SUPPORTING VICTORIES FOR VETERANS

DAV®

KEEPING OUR PROMISE TO AMERICA'S VETERANS

Benefit Fraud Prevention

Protect your benefits. Learn to recognize, prevent and report scams targeting Veterans.

Secure your Data

Protect Payments

Verify Identity

Veteran Centered Scams

Why Veterans Are Targeted?

Veterans are frequently targeted by fraudsters who use sophisticated methods to exploit the consistency of VA benefits.

The Main Goal

Scammers aim to steal money or access sensitive personal identifiable information (PII) to commit identity theft.

Consistent Income Source
Scammers know that veterans receive reliable compensation, pension and disability payments on a specific date.

False "Overpayments"
Fraudsters claim you have been "overpaid" and must return money immediately or they attempt to redirect your deposits.

Impersonating Officials
Criminals pretend to be VA employees or Government agents to gain your trust and lower your guard.

Benefit "Maximization" Schemes
Offers to "increase" or "maximize" your benefits for a fee are often traps to harvest your data and money.

Veteran Centered Scams

Why is Fraud Rising?

Fraud is surging globally due to the convenience of advanced technology, economic instability and the ease of digital anonymity.

Digital Reach
Increased use of text, email and social media allows scammers to reach millions instantly at low cost.

Sophisticated Tools
AI, Spoofed caller IDZs and professional looking fake websites makes impersonation harder to detect.

Economic Pressures
Global economic instability fuels organized scam networks aggressively seeking financial gain.

Reliable Targets
Veterans are specifically targeted because of the known existance of government backed benefits.

GI Bill Fraud

Understanding the threat

What is GI Bill Fraud?

Education scams are when a fraudulent company or college/individual misleads students. Scammers will also attempt to charge upfront fees for free programs.

Targets

Scammers often promise to “unlock” or “maximize” GI Bill benefits for a fee or use phishing to steal login credentials.

Reporting & Prevention

Verify schools via the GI Bill Comparison Tool. Never pay a third party to apply for your own benefits. You should report fraud, scams and identity theft to the US Department of Education Office of the General Counsel.

Romance and Friendship Fraud

Understanding the threat

What is Romance & Friendship Fraud?

Scammers assume a fake online identity to gain your affection or trust. The scammer then uses the illusion of romance or close friendship to manipulate or steal from you.

Targets

Attackers create fake profiles through popular social media or dating sites. Once contact is made they attempt to chat with the victim, often times multiple times a day. Ultimately they present a story and ask for money

Reporting

Report fraud, scams and bad business practices to the Federal Trade Commission. reportfraud.ftc.gov

Pension Poaching

Understanding the threat

What is Pension Poaching?

Financial predators target veterans and survivors, charging fees to “qualify” them for VA Pension benefits.

Targets
Poachers often advise you to hide assets to qualify for benefits which can cause severe legal issues and disqualification from Medicaid.

Methods
Often impersonates official government agencies, trusted organizations or legal aid.

Age 65+ Fraud

Understanding the threat

What is Age 65+ Fraud?

Age 65+ veterans are often vulnerable populations and are frequently targeted by fraudsters.

Targets

The number of veterans VA provides pension benefits to as of June 2025 who are 65+ years old is 114,162.

