AARP FRAUD WATCH NETWORK

WATCHDOG ALERT HANDBOOK

13 Ways Con Artists Steal Your Money

AARP Fraud Watch Network

aarp.org/fraudwatchnetwork

Watchdog Alerts / Tips & Resources / Free for Everyone

WATCHDOG ALERT HANDBOOK: 13 WAYS CON ARTISTS CAN STEAL YOUR MONEY

Identity theft, investment fraud and scams rob millions of Americans of their hard-earned money. Last year, 16.7 million people from communities across the nation lost nearly $17 billion to identity fraud alone according to the Federal Trade Commission (FTC).

The AARP Fraud Watch Network is working to empower you in the fight against fraud. It puts proven tools and resources at your fingertips:

- Scam alerts, delivered right to your inbox;
- A scam-tracking map, where you can report scams and learn about scams from other fraud fighters around the country and in your area;
- A free helpline at 1-877-908-3360 where you can speak with volunteers trained in fraud counseling

AARP: A HISTORY OF SAFEGUARDING AMERICANS' FINANCIAL SECURITY

AARP began more than 60 years ago when its founder, Dr. Ethel Percy Andrus, discovered a retired teacher living in a chicken coop. She was appalled that a woman who worked her whole life couldn't even afford a place to live. She started AARP to protect the financial security of older Americans. Fighting identity theft and fraud is part of that core mission.

IDENTITY THEFT

Identify theft occurs when someone steals personal information that could be used to falsely apply for credit or for government benefits. Here are three common ways con artists steal your identity.

1. PHISHING

Someone contacts you via email and says there is some problem with your bank account and you need to verify the account with a Social Security Number, bank routing number or birth date.

2. STEALING MAIL OR SENSITIVE DOCUMENTS

Personal information is taken from your trash, your office or from social media websites and used to steal your identity.

3. BOGUS JOB OPPORTUNITIES

Con artists post bogus job offers on various employment websites. The scammer may use or sell your personal information provided in the job application.

Protect yourself from identity theft, investment fraud, and other common scams. When it comes to fraud, vigilance is our number one weapon!

INVESTMENT FRAUD

4. GOLD COIN SCAM

You hear an ad on the radio that describes how the world economy is shaky and the only thing you can really rely on during periods of economic uncertainty is precious metals. You call a toll-free number and are pitched on buying gold and silver coins that will undoubtedly go up significantly in value. What you are not told is that the coins are being sold at a 300-500% mark up and you will lose money the minute you buy them.

5. FREE LUNCH

The scammer invites a hundred people to a seminar, where he or she presents an unbeatable investment opportunity. You must sign up right then and there. You can't sign up later because he or she is leaving town in two hours, and if you don't take advantage before they leave, you will lose all chances of cashing in on the opportunity. It's all about getting you to commit quickly without taking the time to think about whether it sounds like a scam.

6. OIL AND GAS SCAMS

Someone calls and tells you they are drilling for oil off the Gulf Coast or in Mississippi, and they have this great new technology that allows them to find oil where no one else has ever been able to drill. But they don't tell you if they are a registered broker or if the investment is registered with the state or the SEC. And they don't tell you that even legitimate energy investments almost always bear a high degree of risk, which could result in you striking out while trying to strike it rich.

OTHER COMMON SCAMS

7. FAKE CHECKS

You get a call saying you won a major prize, and you won't even be responsible for the processing fee, They will offer to pay you more than the cost of the processing fee with a cashier's check, then ask you to pay a portion of it back as a handling fee. The cashier's check appears to clear the bank, but is eventually determined to be no good, leaving you without your merchandise and having paid a fee.

8. TECH SUPPORT SCAMS

You get a call or a popup warning that your computer has a virus. You are then told to hand over remote access to your computer to fix it. Afraid of the consequences of inaction, you allow the con to take remote control of your computer and they actually install a virus and charge you to remove it, or they will convince you to purchase a worthless computer maintenance program.

