VA | U.S. Department of Veterans Affairs

HELLO.

Welcome to the Fraud Prevention Kit

WHAT'S INSIDE?

Learn about Fraud
and what you can do about it.

About Fraud

Fraud attempts targeting Veterans, their families, survivors, and caregivers are on the rise. Fraud can be defined as intentional deception that results in the loss of money or benefits. Fraudsters, or bad actors, are actively evolving new tactics to deprive Veterans of their hard-earned cash and benefits. A November 2021, American Association of Retired Persons (AARP) study found that 78% of Veterans have been targeted by scams designed to exploit their military services history.

REPORT POTENTIAL FRAUD

For healthcare-related fraud, please contact the Veterans Health Administration, Office of Integrity and Compliance Helpline at 866-842-4357 (VHA-HELP).

For suspected VA Benefits fraud call the VA Benefits Hotline - 1-800-827-1000.

Veterans are often targeted because they have access to benefits and resources. Imposter scams account for nearly 40% of the military community's fraud losses. Imposter scams can be anything from online romance scams to grandparent scams claiming the grandchild is in trouble. Often the goal is to gain access to benefits the government provides to those who served. Scams affect every age group harming younger people and older adults.

Below are a few examples of real-life examples of fraud:

A Marine Corps Sergeant discovered there were dozens of fake Facebook accounts using stolen photos of him. These fake accounts flourish on Facebook and Instagram where bad actors impersonate real American service members to cheat people out of money. Stories of these types of imposter scams are all too prevalent. Another typical scam we see are advertisements of special loan rates or terms for military/Veterans. One retired Army Veteran experienced this by refinancing with what looked like favorable rates only to learn that they lost over $25,000, while only getting $5,000 in return. They were taught trust but verify and thought they had done due diligence only to be scammed.

Know that if you have experienced fraud, you are not alone. Often there is shame or victim blaming in stories about fraud. In reality, criminals are sophisticated and prey on good intentions and trust. It should always be shame on them, not shame on you.

About This Toolkit

We are fighting back with initiatives to protect and provide assistance to Veterans, their families, survivors, and caregivers. This toolkit is a partnership amongst federal agencies, Veteran Service Organizations (VSOs), Military Service Organizations (MSOs) and the VA to arm our Veterans with the knowledge of the common schemes we are seeing. We will provide tips and tricks to prevent this from happening. The first section of the Toolkit talks about General Fraud followed by the following areas: Imposter Scams, Healthcare, Finances, Housing, PACT Act, Employment, Education, Memorialization. Each area has a corresponding icon


Imposter Scams


Health Care


Finances


Housing


PACT Act


Employment


Education


Memorialization

Signs it's a scam

1. **Scammers PRETEND to be from an organization you know.** Scammers PRETEND to be from a trusted source or an organization you know. Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the Social Security Administration, U.S. Department of Veterans Affairs, the IRS, Medicare, or law enforcement. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations. They may use names, logos, or links similar to legitimate groups to try to confuse you.

2. **Scammers may appear to be from a trusted source.** They may use real logos and links that appear okay because they appear to be legitimate links or similarly named. Scammers may use names of real government officials, pictures, or attachments to try and prove their legitimacy and gain your trust. They may even spoof legitimate phone numbers.

3. **Scammers may say there's a PROBLEM or a PRIZE so they need to confirm information.** They might say you're in trouble with the government, you owe money, or someone in your family had an emergency. They might say there's a virus on your computer, that you have a package, or a refund is waiting for you. And often they include links to click on that appear to be a legitimate agency/organization website. DO NOT CLICK THE LINK

4. **Scammers may PRESSURE you to act immediately or share sensitive information.** Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story. This is exactly what you want to do. It is important to take the steps found on Page 8.

5. **Scammers may use payments that are hard to trace.** They often insist that you pay using cryptocurrency, by wiring money through a company like Zelle, Venmo, MoneyGram, Western Union or pay as friend to friend. These are all electronic banking apps that you may have loaded onto your phone. They may also request you put money on a gift card and then give them the PIN number on the back.

6. **Scammers may threaten to arrest you immediately if you do not pay.** They may threaten legal action against you or your loved ones.

How to Avoid a Scam

- **Protect your personal or financial information in response to a request that you didn't expect, even if the caller has some of your personal information.** Legitimate organizations won't email or text to ask for your sensitive personal information, like your Social Security number, bank account or credit card number.

- **Know how a scammer tells you how to pay.** Never pay someone who insists you pay with cryptocurrency; mobile payment app like Venmo, Zelle; or wire transfer service like Western Union or MoneyGram; or a gift card. And never deposit a check and send money back to someone.

- **Block unwanted calls and text messages and report them as a scammer.** Take steps to block unwanted calls and to filter unwanted text messages. Use call blocking or call labeling technology that is available on your cell phone or traditional landline. Many text and e-mail applications will allow you to report the number/e-mail.

- **Resist the pressure to act immediately.** Legitimate businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer. Hang up and use a publicly available phone number to reach out to that organization directly.

- **Stop and talk to someone you trust.** Before you do anything else, tell someone – a friend, a family member, a neighbor – what happened. Talking about it could help you realize it's a scam. If you think the message you have received is a scam, do not reply to the message unless and until you are confident that you have verification that the message is legitimate. If the message refers to a specific organization, use a publicly available phone number to reach out to that organization.

- For more resources on Fraud and scams, the Consumer Protection Financial Bureau also provides additional tools https://www.consumerfinance.gov/consumer-tools/fraud/

- Visit out website for additional information on how to avoid Fraud and scams: www.va.gov/VSAFE

How to Report a Potential Scam

Don’t stand by and let bad actors steal the benefits you’ve earned.

