

AARP WATCHDOG ALERT HANDBOOK

VETERANS' EDITION: 10 WAYS CON ARTISTS TARGET VETERANS







WATCHDOG ALERT HANDBOOK: TEN WAYS CON ARTISTS TARGET VETERANS

As a veteran, you have protected our country with your service. Now let us help you protect yourself from scams that target veterans and your guaranteed benefits. As with all scams, vigilance is your number one weapon.

The AARP Fraud Watch Network is a go-to resource for:

- The latest breaking scam alerts, delivered right to your inbox;
- A scam-tracking map featuring warnings from law enforcement and people in your state who are sharing their experiences so you'll know what to watch out for;
- The Con Artist's Playbook—a
 handbook of interviews with
 con artists who reveal how they steal
 your hard-earned money; and
- A phone number you can call to talk to volunteers trained in how to spot and report fraud.

Protect yourself from identity theft, investment fraud, and other common scams.

Our *Watchdog Alert Handbook* gives you information about the nine most common ways con artists steal from veterans.

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.



BENEFITS FRAUD

This type of fraud occurs when a scammer attempts to manipulate or gain access to a veteran's government benefits.

1. BENEFITS BUYOUT SCAM

Scammers offer an upfront payment of cash in exchange for a veteran's future disability or pension payments. These buyouts are typically a fraction of the value of the benefit.

2. CHARGING FOR RECORDS

A scammer attempts to charge for access to a veteran's military records or government forms. Never pay for your records; all information is free through your local VA.

3. INVESTMENT/PENSION SCAM

Unscrupulous investment advisers claim the veteran may be able to claim additional government benefits by overhauling their investment holdings. Get credible information on how to qualify for veterans benefits by contacting your state veterans' affairs agency. Visit www.nasdva.us and click on "Links."

4. VETERANS CHOICE PROGRAM (VCP) SCAM

Scammers have set up a phone number nearly identical to the number veterans dial to find out if they are eligible to use approved health care providers outside of the VA system. Vets call the fake number, and a message prompts them to leave their credit card information in return for a rebate. They debit your account, and the vet gets nothing in return. Make sure to dial the correct number for the VCP: 1-866-606-8198.

IDENTITY THEFT

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

5. VETERANS ADMINISTRATION PHISHING

Scammers call veterans claiming they work for the VA and ask for personal information to update their records. If you get an unsolicited call from the VA, hang up.



6. EMPLOYMENT SCAMS

Con artists post bogus job offers to recruit veterans on various online job boards. The scammer may use or sell your personal information provided in the job application. It's likely a scam if you have to pay to get the job, you need to supply credit card or banking information, or the ad is for "previously undisclosed" federal government jobs.

OTHER COMMON SCAMS

7. GI BILL EDUCATION MARKETING SCAM

Veterans seeking to take advantage of the GI Bill for college courses may be targets of deceptive marketing tactics that provide false information and encourage them to attend expensive for-profit educational institutions. The VA offers a comparison tool to help you locate a school and determine your benefits. Visit www.vets.gov/education/gi-bill.

8. SPECIAL DEALS FOR VETERANS

Scammers offer special discounts for veterans on a range of products, like loans and car purchases. Often, the products aren't discounted at all, or they don't actually exist. Check out offers carefully, ask more questions than you answer and never wire money to someone you don't know.

9. RENTAL SCAM

A scammer posts a fake rental property on a classified ad website offering discounts for active duty military and veterans. You just need to wire transfer a security deposit to the landlord. Only there is no rental property, and you just lost your security deposit.

10. THE FAKE CHARITY SCAM

A scammer, appealing to your sense of commitment to those who have served, claims to represent a charity helping veterans and their families. Only the scammers pocket the money and divert donations away from legitimate charities that serve veterans. Check out a charity at www.charitynavigator.org or charitywatch.org before supporting one.

GENERAL FRAUD 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.
 - 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

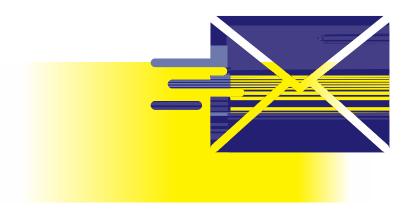
- Watch for missing bills and review your monthly statements carefully. Contact your creditors if a bill doesn't arrive when expected or includes charges you don't recognize.
- Don't invest in anything you are not absolutely sure about. Do your homework on the investment, the company, and the salesperson 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.
- PROTECT YOUR INFORMATION ONLINE
 - Beware of emails that claim to come from a bank, Internet Service Provider, business or charity and ask you to confirm your personal information or account number. If you receive one that is suspicious, forward the email to spam@uce.gov.
 - Avoid conducting personal or financial business on shared/public computers or over public wireless hotspots.
 - 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" not the usual "http."

PROTECT YOUR MAIL

Every day, the U.S. Postal Service safely and efficiently delivers millions of checks, money orders, credit cards, and merchandise. Unfortunately, such items are also attractive to thieves. Here's what you can do to protect your mail from thieves:

- Don't let incoming or outgoing mail sit in your mailbox.
 You can significantly reduce the chance of being victimized by simply removing your mail from your mailbox every day.
- If you change your address, immediately notify your Post Office and anyone with whom you do business via the mail.
- Hand outgoing mail to your letter carrier, or mail it at the Post Office, an official blue USPS collection box on the street, or a secure receptacle at your place of business.



- Never send cash or coins in the mail. Use checks or money orders. Ask your bank for "secure" checks that are more difficult to alter.
- If you have concerns about security in your neighborhood, consider installing a lockable mailbox or obtaining PO Box service from your local Post Office.
- 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 charitywatch.org or charitynavigator.org.



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



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**.



MILITARY CONSUMER

This site, operated by the federal government, empowers military and veteran communities with tips and tools to be informed consumers. Access online at **www.military.consumer.gov**.

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**.

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 **ftccomplaintassistant.gov**.

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 **sec.gov/investor** or **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**.

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**.





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.



aarp.org/protectveterans