9. DISASTER-RELATED CHARITY FRAUD

Every time there is a major natural disaster somewhere in the country, scammers come out of the woodwork sending emails, making phone calls, and setting up fake charity websites to raise money for the victims of the disaster. You think the money is going to help victims, but it is really going to line the pockets of a criminal.

10. SWEETHEART SCAMS

You go onto a dating website in hopes of meeting that special someone. You meet a person who quickly expresses an interest in you. But they can never meet (claiming to be always traveling), and always find excuses not to call, limiting their contact to things like instant messaging or email. Unfortunately, it is really a con artist who builds an emotional bond with you and then starts asking you for money.

11. TIMESHARE SCAMS

You are trying to sell your timeshare property. You are called by someone claiming to represent a company that helps owners sell their properties. They may even say you have a specific buyer already lined up. They tell you that all you need to do is pay an upfront fee to cover various costs. They even provide you with official-looking paperwork. Then, after you pay that upfront fee, they disappear.

12. THE GRANDPARENT SCAM

A young person calls you pretending to be your grandson or granddaughter. They tell you they have been arrested for drunken driving or they are being detained for some other reason and they need you to wire them $3,000 or $1,700 or some other amount to get them out of trouble. They may have gotten your grandson's name from social media or they may have just waited for you to say, "Is this Joey?" and then they continue the ruse.

13. THE FOREIGN LOTTERY SCAM

You receive a letter or a phone call saying you may have won a foreign lottery. All you have to do to collect your winnings is to wire money to the caller for taxes or a "processing fee." The fact is that foreign lotteries are illegal and if you have never entered a lottery, it's impossible to win.

NEVER GIVE PERSONAL INFORMATION TO TELEMARKETERS WHO CALL YOU ON THE PHONE.

PREVENTION TIPS

PROTECT YOUR SOCIAL SECURITY NUMBER (SSN) & PERSONAL INFORMATION

- Don't carry your Social Security card in your wallet.
- Don't print your SSN or driver's license number on your checks.
- Medicare recently rolled out cards that no longer contain your Social Security number. Beware of calls purportedly from Medicare asking you to verify your Social Security number over the phone.
- Shred sensitive information.
- Limit the number of credit cards you carry.
- Keep copies of credit cards (front and back) in a safe place in case a card is lost or stolen.

MONITOR YOUR BILLS & FINANCIAL ACCOUNTS

- Watch for missing bills and review your monthly statements carefully. Contact your creditors if a bill doesn't arrive when expected or includes charges you don't recognize. Most banks and credit card companies offer electronic access to your account, which can help with regular monitoring. Its important to sign up for that access, and keep your login and password information secure.
- Don't invest in anything you are not absolutely sure about. Do your homework on the investment, the company, and the salesperson to ensure that they are legitimate. You can look them up at **finra.org/BrokerCheck and sec.gov**.

WATCH OVER YOUR CREDIT REPORTS

- You are entitled to one free credit report each year from each nationwide credit bureau. To get your free report, go to **annualcreditreport.com** or call **1-877-322-8228**.

PROTECT PERSONAL IDENTIFICATION NUMBERS (PINs) & PASSWORDS

- Don't carry your PINs and passwords in your wallet or purse.
- Avoid using easily available information for your PINs or passwords such as your mother's maiden name, your or a family member's birth date, your SSN or phone number, or a series of consecutive numbers (i.e., 1, 2, 3, 4).
- Choose a different PIN for each account. Consider using a password manager, which is a free program (Do an online search for "password manager") to help keep track of them.

PROTECT YOUR INFORMATION ONLINE

- Beware of emails that claim to come from a bank, Internet Service Provider, business or charity that asks you to confirm your personal information or account number. If you receive one that is suspicious, forward the email to the Federal Trade Commission at **spam@uce.gov**.
- Avoid conducting personal or financial business on shared/public computers or over public wireless hotspots. And if you find you use public Wi-Fi regularly, play it safe and sign up for a Virtual Private Network (VPN) that keeps your data secure by routing your communications through a secure, third-party server.
- Install the latest version of established anti-virus software.
- Make sure websites are secure, especially when shopping online. A secure website will begin with "https".