For healthcare-related fraud, please contact the Veterans Health Administration, Office of Integrity and Compliance Helpline at 866-842-4357 (VHA-HELP).

For suspected VA Benefits fraud call the VA Benefits hotline - 1-800-827-1000.

For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC) Online: https://reportfraud.ftc.gov

For more resources on Fraud and scams, the Consumer Protection Financial Bureau also provides additional tools https://www.consumerfinance.gov/consumer-tools/fraud/

Scammer Tactics – Don't Click

Spoofing – Disguising an email address, social media profile, sender name, phone number, or website address to convince you that you are interacting with a trusted source.

Email Phishing – Email sent with the intention of deceiving you to act, such as updating a password or clicking on an attachment.

Smishing – Phishing via text messaging. The fraudulent text may appear to come from a reputable business, but it designed to trick you into revealing personal information. Do not click the link. Instead log onto the official account directly on a secure computer browser.

Vishing – Voice phishing occurs via phone. The caller typically leaves an "urgent" message, making recipients believe they will be fined or miss out on an opportunity if they do not respond immediately.

Angler Phishing – Targets social media users. Bad actors will direct message to disgruntled customers, pretending to be customer service agents, to obtain personal information or other account credentials.

Evil Twin Hotspot – Fraudulent Wi-Fi access points designed to trick users into connecting to them so they can steal sensitive information or redirect links to malicious sites.

Juice Jacking – Bad actors use public USB ports to introduce malware and monitoring software onto devices. Always carry your own charger and use an electrical outlet instead.

Pop-up Phishing – Fraudulent messages that have been infected with malicious code, "pop up" on otherwise legitimate websites enticing you to click on them to corrupt your device or data.

Tell Me About Yourself – During a phone call, the scammer may ask you to verify who you are by asking you to confirm your personal information to access records.

Protection For You and Your Family – Cyber

Protect Yourself
When receiving email, hover your cursor directly over the link without clicking it, and read the text that pops up to see the intended destination look for things like misspellings.

Be careful what you download. Never open an email attachment from someone you do not know and be wary of email attachments forwarded to you.

Be suspicious of emails or text messages marked “urgent”.

Be careful about sharing personal information such as social security number online and on social media.

Check that the actual email address matches the organization they claim to be from.

Access official website, phone number email to re-confirm official information.

Check for poor spelling or grammar, as well as confirming logos are official.

Cyber
Activate multi-factor authentication on your accounts. A password isn’t enough to keep you safe online any longer. Use multi-factor authentication when you can. A second layer of identification, such as entering a code sent via text message or email, can help the service provider verify logins.

Update your software. Bad actors take advantage of system flaws so it’s important to update your device operating systems and applications.

Do not click. More than 90% of successful cyber-attacks start with a phishing email. Once they have your information, they can use it on legitimate sites. They may also try to get you to run malicious software, also known as malware. If it’s a link you don’t recognize, trust your instincts, and don’t click. Suspicious texts will also often contain dangerous links.

Use strong passwords. Be mindful of password storage, complexity, and usage. Make sure your passwords are unique, use a combination of letters, numbers, and special characters, and are case sensitive.

Protection For You and Your Family – Phone

Phone

If you are contacted by someone claiming to be from the government or military, there are some red flags to watch out for that may indicate that you are being scammed, such as:

- Unsolicited computer-generated voice calls asking you to press a number to speak with someone are almost always a scam. Hang up on these types of calls.
- The caller asks for personal information, like your Social Security number, mother's maiden name, or bank account information.
- The caller claims to be from a government agency, like the IRS, VA or Social Security Administration or warns about an issue related to your Social Security number or other personal information.
- They demand immediate payment, often through payment app or service, gift cards, prepaid debit cards, wire transfer, cryptocurrency, bank transfer or payment, money order, or encourage you to move your money to a "protected" bank account.
- The caller threatens to arrest you or have your utilities cut off if you don't pay.
- The caller claims you will face legal action unless you do what they say, which often involves payment or transferring money.
- If you get an inquiry from someone who says they represent a company or government agency, hang up and call the phone number on your account statement, or on the company's or government agency's website to verify authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.

Immediate Actions

If you think you are the victim of an imposter scam, it is important to act right away to protect yourself and your finances. Here are some steps to take if you think you have been scammed:

- Stop all contact with the individual(s) who contacted you.
- Save all information or messages about the individual(s) who contacted you pretending to be in case you need to take legal action.
- If you provided financial information, like your credit card number or bank account information, contact your bank or credit card company right away. They may be able to help you cancel the transaction or get your money back.
- If you sent funds via gift card or money transfer, report the scam to the issuer. They might be able to help you stop the transaction. Find their contact information by visiting their website.
- If you provided personal information, like your Social Security number, you may be at risk for identity theft. Report identify theft and get a recovery plan at https://www.identitytheft.gov/#/
- Keep an eye on your credit report and financial accounts for any unusual activity and consider placing a freeze on your credit.
    - Equifax Security Freeze https://www.equifax.com/personal/credit-report-services/credit-freeze/
    - Experian Freeze Credit https://www.experian.com/freeze/center.html
    - Transunion Freeze Credit https://www.transunion.com/credit-freeze
- Consider adjusting your mobile settings to block spam calls, texts, and emails.