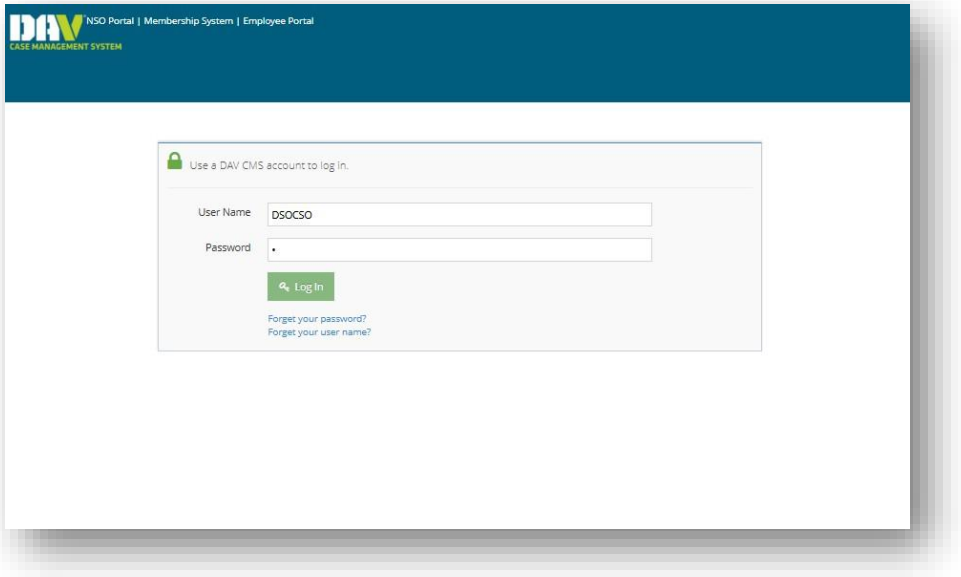
Reporting

If you miss a VA benefit payment, call the VA directly at 1-800-827-1000. Report fraud, scams and bad business practices to the Federal Trade Commission.
consumercompliance.fcc.gov

Protecting Client Data: Secure Wi-Fi

On June 23, 2025, DAV announced updates to our Department and Chapter Service Officer Certification Program.

- ✓ Access provided to the DAV Case Management System (CMS).
- ✓ Requires internet access, whether hardline or Wi-Fi.



Protecting Client Data: Secure Wi-Fi

CMS is a robust platform allowing for efficient organization, management, and sharing of client information among DAV service officers.

It offers several key benefits, including:

- ✓ Access to existing client contact information.
- ✓ Real-time claims submission to your local National Service Office.
- ✓ Electronic recordkeeping of all communications (*e.g., phone calls, interviews, notes, claim submissions*), enhancing coordination with National Service Officers.

Our Responsibility to Protect Client Data

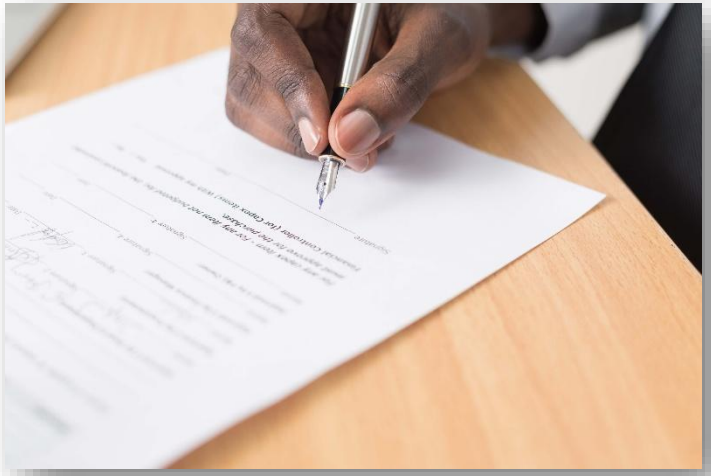
Why does this matter?

- ✓ Claims files contain highly sensitive personal data.
- ✓ Identity theft risk is significant.
- ✓ One breach can impact multiple clients.
- ✓ Data protection is a part of advocacy.

Safeguarding a client's information is just as important as preparing their claim.

A Look Inside a Claims Submission

What is at risk?



- ✓ Social Security Numbers
- ✓ Medical Records
- ✓ Service Records
- ✓ Financial and Dependency Information
- ✓ Direct Deposit Details

The Myth of “Known” Wi-Fi

Known Networks are NOT Secure Networks

- ✓ Saved networks can be spoofed.
- ✓ Devices auto-connect without verification.
- ✓ Attackers create “evil twin” networks.
- ✓ Public guest Wi-Fi is easily monitored.

If your device connects automatically, it may not be connecting to the real network.

High Risk Locations

Where does risk increase?

- ✓ Coffee Shops
- ✓ Fast Food Restaurants
- ✓ Airports
- ✓ Shared Office Spaces
- ✓ Community Centers

Public or shared networks may not be appropriate for submitting claims.

Best Practice: Secure Connections Only

So, what should we do?

