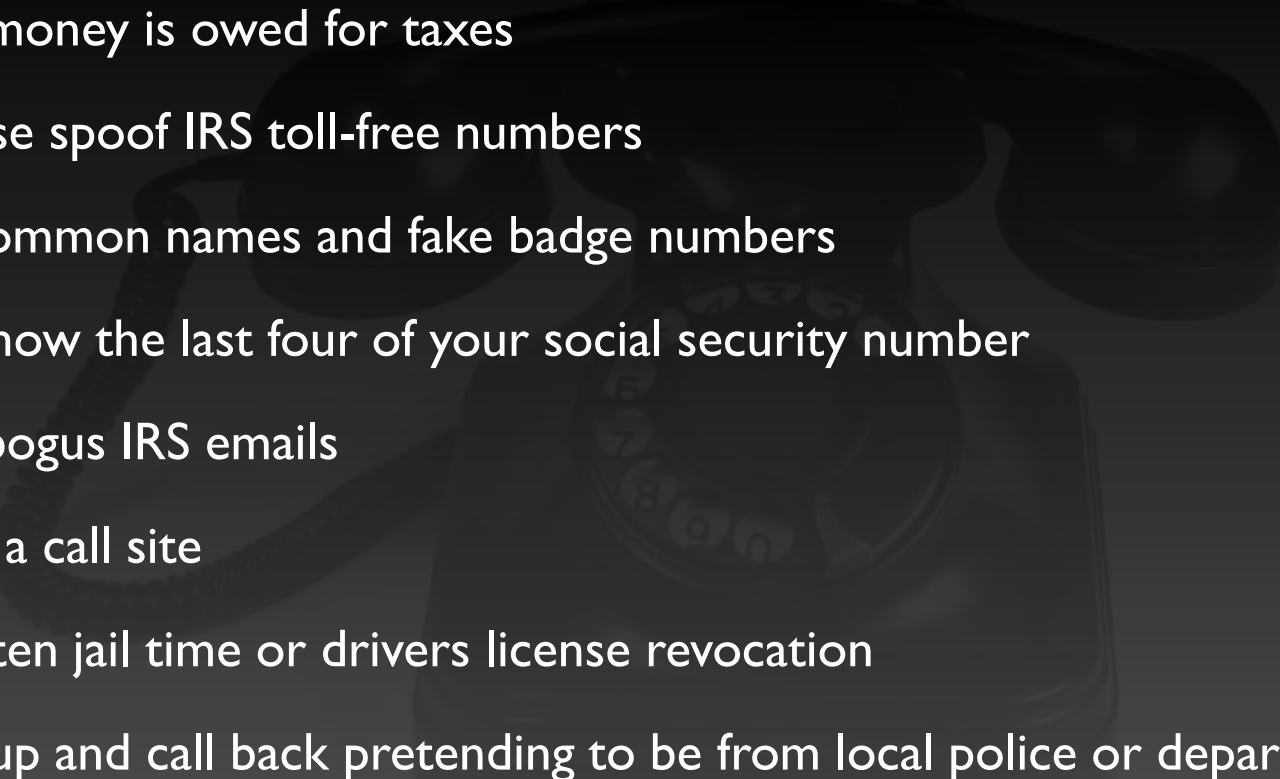
- Save enough to cover six months of living expenses before you invest
 - Do not make any investments unless you understand them fully
 - Become better informed
 - Be wary of marketing tactics like a free lunch seminar
 - Understand the risks before investing
 - Tell your financial advisor of your financial objectives and risk tolerance
- 



GRANDPARENTS SCAM

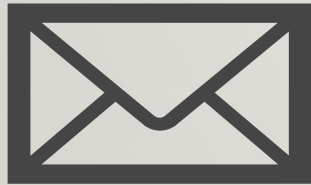
- Person claiming to be grandchild calls stating they are in trouble and need funds immediately.
- Scammer typically know the grandchild's name, usually cry to disguise voice and place for victim to wire them money.
- While doing this, they request for them to not tell other family members

IRS TELEPHONE SCAM

- State money is owed for taxes
 - May use spoof IRS toll-free numbers
 - Use common names and fake badge numbers
 - May know the last four of your social security number
 - Send bogus IRS emails
 - Mimic a call site
 - Threaten jail time or drivers license revocation
 - Hang up and call back pretending to be from local police or department of motor vehicles
- 