Protection For You and Your Family – Identification

- Use additional security measures such as multi-factor identification, which requires two or more proofs of identity to grant you access.
- Don’t share your login information over the phone or via email with others.
- Set up electronic access to all financial accounts. You can set alerts to text you with each transaction, so you can track activity, as well as other alerts. Use an app to access if possible because it has more encryption and other protections. You don’t have to wait a month or a quarter to review your account activity.
- Don’t deposit VA benefits directly into a family member or caregiver’s bank account unless the person is court appointed or a VA appointed fiduciary.
- To protect yourself now against future identity fraud, add a fraud alert to your credit reports. A fraud alert requires a lender to contact you before opening a new account in your name.
    - Equifax Fraud Alert https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
    - Experian Fraud Alert https://www.experian.com/fraud/center.html
    - TransUnion Fraud Alert https://www.transunion.com/fraud-alerts
- If you are uncomfortable with a call from someone claiming to be from the VA, hang up, and call MYVA411 or your local VA facility to confirm whether the call was legitimate.
- Vary your login information.

Imposter Scams

Don't send money or share personal information in response to an unexpected request — whether it comes as a text, a phone call, email, or direct messages on social media.

Scammers can be convincing and find ways to make their story seem real. They sometimes use information from social networking sites to convince you they know you. They might hack into a loved one's email account to seem like it's really someone you know.

Is a distressed friend or loved one in touch? Check it out. Look up that person's phone number yourself and check in. Call another family member to see what they know. Is there a real emergency?

Does it seem to be the Internal Revenue Service (IRS) calling? Hang up. The IRS will never contact you initially by phone. The real IRS won't accept payment by prepaid debit cards, iTunes cards, gift cards, or wire transfers. They also won't ask for a credit card over the phone. If you have tax questions, visit IRS.gov or call the IRS at 1-800-829-1040.

Same goes for the Social Security Administration (SSA). The SSA will not request payment by prepaid debit cards, iTunes cards, gift cards, or wire transfers.

Getting friend requests on social media from people that you are already friends with. This is a sign that your friend's account may have been spoofed.

Does a caller say you've been selected to get a grant or other money from the government? Even if you've recently completed the Free Application for Federal Student Aid (FAFSA), a real government agency won't ask you to pay a processing fee related to FAFSA or for a grant that you have already been awarded.

Does the caller say your computer has a virus and they can help? Hang up. Never give control of your computer or your credit card information to someone who calls you out of the blue.

Is your online romantic interest asking for money? Scammers make fake profiles and sometimes use photos of other people – even stolen pictures of real military personnel. Scammers want your money in a way that makes it hard for you to get it back. They'll tell you to wire money through a company like Western Union or MoneyGram, put money on gift cards (like Amazon, Google Play, iTunes, or Steam) and give them the PIN codes, send money through a money transfer app, or transfer cryptocurrency.

Common Schemes – **Online Romance**

Romance scams are when a criminal adopts a fake online identity to gain your affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from you.

U.S. Department of Veterans Affairs

ChooseVA

Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- Scam artists often say they are engaged in projects outside the United States. That makes it easier to avoid meeting in person. They often ask for money for a medical emergency or unexpected legal fee.
- Scammer's intention is to establish a relationship and gain trust as quickly as possible. Scammers may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will ask for money.
- You meet someone on a dating site, simply playing an online game, or scrolling your social media feed. This person takes a quick interest in you, suggests you move to another platform to talk, and turns on the charm. They will flatter you, ingratiate themselves, and convince you that you belong together. Only you never meet in person. Eventually, they will start asking for money that may start small and become more frequent and larger over time. The requests for money turn into demands, and they are relentless. Remember sometimes these are fake accounts like the Marine Corps Sargeant who found that his image was used to gain people's trust and then scam them out of money.

Tips to Avoid Scams

Do's

- ☐ Do a reverse image search of the person to see if the image, name, or details have been used elsewhere. Google Image Search tool helps to identify a person using a picture.
- ☐ Do go slowly and ask a lot of questions using video calls through your phone or computer. Be cautious of individuals that are not available to video call due to poor service or being out of country.
- ☐ Do beware if the individual seems too perfect or quickly asks to communicate with you directly.
- ☐ Be careful about the information you share online and/or social media. This information can be used against you.

Don'ts

- ☐ Do not send money to anyone you have only communicated with online or by phone. i.e., Venmo, PayPal, or other mobile payment services
- ☐ Do not share your bank account information with anyone you have only met online, as they are most likely trying to steal from you.

REPORTING INFORMATION

FOR ALL NON-VETERAN AFFAIRS RELATED FRAUD, REACH OUT TO THE FEDERAL TRADE COMMISSION (FTC)

- *Online: https://reportfraud.ftc.gov*

Common Schemes – **Health Care Fraud**

U.S. Department of Veterans Affairs

Choose VA

Health care fraud occurs when an individual or company knowingly mis-represents or mis-states something about the type, the scope, or the nature of the medical treatment or service provided, in a manner that could result in unauthorized payments being made.

Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- Medical providers outside the VA may try to scam the VA when they submit claims to receive payment from VA for the services they provide you. For example, they could bill for services they didn't provide or even submit duplicate bills to get paid more than once.
- Providers suggesting treatments or procedures you do not need, to obtain payment from VA.
- Be wary of unproven medical care, equipment, and procedures.

Do's

- ☐ Protect your personal health care and insurance information. Scammers will try to use this information to gain access to your account – and even steal your identity.
- ☐ Review all paperwork to confirm accuracy and authenticity. Confirm dates of service for care received, patient's name, provider's name, location, and types of services.
- ☐ Check your explanation of benefits (EOB) from your provider Did you visit the doctor listed on the date indicated? Does the EOB contain any procedures or treatment that do not look correct to you? VA wants to know! For a resource on understanding an EOB, https://www.va.gov/COMMUNITYCARE/docs/pubfiles/brochures/HowToReadAnEOB.pdf
- ☐ Check all billing from providers if you receive a VA statement or EOB.