- ✓ Use private, password-protected networks
- ✓ Prefer hardwired connections, when in doubt
- ✓ Avoid open and public Wi-Fi
- ✓ Disable auto-join on public networks

Strengthen Your Defense

What are some layers of protection?

- ✓ Keep all devices updated.
- ✓ Lock screens when away.
- ✓ Update passwords regularly.
- ✓ Use a password protected Wi-Fi, or personal Hotspot.
- ✓ Delete all claims and evidence immediately after CMS submission.

Security works best in layers, not in single solutions.

Protecting Client Data is Crucial

Cybersecurity is Client Protection

- ✓ Every department and chapter service officer plays a vital role
- ✓ Data protection reflects organizational integrity
- ✓ Clients trust us with their most personal information

If we wouldn't leave paper claims and evidence unattended in public, we shouldn't expose digital files either.

For More Information

dav.org

Protect Yourself From Education Fraud

HELPFUL TIPS FOR VETERANS TO PROTECT THEIR BENEFITS

One of the most important investments you can make is your education. While your education benefits, such as the Post-9/11 GI Bill, can help you further your education and launch an exciting new career, verifying the information published by educational institutions is essential.

Department of Veterans Affairs (VA) wants to ensure Veterans make the best education decisions this back-to-school season and receive value for their hard-earned benefits. We encourage Veterans and their beneficiaries to know the warning signs of education fraud and proactively prevent fraud.

WHAT ARE THE TYPES OF SCAMS TARGETING YOUR EDUCATION BENEFITS?

- **Job Scams.** Job Boards or Advertisements targeting specific demographics may be misleading or fake and require personal information or money to get the job. You can find free, official information about federal jobs at USAJOBS.gov, FedsHiresVets.gov, and CareerOneStop.org. Your State's Department of Labor may have job listings, contacts for local job offices, and resources for counseling and referrals.
- **Student Loan Scams.** Educational institutions may promise immediate student Loan Forgiveness or debt cancellation to entice Veterans to enroll classes.
- **Scholarship Scams.** Educational institutions may "guarantee" Veterans a scholarship in exchange for a redemption/processing fee.
- **Seminars.** Veterans may be promised a scholarship and financial aid under the guise of high-pressure sales pitches where they feel pressured to pay immediately or risk losing the so-called "opportunity."
- **Free Gifts.** Veterans may be promised incentives such as free laptops, gift cards, or other "freebies" for enrolling in courses.

HOW CAN YOU PROTECT YOUR EDUCATION BENEFITS?

- ✓ **Choose GI Bill Approved Schools.** Use the WEAMS Institution Search Tool to find GI Bill approved schools.
- ✓ **Use the GI Bill Comparison Tool.** Compare the benefits you'll receive at different schools.
- ✓ **Learn about the Principles of Excellence Program.** The program requires schools that receive federal funding through programs such as the GI Bill to follow certain guidelines.
- ✓ **Check out the National Resource Directory Database.** The database provides validated resources that support recovery, rehabilitation, and reintegration for Service members, Veterans, family members, and caregivers.
- ✓ **Find schools that take part in the Yellow Ribbon Program.** The program can help you pay for school costs not covered by the Post-9/11 GI Bill.

Report Suspicious Activity

- To report a missing VA benefits payment, please call the VBA National Call Center at 800-827-1000.
- File a complaint with Federal Trade Commission (FTC).

Benefits Delivery Protection & Remediation
Protecting America's Heroes

PROTECTING YOURSELF FROM ROMANCE AND FRIENDSHIP SCAMS

Fraud Prevention Tips for Veterans

VBA IS COMMITTED TO DETERRING FRAUDSTERS

Have you or a loved one been the victim of an online romance scam? Are you wondering how you can protect your data and safeguard your benefits?

We are here to help. The Veterans Benefits Administration (VBA) is proud to honor Veterans by actively working to identify growing fraud threats and trends. Veterans need to be aware of the fraudster's tactics and stay abreast of methods to protect their data and themselves.

$1.2 billion

The total reported losses from romance scams according to the 2024 Federal Trade Consumer Sentinel Data Book.