IRS TELEPHONE SCAMS

THINGS TO REMEMBER



The IRS **ALWAYS** send a written notification by the United States mail



The IRS **NEVER** asks for payment or credit card information over the phone



The IRS **NEVER** requests personal or financial information via email

PHANTOM DEBT COLLECTION SCAMS

Tricks victims into paying debt that doesn't exist

Contacts victims via phone

Refuse to answer any questions

Have information about victims

Use threat and scare tactics

Pose as law enforcement agent or government employees

Refuse to give you a mailing address or phone number

Ask for personal information

Ask you to buy a prepaid debit card and send them the card

SAFEGUARDS FOR DEBT SCAMS



Ask their name, telephone number and address



If you don't recognize the debt, ask for more information in writing



You have the right to get a breakdown of the amount owed



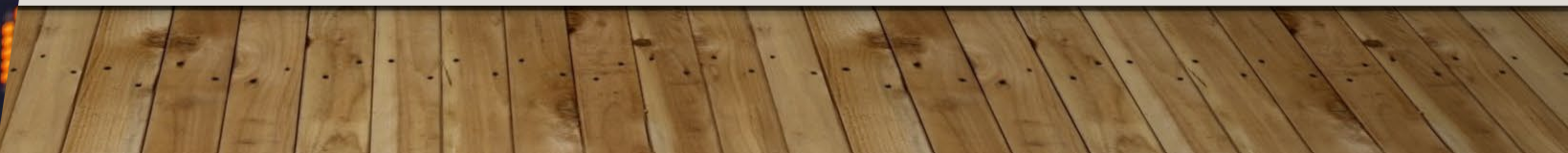
Don't give any financial or sensitive information



Keep copies of related papers

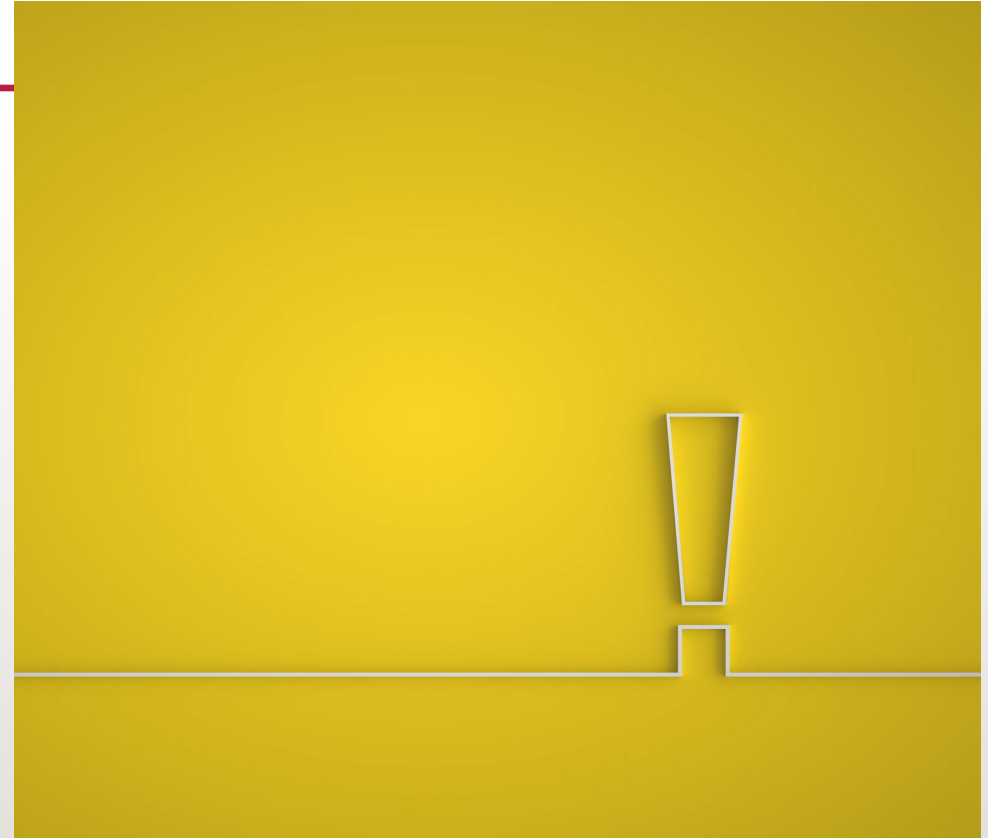


LOTTERY & SWEEPSTAKES SCAMS

- Call, email or text regarding lotteries, drawings or sweepstakes
 - Request upfront processing fees or taxes
 - Send authentic-looking claims checks
 - They may also pose as an attorney for winners
- 

TIPS FOR LOTTERY SCAMS

- You cannot win a contest unless you enter
- Never “pay to play”
- Be suspicious of pressure to wire funds
- Pay attention to warning from your Financial Institution
- If the caller claims an emergency, check it out as a number that you know to be valid
- Be wary of requests for secrecy



CHARITY SCAMS

WHAT ARE THE SIGNS?