Don'ts

- ☐ Do not trust someone who contacts you saying they're affiliated with the Department of Veterans Affairs. Scammers use official-looking names,

seals, and logos. If you're not sure if the "offer" is legit, hang up and call your VA representative directly.

- ☐ Do not share personal health information or health insurance information with others. If anyone says they need your information, it's a scam.
- ☐ Do not provide your Social Security number, medical records, or other personally identifiable information to anyone offering claims assistance without verifying accreditation status.
- ☐ Do not sign a blank form for someone else to complete later. Always review the completed form before signing and keep a copy of the completed form for record keeping purposes.
- ☐ Do not order medical equipment over the phone unless advised to do so by your physician. Hang up on unsolicited calls offering you special services or something that sounds too good to be true.
- ☐ Do not be silent if you think VA is paying for services you didn't receive. Don't agree to treatments or procedures you are uncomfortable with just because a new provider says they are necessary.

REPORTING INFORMATION

For healthcare-related fraud, please contact the Veterans Health Administration, Office of Integrity and Compliance Helpline at 866-842-4357 (VHA-HELP).

Common Schemes – **Insurance**

Insurance scams are a false representation of fact with the intent to deceive, including actions taken based on misrepresentation.

U.S. Department of Veterans Affairs

Choose VA

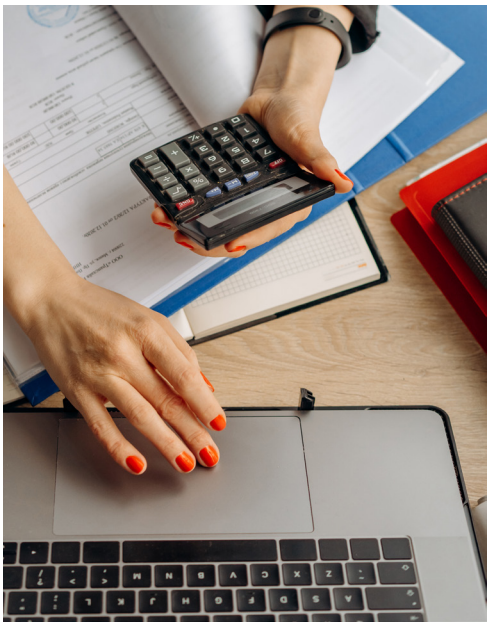
Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- Commercial insurance advertising low rates, offering insurance when you have pre-existing conditions, or offering extremely attractive insurance deals.
- Trick you into buying an annuity and other products where you end up paying more than the benefit.
- Persons without legal authority from the Insured Veteran or VA Fiduciary Services attempting to gain information about your VA insurance policy.
- Examples of fraudulent actions or attempts by a bad actor who is trying to get access to life insurance proceeds that they are not entitled to.
  - A Veteran's beneficiary designation is updated without their knowledge.
  - Improper claimant or agent alleging entitlement to insurance proceeds.
  - Claim funds are disbursed to fraudulent payee.

Do's

- ☐ If you get an inquiry from someone who says they represent a company or government agency, hang up and call the phone number on your account statement, or on the company's or government agency's website to verify authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.
- ☐ Confirm you are working with a VA-accredited individual(s) authorized to assist with benefits claims by searching Office of General Counsel Accreditation website. https://www.va.gov/ogc/apps/accreditation/index.asp



Don'ts

- ☐ Do not share personal identifiable information (PII) or consult with persons who do not have appropriate authority to inquire about the VA Insurance policy.
- ☐ Do not believe the get rich quick schemes with guaranteed large benefit awards where they want you to act quickly and guarantee instant/winning results.

REPORTING INFORMATION

FOR SUSPECTED VA HEALTHCARE RELATED FRAUD CALL THE VHA OIC HELPLINE

- → For healthcare-related fraud, please contact the Veterans Health Administration, Office of Integrity and Compliance Helpline at 866-842-4357 (VHA-HELP).
- → For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC)
  - *Online: https://reportfraud.ftc.gov*

Common Schemes – $ Disability and Pension Benefits

U.S. Department of Veterans Affairs

ChooseVA

Many recipients of these benefits are targets for fraudulent activity. Scammers use a variety of methods to either swindle Veterans out of earned benefits or convince them to apply for benefits they are not eligible for.

Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- Offering to assist in preparing or filing your VA benefits application without VA's recognition to do so and charging a fee for such services.
- Offering you an up-front lump-sum payment in exchange for your monthly VA payments going forward. VA benefits cannot be assigned.
- Redirecting mail or benefits to a non-beneficiary, such as a caregiver who is not a VA fiduciary.
- Requesting that the Veteran move money into different accounts or reallocate investments to qualify for a VA pension payment.
- Advertising that boasts they can get you your benefits faster for a fee.
- Referring you to a doctor, who coaches or guides you to report medical conditions you do not actually have and that do not reflect the true impact of your condition. You are then given forms, signed by the doctor, but which you have certified as true and accurate.