PREVENTATIVE MEASURES

Romance and friendship scams are becoming increasingly popular on online platforms. Veterans must be cognizant of the risks and vulnerabilities that may leave them susceptible to attack. **The following tips and behaviors can help Veterans practice safe online behavior and prevent fraud.**

- ✓ **Trust your instincts.** Fraudsters may be overly flattering to befriend individuals or attempt to quickly establish a relationship or friendship. If your online interactions with a user seem too good to be true or feel disingenuous, cease communication immediately.
- ✓ **Request a phone or video chat early.** With online friends or love interests, ask to schedule a call after connecting to confirm they match their profile.
- ✓ **Check for evidence of suspicious activity.** Check for evidence of suspicious activity and perform a Google search with the name of the organization or person plus the words "scam", "review" and "complaint".
- ✓ **Conduct a reverse-image search.** This process can help confirm if profile photos are legitimate.
- ✓ **Never send bank information or payment to "online friends" or others.** Fraudsters may request monetary assistance for financial woes or threaten to release or destroy your private photos or conversations if you fail to comply and send payment or banking information. If you are being blackmailed, do not respond, and report the incident immediately.
- ✓ **Never share your VA login credentials and regularly change your passwords.** Keep all personal VA information (e.g., VA.GOV, eBenefits logins) private, never share personally identifiable information (PII) with "online friends" and do not use PII in your passwords.

HOW ROMANCE AND FRIENDSHIP SCAMS HAPPEN

A fraudster creates a fake profile on a social media or dating app

They connect with the victim and attempt to establish a fast relationship through frequent communication

Once trust is gained, the fraudster will ask for money, PII, or other compromising information

REPORTING FRAUD

- If you miss a VA benefits payment, identify a discrepancy in payments, or find suspicious activity with your direct deposit account, contact the VA immediately at 1-800-827-1000.
- File a complaint with the Federal Trade Commission by visiting reportfraud.ftc.gov.
- Visit the Cybercrime Support Network for additional resources to help Veterans.

Benefits Delivery Protection & Remediation
Protecting America's Heroes

U.S. Department of Veterans Affairs

Age 65+ Fraud Prevention Campaign

Protecting Our Elderly Veterans Against Fraud

Have you or a loved one received a suspicious call from an organization claiming affiliation with the Department of Veterans Affairs (VA)?

114,162 The number of Veterans VA provides pension benefits to as of June 2025 (65+). Vulnerable populations are frequently targeted for elderly scams by fraudsters.

The A,B,Cs of Pension Poaching

A financial scam targeting Veterans, survivors, and their families	**B**ecoming a preferred method by criminals to defraud the elderly	**C**ommonly involving financial maneuvers to defraud claimants

Tips to Share with Veterans in Your Community

Don'ts:

- ⊘ **Don't** share your personal information (e.g., VA.GOV, eBenefits), or other VA login Credentials with anyone.
- ⊘ **Don't** sign a blank form to be filled out later without seeing the contents.
- ⊘ **Don't** deposit VA benefits directly into a family member or caregiver's bank account unless the person is court appointed or a VA accredited fiduciary.

Do's:

- ✓ **Do** be alert! Identity theft is not always committed by strangers.
- ✓ **Do** frequently change and maintain strong passwords and never use Personally Identifiable Information (PII) in the password.
- ✓ **Do** be vigilant if someone offers to hide or rearrange your assets to qualify for VA pension. You may be required to repay benefits to the government.
- ✓ **Do know VA does not charge for processing a claim or request a processing fee.**

How BDP&R Helps

When a fraudulent payment redirect case is reported or suspected, Veteran Benefits Administration's (VBA) Benefits Delivery Protection and Remediation (BDP&R) team investigates the incident and confirms the fraudulent activity.

- BDP&R determines the necessary actions to protect the Veteran's benefits
- BDP&R reports those responsible for the alleged fraud
- BDP&R immediately reinstating the Veteran's benefits, making the Veteran whole again.

BDP&R works diligently to serve America's Veterans and remains committed to protecting all Veterans and beneficiaries, specifically the most vulnerable, from fraud and abuse.