PROTECT YOUR MAIL

- Call **1-888-5-OPT-OUT** or visit **optoutprescreen.com** to stop pre-approved credit card applications that a thief could steal and use to get credit in your name.
- Place outgoing mail into a locked mailbox such as a blue postal service box.
- Don't leave incoming mail sitting in an unlocked mailbox.
- Cut down on junk mail by contacting the Direct Marketing Association at **dmachoice.org**.

BE CAUTIOUS OF SCAMS & FRAUDS

- Never give personal information to telemarketers who call you on the phone. To cut down on unwanted telemarketing calls, sign up for the Do Not Call Registry at **donotcall.gov** or call **1-888-382-1222**.
- Double-check references for door-to-door sales, home repair offers and other products. Verify that businesses and others who contact you are who they claim to be before you provide any personal information. If you think the request for information is legitimate, contact the company at a number you know is valid to verify the request.
- Check out a charity before donating to make sure they are legitimate at **give.org** or **charitynavigator.org**.

RESOURCES

AARP Fraud Watch Network

AARP Fraud Watch Network provides you with access to information about identity theft, investment fraud and the latest scams. Access online at: **AARP.org/fraudwatchnetwork**.

AARP Fraud Watch Network Helpline

Highly trained AARP Foundation volunteers are available to answer questions and offer peer counseling, support and referral services to fraud victims and their family members. Call toll free: **1-877-908-3360**.

The National Association of Attorneys General

The National Association of Attorneys General (NAAG) site provides contact information for all state attorneys general. Most state attorneys general welcome consumer inquiries and complaints about frauds occurring in the marketplace and many offer complaint mediation services as well. Access online at: **NAAG.org**.

FINRA Investor Education Foundation

This site, operated by the FINRA Investor Education Foundation, provides critical information about how to avoid investment fraud, including allowing you to check to see if a broker or a particular investment advisor is registered. It is particularly helpful in addressing a variety of investment frauds such as gold coins and oil and gas scams. Access online at: **saveandinvest.org**.

The North American Securities Administrators Association (NASAA)

This website is where you can find your local state securities regulator, who takes complaints against brokers and dealers that may have engaged in investment fraud. Access online at: **NASAA.org**.

U.S. Postal Inspection Service

This site, sponsored by the U.S. Postal Inspection Service, has information about how to protect yourself from mail fraud and how to identify when you've been targeted. Access online at: **deliveringtrust.com**.

Federal Trade Commission (FTC) Consumer Help

Call the Federal Trade Commission to file a complaint against a company if you feel you have been defrauded.

Call toll-free 1-877-FTC-HELP (1-877-382-4357) or visit **www.ftc.gov/complaint**.

Securities and Exchange Commission

The SEC is a good resource for checking up on an investment adviser and investment products. You can also call them at 1-800-SEC-0330 if you would prefer to speak with someone by phone. Access online at: **investor.gov**.

Consumer Financial Protection Bureau

If you have a complaint about fraudulent activity involving a bank account or service, credit reporting, debt collection, among other areas, contact the CFPB to file a complaint. File online at: **consumerfinance.gov/complaint**.

National Association of Insurance Commissioners

Visit the NAIC website if you want to reach a state insurance agency about an insurance product or salesperson. Find your state at: **naic.org/state_web_map**.

Commodity Futures Trading Commission (CFTC)

The CFTC can assist with problems in commodity futures, precious metals, and foreign currency trading. Call 1-866-366-2382 or visit **cftc.gov/consumerprotection**.

To talk to a volunteer trained in how to spot and report fraud, call the AARP Fraud Watch Network Helpline at 1-877-908-3360

Fraud Watch Network

aarp.org/fraudwatchnetwork

Watchdog Alerts / Tips & Resources / Free for Everyone

D19948 (1218)