- Refuse to provide information
- Won't provide proof that a contribution is tax deductible
- Mimic name from another organization
- That you for a pledge that you don't remember making
- Pressure victims to donate immediately
- Ask victims to donate cash or wire money
- Request private account information and routing numbers
- Guarantee sweepstakes winnings in exchange for a contribution



HOW TO PROTECT YOURSELF FROM CHARITY SCAMS

- Ask for information such as name and address
- Do your research using the organization's name, never donate until you do!
- Check if the charity is trustworthy
- Ask the name of the charity and the percentage of donations that goes directly to cause
- Contact the charity directly about solicitation
- Keep records of your donations
- Make annual donation plans
- Learn if the organization is eligible for deductible contributions
- Pay by check or credit card
- Never send cash or wire money
- Be wary of charities that spring up suddenly in response to current events/disasters

Thieves steal your personal financial information and use your identity to commit fraud and other crimes

Information thieves use:

- Social security number
- Birth date
- Credit card and account numbers
- PINs and passwords





PROTECTING YOURSELF FROM IDENTITY THEFT

- Protect your personal information
- Protect incoming and outgoing mail
- Sign up for direct deposit
- Use a shredder to destroy 'financial trash'
- Monitor bank accounts and credit card bills
- Avoid come-ons for personal information
- Review your credit report annually and report fraudulent activity if you see it
- If you are a victim;
 - Place initial fraud alert with one of the major credit reporting companies
 - Request copies of your credit report
 - Make an identity theft report
 - Consider placing a security freeze on your credit report
 - Contact Federal Trade Commission: Call 1-877-IDTHEFT (438-4338) or [identitytheft.gov](https://www.identitytheft.gov)

MEDICAL IDENTITY THEFT

- When someone steals your personal information and uses it for services, then bills Medicare for:
 - Medical treatment
 - Prescriptions drugs
 - Surgery or other services
- Risks include
 - Medicare may deny coverage for a service or equipment
 - It can affect your medical and insurance records- can change your blood type or record a diagnosis for disease you don't have
 - You could receive wrong, perhaps harmful, treatment
 - It is costly to correct



MEDICAL IDENTITY THEFT WARNING SIGNS & SAFEGUARDS

- Warning signs include;
 - A bill for services you did not receive
 - Contact from a collection agency for money you do not owe
 - Notification from insurance company that you have reached your limit for medical benefits
 - Denial of insurance for a medical condition you do not have
- Safeguards
 - Protect your Medicare and insurance cards
 - Review Medicare summary notices, explanation of benefits statements, and medical bills
 - Be careful about sharing personal information
 - Beware of offers for free equipment, services or goods in exchange for your Medicare number
 - Shred papers with your medical identity and destroy prescription labels before throwing bottles in the trash





REVERSE MORTGAGES

WHAT ARE THEY?

Allows homeowners 62 and older to borrow against their equity in their homes.

Monthly interest charges are added to loan amount

Available lines of credit, in regular installments, or as a lump sum

Repayable when you no longer live in the home

Must maintain the home and pay property taxes and insurance



REVERSE MORTGAGE SCAMS

- Family member or others pressure homeowner to get a reverse mortgage so they can “borrow” the money
- Scammers require borrower to sign power of attorney or otherwise sign over proceeds
- Broker pressure borrowers to purchase other financial products
- Scammers may promise that you can stay in your home or ask for a lot of money to help you
- Scammers might promise guaranteed or immediate relief from foreclosure and might charge you very high fees for few or no services

CONTRACTOR/HOME IMPROVEMENT FRAUD

- Scam artists use high pressure tactics to sell unneeded and overpriced contracts for “home improvement”
- Promises for quick work at below market prices
- Deliver substandard, unnecessary, or damaging work
- Pressures to pay through threat or intimidation
- May pose as a government official and demand a fee



TIPS TO AVOID CONTRACTOR FRAUD

- Verify the ID of anyone claiming to be a government employee
- Obtain written bids from your local contractors
- Avoid contractors who approach you
- Check for licenses and complaints
- Check references
- Require a clearly written contract
- Don't pay in advance; never pay cash
- Don't provide personal financial information
- If you need a loan, don't let the contractor steer you to a lender
- Withhold final payment until you are satisfied, and all required inspections are complete

PLANNING FOR THE UNEXPECTED

- Preparing for future health problems or disasters:
 - Gives you control
 - Relieves the stress of decision-making from caretakers and family members
 - Saves money and helps avoid financial setbacks
 - Allows time to gather information and compare options
- Prepare a plan; Review income and expenses
- Make sure a trusted family member knows where to find necessary documents
- Set up trusted family members know where to find necessary documents
- Set up direct deposit or income and benefit checks
- Consider automatic payments of important, recurring bills
- Consider a durable power of attorney
- Make sure you are properly insured
- Maintain a healthy lifestyle

WHAT WILL YOU NEED?

- Driver's license or government-issued ID
- Insurance cards
- Social security card
- Passport
- Birth Certificate
- Cash
- ATM, debit, and credit cards
- Checkbook (blank checks and deposit slips to last a month)
 - Sign up for internet banking services
 - Review your insurance coverage
- Phone numbers for financial service providers
- Important account numbers
- Key to safe deposit box
- What else to consider
 - Prepare emergency evacuation bags
 - Arrange for automatic bill payments from bank accounts



PROTECTING YOUR DOCUMENTS



- Make backup copies of important documents
- Make an electronic image for easy storage
- Give a copy to loved ones or tell them where to find documents in an emergency
- Store backups at a distance from home in case of disaster affected entire community
- Make a record of all credit/debit cards with account and contact numbers to report lost/stolen
- What to keep; where to keep it
 - Safe deposit box; include birth certificate and original of important contracts
 - Fireproof safe; include passport, medical care directives, and will

QUESTIONS?