How to Report Fraud or Pension Poaching

If you miss a VA benefits payment, identify a discrepancy in payments, or find suspicious activity with your direct deposit account, contact the VA immediately at 1-800-827-1000.

You may also file a complaint with the Federal Trade Commission by visiting consumercomplaints.fcc.gov

How Can You Help

VA is committed to defeating fraudsters who target elderly Veterans by **educating all advocates on the fraud targeting and pension poaching tactics being used against Veterans.** Please join us in making VA a hostile environment for fraudsters by encrypting emails when using Veteran information, ensuring antivirus computer updates, and locking your computer when away.

VA | U.S. Department of Veterans Affairs

Benefits Delivery Protection & Remediation
Protecting America's Heroes

Protect Your Donations

Fraud Prevention Guidance to Spot and Avoid Charity Scams

The Department of Veterans Affairs (VA) provides necessary resources and education to protect Veterans from experiencing charity fraud. By raising awareness and offering guidance on how to identify and avoid these scams, we aim to ensure that Veterans can confidently support causes they care about without falling for deceitful tactics.

COMMON TACTICS OF CHARITY SCAMS

- **Unsolicited Contact:** Be cautious of high-pressure requests, unexpected calls, emails or social media messages asking for donations.
- **Lack of Transparency:** If a charity is unable or unwilling to provide clear information about how donations are used, it's a red flag.
- **No Proof of Tax-Exempt Status:** Verify whether the charity is registered as a tax-exempt organization with the IRS.
- **Look-alike Names and Websites:** Watch out for charities with names or websites similar to well-known organizations.

PREVENTATIVE MEASURES

- **Verify Nonprofit Status:** Use the Internal Revenue Service (IRS)'s Tax-Exempt Organization Search Tool and sites like Charity Navigator, CharityWatch, BBB Wise Giving Alliance and Great Nonprofits to look up the charity and read their ratings.
- **Research the Charity:** Search online for the charity using phrases like "best charity" or "highly rated charity." You can also check the charity's website, mission statement and research their track record.
- **Know Who is Asking:** Verify any request from a charity is legitimate by contacting the charity via phone or visiting its website. Obtain written information (including annual reports) to know how your donation is distributed.
- **Keep Personal Information Private:** Never give out personally identifiable information (PII) to a solicitor either by telephone, mail or door-to-door.
- **Check Donation Taxability:** Make sure the donation is tax-deductible meaning you can deduct your donation on your federal tax return. Tax-exempt means the charity does not have to pay taxes. Even if a charity is tax-exempt, your donation may not be tax-deductible.
- **Avoid Paying Cash:** Pay charities by credit card payment or by check that is payable to the fund, not an individual.

$21 million

Total losses from charitable solicitation fraud reported by the Federal Trade Commission (FTC) in 2022. In 2023, there were 9,809 charitable solicitation reports reported to the FTC.

How to Report Suspicious Activity:

- If a Veteran is missing a VA benefits payment, identifies a discrepancy in payments, or finds suspicious activity with their direct deposit account, contact the VA immediately at 800-827-1000.
- Veterans who suspect they have experienced fraud can find resources to file a report to the appropriate agency by visiting www.vsafe.gov or calling 833-38V-SAFE.

Benefits Delivery Protection & Remediation
Protecting America's Heroes

VA | U.S. Department of Veterans Affairs

Fraud Prevention Alert

U.S. Department of Veterans Affairs

Benefits Delivery Protection & Remediation
Protecting America's Heroes

Beware: Scammers are impersonating the Department of Veteran Affairs!

NEED ASSISTANCE?

Accredited attorneys, agents, and Veterans Service Organizations (VSO) are available help you file claims. Click on the link to find accredited representatives to support you.

Use the VA Office of General Counsel (OGC) Accreditation Search Tool to confirm and validate the credentials of companies and law firms.

PROTECTING YOURSELF AND YOUR BENEFITS

Scammers are targeting Veterans and their families by creating fraudulent letters, emails, and texts often including fake VA letterheads and logos, making it difficult to distinguish genuine VA communications from scams.