Tips to Avoid Scams – Disability and Pension Benefits

Do's

- ☐ Apply directly to VA. Veterans may submit applications for VA benefits securely https://www.benefits.va.gov/BENEFITS/Applying.asp via https://www.va.gov or in person at any regional office. Veterans may file claims directly with VA and VA will help gather the necessary evidence. There are no costs or hidden fees to apply.
- ☐ Validate: If you wish to seek assistance on your claim by a Veteran Service Organization (VSO) representative, agent, or attorney, use the Office of General Counsel Accreditation tool to confirm and validate their accreditation. https://www.va.gov/ogc/apps/accreditation/index.asp
- ☐ Always make sure you are on the official VA website as there are many imposter websites hoping to tangle you in their web.
- ☐ In general, be suspicious of online websites charging a fee for an otherwise free government product or service.

- ☐ Be aware that there are individuals and organizations that are targeting Veterans, particularly elderly war-time Veterans, by offering to provide claims assistance as a way to promote their other business interests. Generally, these individuals or organizations are not accredited or recognized by VA; others could potentially be misusing their VA accreditation.
- ☐ Do know that all VA-accredited VSO representatives, attorneys and agents must follow the standards of conduct for VA-accredited individuals, which expressly prohibit the charging of unlawful or unreasonable fees and engaging in unethical behavior.
- ☐ Do remember that any business or individual that prepares, presents, or prosecutes VA benefit claims without

the proper VA recognition is doing so contrary to law.

- ☐ Do report misconduct that occurs in the course of claims assistance or the improper charging of fees to VA's Accreditation, Discipline, & Fees Program office. More information on how to make a report can be found here: https://www.va.gov/ogc/accreditation.asp.

DON'TS

- ☐ Do not use an individual or organization that is not recognized by VA. There are important safeguards tied to accreditation, such as the opportunity for claimants to request the review of their fee agreements.
- ☐ Do not payan unauthorized company to help you with your VA claim. Only VA-accredited agents and attorneys are permitted to charge a fee, but only for services performed after VA has issued its initial decision on the claim.
- ☐ Do not provide login information, Social Security number, address, or bank information to an unverified email. Do not provide such personal information during a cold call from someone alleging to be from VA. Do not sign a blank form that someone else is supposed to complete later. Always review the completed form before signing and retain a copy of the completed form for your records.
- ☐ Do not participate in a scheme where you are being told to lie or exaggerate your symptoms to the VA. You could go to jail if caught and will have to return funds to the VA for benefit increases.

REPORTING INFORMATION

FOR SUSPECTED VA BENEFITS FRAUD CALL THE VA BENEFITS HOTLINE

- *Phone: 1-800-827-1000.*

→ For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC)

- *Online: https://reportfraud.ftc.gov*

$ Common Schemes – Loans

Finance scams related to loans are when a fraudulent company or individual provides a service that is not in the best interest of the individual. A loan scam is a loan offered under false pretenses. The scammer will often offer to provide services with high rates and fees, or by hiding the actual cost of the loan.

U.S. Department of Veterans Affairs

ChooseVA

Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- Be wary of high interest rates on home and car loans.
- Avoid any loan asking for money up front. Legitimate lenders will charge you a fee after your loan has been approved, not before.
- Lender who is promoting or pressuring you to take a loan with a Variable Interest Rate when they know that you may not have the financial income to repay the loan when the interest rate increases.
- Bad actors will offer loans without credit checks often targeting those with bad credit or debt problems. If the lender is not asking for a credit check it may not be a valid offer.

Do's

- ☐ Validate: If you are interested in working with a Veteran Service Organization (VSO), agent, or attorney, use the Office of General Counsel Accreditation tool to confirm and validate their credentials. https://www.va.gov/ogc/apps/accreditation/index.asp
- ☐ The VA can assist you if you are falling behind on payments and need financial assistance instead of falling for a scam for help. There are several areas to seek assistance, include the VA Loan Guaranty service provides special loan rates for Veterans seeking to purchase homes using VA mortgage financing. Contact the VA directly to assist you with managing your debt. https://www.va.gov/manage-va-debt/

- ☐ Things scammers say to take advantage of you.
  - Everyone gets approved. Bad credit – no problem.
  - Reduced interest rate loans.
  - Special loan terms for Veterans

Don'ts

- ☐ Avoid payday or title loans – these are the types of loans that provide money the same day. These types of loans have high interest rates and fees. Consumer Financial Protection Bureau (CFPB) has more information available on payday loans at https://www.consumerfinance.gov/consumer-tools/payday-loans/
- ☐ Do not ever give your VA, Social Security number or any other government benefits account information such as your username and log-in information during any loan application process.
- ☐ Do not choose a lender that requires no documentation or background checks to provide you with a loan.

REPORTING INFORMATION

FOR SUSPECTED VA BENEFITS FRAUD CALL THE VA BENEFITS HOTLINE

- *Phone 1-800-827-1000*

→ For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC)

- *Online: https://reportfraud.ftc.gov*

Common Schemes – Home Loans and Housing

U.S. Department of Veterans Affairs

Choose VA

Home loan or housing scams may involve mortgage lenders, brokers and other entities making false promises; credit organizations charging excessive fees or making false promises to provide free services. Scammers may also offer to provide you with home repair or offer to assist you with services with the intent to manipulate and/or steal from you.

Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- Someone calling requesting you to cancel mortgage payments and resend the funds elsewhere.
- Using another Veteran's disability status for property tax exemption.
- Unaccredited VA home loan companies offering services at information fairs may be attempting a scam.
- Someone telling you to make mortgage payments to someone other than your current loan servicer.
- Someone pressures you to sign papers you haven't had a chance to read thoroughly or that you don't understand.
- Online scams to get first and last month's payment up front and yet the property isn't theirs to rent out and the scammer take your money.
- Home improvement scammers will offer to help fix up your home, ask for payment up front, and may never complete the work or overcharge.

