PAvets@attorneygeneral.gov. **Standard procedure if your personal information has been compromised...**

- Contact the police
- Immediately close all accounts
- Open new accounts with different pin numbers or passwords
- Report it to the Office of Attorney General: 1-800-441-2555; and the Federal Trade Commission: 1-877-ID-THEFT (438-4338)
- Start a secure file of all correspondence
- Contact 3 major credit bureaus and place a "fraud alert" on your report

Equifax: 1-800-525-6285, www.equifax.com Experian: 1-888-397-3742, www.experian.com TransUnion: 1-800-680-7289, www.transunion.com

Almost 80% of veterans have been in the last five years

Safeguarding your passwords:

- 1. Create password with a minimum of 12 characters
- 2. Mix letters, numbers and special characters
- 3. Consider a unique phrase, add numbers at the beginning and end
- 4. Never write your password down or store it on your computer
- 5. Change your password regularly, and immediately if you suspect someone has guessed it

Annual Credit Reports –

Consumers are eligible to one free credit report from each bureau per year, so you can stagger requests and receive a report every four months.

To get your free credit report:

- Log on www.annualcreditreport.com
 - Call 1-877-322-8228 or
 - Write Annual Credit Report request P.O. Box 105283 Atlanta, GA 30348-5283

Veterans Crisis Hotline: **1-800-273-8255**

Combating Veteran Scams and Fraud



Michelle A. Henry Pennsylvania Attorney General

Office of Military and Veteran Affairs www.attorneygeneral.gov Pavets@attorneygeneral.gov **717-783-1944**



Pennsylvanians have a proud history of military service. Today, over 830,000 U.S. veterans call Pennsylvania home, and there are over 2,200 organizations that serve veterans all across our Commonwealth.

In gratitude for their service, veterans have access to a wide range of benefits and services to support them and

their families after they take their uniforms off. Unfortunately, as a result, veterans and those who support them are often the targets of scams and fraud, including identity theft. According to a survey by AARP, veterans are twice as likely to be targeted by con artists and fall victim to fraud compared to non-veterans.

Our veterans and their families have sacrificed to serve our country. It's the least we can do to stand up for them, prevent them from being scammed, and take down anyone who tries to do so. That's why my Office of Military and Veterans Affairs works every day to help veterans by investigating fraud and scams.

You've done your part to serve your country and community; here in my Office, we're proud to take our turn to serve you.

If you or someone close to you is a veteran who may have been victimized by a scam when filing a claim for benefits, please reach out to us file a complaint either online, by email, or by phone.

Milla

Scammers and identity thieves target veterans because of the additional government benefits they receive. They often appeal to vets' patriotism or exploit elements of a military lifestyle, like frequent travel, to steal their hard-earned benefits.

Best Practices for Veterans

- Don't pay for a service that is free. It is illegal for an accredited veterans' service officer to accept any form of payment from veterans.
- Be cautious when you receive an unsolicited offer for services from an unknown source.
- Do research on the U.S. Department of Veterans Affairs (VA) website into both the entity you are considering working with and the claims process.
- Follow recommendations and referrals of fellow veterans who have had successful experiences filing VA benefit claims with specific veterans' service organizations. Always ask to see the representative's accreditation credentials.

Scams Targeting Veterans

The following are some of the most common scams that target veterans that are currently in the United States:

- Tax Reduction linked to military service
- U.S. Department of Veteran Affairs Disability Payout
- U.S. Department of Veteran Affairs Pension Poaching
- U.S. Department of Veteran Affairs Home Loans
- Education Benefits
- Military Record Copies or Updates
- Bogus Classified Advertisements
- Bogus Veteran Charities
- Military Discounts
- Military Impersonation/Stolen Valor

While each of these scams has unique elements, they share common themes and tactics. They typically start with a contact you didn't initiate, like an unexpected phone call, email or text message or contact through social media. The communication urges your immediate action, to help another veteran in need or protect yourself. The scam concludes with requesting money or your personal/financial information.

Combatting Veteran Scams

- The Internal Revenue Service, U.S. Department of Veteran Affairs and other government agencies will not initiate contact with you through phone calls, emails, text messages through social media.
- Do your research if it sounds too good to be true, it probably is!
- Don't donate over the telephone or computer.
- Don't send upfront payments, especially using wire transfers or providing gift card codes for charitable donations, goods or services.
- Verify that charities are registered in Pennsylvania prior to donating by contacting the Bureau of Charitable Organizations at the Pennsylvania Department of State.
- Impersonating a veteran or member of armed services is a crime.
- If you suspect that someone is misrepresenting their status as a Service member or a Veteran or the nature of their goods or services, or you are a victim of a veteran scam, file a complaint with the Office of Attorney General's Military and Veterans Affairs by calling 717-783-1944 or emailing