- ✓ **Fake VA Letterheads and Logos:** Scammers often fake VA letterheads, logos, and phone numbers to seem authentic. VA letters include appeal rights.
- ✓ **Claims of Overpayment:** Scammers claim you have been overpaid on your VA benefits and now owe money back to VA.
- ✓ **Pressure tactics:** Scammers may pressure you into making immediate payments directly to them, instead of through official VA payment channels.
- ✓ **Requests for Sensitive Information**: Scammers may ask for sensitive information, such as your VA credentials, passwords, or financial information.
- ✓ **Verify overpayments:** Verify the authenticity of debt notifications by logging into your official VA.gov account. For more information visit va.gov/manage-va-debt.
- ✓ **Be cautious of unsolicited contact:** Be wary of unsolicited emails or texts, demanding personal details or directing you to external websites that are not part of VA.gov.
- ✓ **Do not pay upfront fees:** If someone demands an upfront payment to help with your VA debt or claims, it's a scam. VA provides free help with managing debts and claims.
- ✓ **Never Share login information:** VA will never ask for your VA login credentials or password.

RESOURCES AND TOOLS

Veterans who suspect they have experienced fraud can find resources to file a report to the appropriate agency by visiting VSAFE.gov or calling 833-38V-SAFE.

File a complaint with the Federal Trade Commission at ReportFraud.FTC.gov or your state attorney.

If you gave your personal information to a scammer, go to IdentityTheft.gov for steps you can take to protect your identity.

If you are unsure about a phone call, letter, email, or text, contact VA directly at 1-800-827-1000.

Disabled American Veterans
Mid-Winter Conference
February 22 – 25, 2026

Fraud is the intentional misrepresentation of information to receive unearned payments. It's on the rise globally, prompting businesses and individuals to enhance their security measures. Veterans are frequently targeted by fraudsters who are becoming increasingly sophisticated in their methods.

Veterans are particularly vulnerable because of the consistency of VA compensation, pension, and disability payments. Scammers exploit this steady income by impersonating officials, claiming false "overpayments," or offering to "maximize" benefits for fees. Their goal is to steal money or access sensitive personal information.

The table below highlights some of the most common VA benefit scams targeting Veterans. It includes information on tactics used by fraudsters, how to protect your benefits, and links to report scams.

Education-GI Benefits Fraud	• Using VA education benefits wisely: A guide to fraud prevention • VSAFE: Education Scams • What are the signs of a student loan scam? (CFPB) • Protect your G.I. Bill benefits from scams!
Imposter Scams	• VSAFE: Imposter Scams • Impersonation is Everywhere: Guard Yourself! • How To Avoid a Government Impersonation Scam (FTC) • Digital Defense: Empowering Veterans Against Smishing Threats • World Elder Abuse Awareness Day: Protecting older adults from government imposter scams
Job Scams	• VSAFE: Employment: Business and Job Opportunities • Avoiding Job Scams on National Hire a Veteran Day Beware of job scams targeting Veterans
Overpayment Scams	• New scam: VA Benefits Overpayment • Veterans and caregivers: Recognize VA benefits overpayment scams (FTC) • Glad You Asked: Overpayment Scams (video) • SITREP: NEW VA Overpayment SCAMS Targeting Veterans (video)
Payment Redirect Scams	• Protect your benefits: Combatting Payment Redirection Fraud

Pension Poaching Scams	• VA OIG Fraud Alert: Protect Veterans from Pension Poaching • Pension Poaching FAQ • Pension Poaching Prevention: Spot a Scam, Stop a Scam! Be Prepared, Be Educated, Be Vigilant. • Prevent pension poaching fraud and protect your VA benefits • Know who to trust with your VA pension benefits
Additional Tools and Reporting Information	• If a Veteran is missing a VA benefits payment, identifies a discrepancy in payments, or finds suspicious activity with their direct deposit account, they should contact VA immediately at 1-800-827-1000. • Veterans who suspect they have experienced fraud can find out more and report to the appropriate agency at https://vsafe.gov/ or by calling (833) 38V-SAFE. • To learn more about scams impacting VA benefits, please visit: VBA Fraud Prevention site (https://benefits.va.gov/BENEFITS/fraud-prevention.asp). • Subscribe to VBA monthly newsletters and keep an eye out for fraud prevention information on VA News!