Tips to Avoid Scams – Home Loan and Housing

Do's

- ☐ Validate: If you are interested in working with a Veteran Service Organization (VSO), agent, or attorney, use the Office of General Counsel Accreditation tool to confirm and validate their credentials. https://www.va.gov/ogc/apps/accreditation/index.asp
- ☐ Get receipts for any monies paid for services.
- ☐ Check with multiple lending institutions for rates a
- ☐ Read the fine print.
- ☐ Considering an Interest Rate Reduction Refinancing Loan (IRRRL) and refinancing a VA loan? Shop around for lenders, compare no-obligation rate quotes between lenders and against your current loan, and then discuss your options. For more information https://www.military.com/money/va-loans/irrrl-facts-for-veterans.html
- ☐ Be cautious of renting from someone inquiring if the VA will pay to fix a rental home.
- ☐ Gather information from reputable sources. For example, additional mortgage resources are available from the Consumer Financial Protection Bureau website https://www.consumerfinance.gov/consumer-tools/mortgages/

Don'ts

- ☐ Do not pay money for someone to fill out housing assistance applications and recertifications for you. VA provides these services for FREE.
- ☐ Do not pay fees before services are provided.
- ☐ Do not sign over the title to your property.

- ☐ Do not ever give your VA, Social Security number or any other government benefits account information such as your username and log-in information during any housing application process.
- ☐ Do not give out personal information to a lender or servicer who contacts you out of the blue. Scammers can spoof phone numbers, so you can't rely on caller identification. If you're unsure, it's always safer to hang up and call your loan servicer directly at the number on your mortgage statement.
- ☐ Do not allow a friend, family member, or any individual to use your information to get disabled Veteran status for property tax reduction.

REPORTING INFORMATION

FOR SUSPECTED VA BENEFITS FRAUD CALL THE VA BENEFITS HOTLINE

- *Phone 1-800-827-1000*

→ For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC)

- *Online: https://reportfraud.ftc.gov*

Common Schemes – **Promise to Address Comprehensive Toxins (PACT) Act**

U.S. Department of Veterans Affairs

Choose VA

Scammers are taking advantage of new opportunities to commit fraud. There's been an increase in PACT Act-related phishing (email), vishing (phone), and social media scams targeting Veterans to access their PACT Act benefits or submit claims on their behalf.

Veterans should be cautious of anyone who guarantees a lucrative financial benefit or service.

Tips to Avoid PACT Act Scams

Do's

- ☐ **Apply directly to VA. Veterans may submit applications for VA benefits securely https://www.benefits.va.gov/BENEFITS/Applying.asp via https://www.va.gov or in person at any regional office. Veterans may file claims directly with VA and VA will help gather the necessary evidence. There are no costs or hidden fees to apply.**
- ☐ **Be cautious of companies who advertise VA benefits can only be obtained with their help. These companies may no be recognized by the VA and may be attempting to charge illegal fees.**
- ☐ **Be cautious of aggressive companies who may try to pressure you to sign their contract through frequent communications or by insisting that "you must act now or lose your chance for benefits."**
- ☐ **Be cautious of companies who claim to be contacting you on behalf of the VA or to have a special relationship with the VA. Contact the VA at 1-800-827-1000 if you are unsure about the authenticity of any messages received.**
- ☐ **Call the VA if you have questions or think benefits for a loved one are not correct.**
- ☐ **Make sure your family is aware of your end-of-life decisions and that you have documented those wishes.**
- ☐ **Check for "https://" at the start of website addresses.**
- ☐ **Enable multi-factor authentication on all accounts.**
- ☐ **Work with Veteran service providers you already know.**
- ☐ **Validate: If you are interested in working with a Veteran Service Organization (VSO), agent, or attorney, use the Office of General Counsel Accreditation tool to confirm and validate their credentials. https://www.va.gov/ogc/apps/accreditation/index.asp**

Don'ts

- ☐ Do not sign a contract agreeing to pay an unauthorized company a percentage of your benefit payment in exchange for their assistance with your VA claim.
- ☐ Do not sign a blank form for someone else to complete later. Always review the completed form before signing and keep a copy for yourself.
- ☐ Do not be fooled by companies who advertise they have special relationships with medical professionals and can guarantee your benefits award. If they are defrauding the Federal government, you could be held responsible for paying those benefits back.
- ☐ Do not provide your social security number, medical records or other personally identifiable information to anyone offering claims

assistance before confirming their credentials using the Office of General Counsel accreditation tool: https://www.va.gov/ogc/apps/accreditation/index.asp.

- ☐ Do not sign forms that are not VA generated or third-party authorization for someone to provide "behind-the-scenes" claims assistance.
- ☐ Do not provide personal, benefits, medical, or financial details online or over the phone. Federal agencies will not contact you unless you make a request.
- ☐ Do not click on online ads or engage with social media that seem suspicious.

- Submit any suspected fraud to ReportFraud.ftc.gov.

Visit the Cybercrime Support Network for additional resources to help Veterans, service members, and their families combat cybercrime.

REPORTING INFORMATION

FOR SUSPECTED VA BENEFITS FRAUD CALL THE VA BENEFITS HOTLINE

- *Phone 1-800-827-1000*

→ For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC)
- *Online: https://reportfraud.ftc.gov*

Common Schemes – **Employment: Business & Job Opportunities**

U.S. Department of Veterans Affairs

ChooseVA

Employment scams may include business or job opportunities such as offers to start new businesses or work-from-home. The scammer then uses the illusion of prospects to manipulate and/or steal from you.

Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- If it sounds too good to be true, it typically is.
- Bogus company sending a large check for you to buy something like computer equipment and then asks you to repay the excess funds via a wire transfer service, cryptocurrency or gift cards.
- Charging a fee for assisting you with completing an employment application.
- Offered wage is higher or lower than the average wage for that job. Check current wages on the internet.
- The link for submission of your application is not connected to the company's official career website, or the job posting is not on the company's official job page or a related official recruitment website.

Do's

Before you accept a job offer, and certainly before you pay for one, take these steps to protect yourself from job scams:

- Do an online search. Look up the name of the company or the person who's hiring you, plus the words "scam," "review," or "complaint." You might find out they've scammed other people.
- Talk to someone you trust. Describe the offer to them. What do they think? This also helps give you vital time to think about the offer.
- Read the fine print. If a job ad looks too good to be true, it is most likely a scam.
- Ask questions about the job description. Scammers will post vague language about the prospective job.
- Check to make sure the recruiter that calls you is who they say they are by doing an online search or calling the company directly.
- Be cautious of conducting interviews through Google Hangouts, Telegram App, Texting apps (TextFree app, TextNow app, WhatsApp).

Don'ts

- ☐ Do not provide personal information during an interview. i.e., Social Security number, driver's license number or bank account information.
- ☐ Do not pay for the promise of a job. Legitimate employers, including the federal government, will never ask you to pay to get a job. Anyone who does is a scammer.
- ☐ Do not bank on a "cleared" check. No legitimate potential employer will ever send you a check and then tell you to send on part of the money or buy gift cards with it. That's a fake check scam. The check will bounce, and the bank will want you to repay the amount of the fake check.

REPORTING INFORMATION

FOR ALL NON-VETERAN AFFAIRS RELATED FRAUD, REACH OUT TO THE FEDERAL TRADE COMMISSION (FTC)

- *Online: https://reportfraud.ftc.gov*

Common Schemes – **Education**

Education scams are when a fraudulent company or individual is misleading or deceiving students. Scammers will also attempt to charge Veterans for services that are available for free.

U.S. Department of Veterans Affairs

ChooseVA

Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- Charging for assistance in filing claims.
- Misreporting educational hours.
- Charges for books and supplies for more than market value.
- Advertise a lower tuition rate than they are billing VA for Veteran student enrollments.
- Instructors teaching the classes are not those advertised.
- Payment is offered to students who register but not asked to attend classes.
- For-profit schools may overpromise education or job opportunities.
- Students report that they only need to sign-in but not attend classes.
- Deceptive advertisements offering debt relief for fees.
- The school has a lack of written policies and procedures or has been unable to produce records (sometimes claimed as lost or destroyed).
- Lying on the Free Application for Federal Student Aid (FAFSA®) form or other federal student loan form in order to qualify for more financial aid.
- Lying on any student loan application/form (Parent Loan for Undergraduate Students (PLUS) Application, Master Promissory Note (MPN), Loan Consolidation, etc.)

Tips to Avoid Scams – Education Do's

- ☐ Apply directly to VA. Veterans may submit applications for VA benefits securely https://www.benefits.va.gov/BENEFITS/Applying.asp via https://www.va.gov or in person at any regional office. Veterans may file claims directly with VA and VA will help gather the necessary evidence. There are no costs or hidden fees to apply.
- ☐ Do confirm that the school is approved and use extra caution and ask multiple sources when considering a for-profit school. Research colleges and employers approved for the GI Bill by using the GI Bill Comparison Tool. https://www.va.gov/education/gi-bill-comparison-tool
- ☐ Do work with a Veterans representative at prospective colleges or universities for the student enrollment process and experience.
- ☐ Only trust reliable sources. i.e., https://www.studentaid.gov or https://www.consumerfinance.gov/consumer-tools/student-loans/
- ☐ Be vigilant if anyone requests payment for services.
- ☐ Confirm payments received are accurate.

- ☐ Do call the VA if a school asks you to register and says you are not required to attend classes or if you the instruction you receive is not what was promised/advertised.
- ☐ DO sign up at https://fsapartners.ed.gov/subscriptions/ to be notified when the Student Loan Debt Relief application becomes available.
- ☐ DO create an Federal Student Aid (FSA) ID at https://www.studentaid.gov. You will not need it for the debt relief application but having an FSA ID can allow you to easily access accurate information on your loan and make sure FSA can contact you directly, helping you equip yourself against scammers trying to contact you. Log in to your current account on https://www.studentaid.gov and keep your contact info up to date.
- ☐ DO make sure your loan servicer has your most current contact information. If you don't know who your servicer is, you can log into StudentAid.gov at https://studentaid.gov/fsa-id/sign-in/landing and see your servicer(s) in your account.

Don'ts

- ☐ **Do not pay anyone to help you apply for loan forgiveness.** Nobody can get your loans forgiven faster, even if you pay them. This program is completely free — and the only way to apply is at Federal Student Aid at https://www.studentaid.gov
- ☐ **Do not share your VA, Social Security number, FSA ID login information or any other government benefits.** If anyone says they need your information to help you, that's a scam. Don't do it. They can cut off contact between you and your servicer — and even steal your identity.
- ☐ **Do not trust someone who contacts you saying they're affiliated with the Department of Education.** Scammers use official-looking names, seals, and logos. They promise special access to repayment plans.
- ☐ **Do not sign a blank form for someone else to complete later.** Always review the completed form before signing and keep a copy of the completed form for recordkeeping purposes.
- ☐ **Do not ever give personal or financial information to an unfamiliar caller.** When in doubt, hang up and call your student loan servicer directly. You can find your federal student loan servicer's contact information at https://Studentaid.gov/manage-loans/repayment/servicers
- ☐ **Do not refinance your federal student loans unless you know the risks.** If you refinance federal student loans that are eligible for debt relief into a private loan, you will lose out on important benefits like one-time debt relief and flexible repayment plans for federal loans.

REPORTING INFORMATION

FOR SUSPECTED VA BENEFITS FRAUD CALL THE VA BENEFITS HOTLINE

- *Phone 1-800-827-1000*

→ For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC)

- *Online: https://reportfraud.ftc.gov*

Common Schemes – **Memorialization – End of Life**

U.S. Department of Veterans Affairs

ChooseVA

Memorialization (End of Life) scams are when a fraudulent company or individual provides a service that is not in the best interest of the individual. The scammer will often offer to provide services with high rates and fees.

Common Schemes

You should be aware of these schemes in case someone asks you to participate, or in case you see fraudulent activity. Indicators of potential fraud include the following:

- Be on the lookout for solicitations claiming to be either authorized and/or endorsed by the government. Government agencies generally do not endorse private sector products and services nor charge for benefits that are already free or low-cost.
- Upselling memorial services and funeral expenses that are not as advertised.
- Care providers learn bills and/or Explanation of Benefits (EOBs) are being issued under their names when they did not provide the service.
- False advertisements that benefits have changed when they really haven't. Double check with your VA representative if you are not expecting benefit changes.
- Scammers offering help advocating for your loved one's wrongful death.
- Be wary of organizations that charge for a "full financial review" before helping file claims. Assistance is available for free to apply for VA Dependency and Indemnity Compensation (VA DIC) and VA Aid and Attendance benefits and Housebound allowance. For more information, visit U.S. Department of Veterans Affairs, Pension Benefits https://www.va.gov/pension/

Do's

Before you accept a job offer, and certainly before you pay for one, take these steps to protect yourself from job scams:

- ☐ Apply directly to VA. Veterans may submit applications for VA benefits securely https://www.benefits.va.gov/BENEFITS/Applying.asp via https://www.va.gov or in person at any regional office. Veterans may file claims directly with VA and VA will help gather the necessary evidence. There are no costs or hidden fees to apply.
- ☐ Validate: If you are interested in working with a Veteran Service Organization (VSO), agent, or attorney, use the Office of General Counsel Accreditation tool to confirm and validate their credentials. https://www.va.gov/ogc/apps/accreditation/index.asp
- ☐ Call the VA if you have questions or think benefits for a loved one are not correct.
- ☐ Make sure your family is aware of your end-of-life decisions and that you have documented those wishes.

Don'ts

- ☐ Do not sign a blank form for someone else to complete later. Always review the completed form before signing and keep a copy of the completed form for recordkeeping purposes.
- ☐ Do not provide your Social Security number, medical records, or other personally identifiable information to anyone offering claims assistance before confirming their credentials using the Office of General Counsel Accreditation tool. https://www.va.gov/ogc/apps/accreditation/index.asp
- ☐ Do not sign a contract agreeing to pay an unauthorized company a fee to help with VA claims. There are Veteran Service Organizations (VSOs), accredited agents, and attorneys that can help Veterans file claims for benefits.

REPORTING INFORMATION

FOR SUSPECTED VA BENEFITS FRAUD CALL THE VA BENEFITS HOTLINE

- *Phone 1-800-827-1000*

→ For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC)

- *Online: https://reportfraud.ftc.gov*

Resources

U.S. Department of Veterans Affairs Fraud Resources
- For suspected VA Healthcare related fraud call the VHA OIC Helpline 1-866-842-4357.
- For suspected VA Benefits fraud call the VA Benefits Hotline - 1-800-827-1000.

U.S. Department of Veterans Affairs
- Veterans Service Organizations (VSO)
- VSO's may offer free help to Veterans applying for VA benefits.
- More information is available at: https://www.ebenefits.va.gov/ebenefits/vso-search

Federal Trade Commission (FTC)
- https://reportfraud.ftc.gov

Consumer Finance Protection Bureau (CFPB)
- https://www.consumerfinance.gov/complaint
- https://www.consumerfinance.gov/consumer-tools/fraud/
- (855) 411-2372

Military Consumer
- https://www.militaryconsumer.gov/protect
- (877) 382-4357

National Do Not Call Registry
- Register your phone number(s) at https://www.donotcall.gov
- (888) 382-1222

Social Security Administration (SSA)
Office of the Inspector General
- Report Fraud https://oig.ssa.gov/report
- Report a Social Security-related scam https://www.ssa.gov/scam/

Federal Bureau of Investigation
- Internet Crime Complaint Center
- https://www.ic3.gov/
- File a complaint https://www.ic3.gov/Home/ComplaintChoice

Better Business Bureau
- https://www.bbb.org/
- File a complaint https://www.bbb.org/file-a-complaint

Federal Communications Commission (FCC)
- https://www.fcc.gov/
- File a complaint https://consumercomplaints.fcc.gov/hc/en-us
- (888) 225-5322

The United States Department of Justice (DOJ)
- File a complaint https://www.justice.gov/criminal-fraud/report-fraud

Department of Defense

Office of Financial Readiness, Consumer Protection at: https://finred.usalearning.gov/

National Resource Directory at: https://www.nrd.gov/

Internal Revenue Service (IRS)
- https://www.irs.gov/identity-theft-central
- https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
- https://www.irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity
- If you believe you have been a victim of identity theft, call the IRS Identity Theft Protection Unit at 1-800-908-4490