Privacy Basic Training for Armed Forces:

Responding to Identity Theft

Have you recently received any unexpected credit cards or account statements in the mail? Have the bills you expected to get in the mail stopped coming? Are you receiving calls or letters about purchases you did not make? Are you being rejected for credit for no apparent reason? These are all signs that you may have fallen victim to identity theft.

Active military personnel, veterans and their families can be particularly vulnerable to identity theft and fraud due to nonstandard work schedules, lengthy absences from home, frequent relocations and duty assignments to remote locations.

To honor the unselfish service of our armed forces, the New York State Consumer Protection Board (CPB) has developed this resource. The CPB suggests the following tips to help prevent our service men and women from falling victim to identity theft and to assist in mitigating the consequences of identity theft:

Prevention

- Keep your personal information in a secure place, especially if you live in barracks or with roommates.
- Cross shred all documents containing your personal information before you discard them.
- Protect your Social Security number. Provide it to others only if absolutely necessary or ask to use another type of identification instead.
- Safeguard your military ID. Keep it with you or in a locked container at all times.
- Safeguard your medical records and dependent information.
- Refrain from providing your personal information on the phone, through the mail and e-mail, or over the Internet.
- Never lend your credit cards or account information to anyone for any reason.
- Never click on links in unsolicited e-mails even if they appear to come from businesses you know. Instead, type in the web address you know to be correct, and contact the business through that address.
- Use security software to protect your computer and keep it up-to-date.
- Don't choose an obvious online password such as your birth date, your mother's maiden name, the last four digits of your Social Security number or your military ID card number.
- Don't let mail pile up unattended if you can't access it. Use a mail stop or P.O. Box, or have someone you trust hold your mail while you are away.
- Check your credit report regularly. The law requires each of the three major credit reporting agencies -- Equifax, Experian, and TransUnion -- to give you a free copy of your credit report every year if you make your request through Annual Credit Report Request Service. See contact information below.
- Regularly monitor your financial accounts and billing statements for suspicious activity.

Provided By:

NYS Consumer Protection Board

Advocating for and Empowering NY Consumers

www.nysconsumer.gov ~ 1-800-697-1220

New York State Division of Veterans' Affairs

www.veterans.ny.gov ~ 1-888-838-7697

- Consider placing an active duty alert on your credit report if you are deployed away from your usual duty station and do not expect to seek new credit while you are deployed. An active duty alert requires creditors to take steps to verify your identity before granting credit in your name.
  - An active duty alert is effective for one year, unless you ask for it to be removed sooner.
  - If your deployment lasts longer than a year, you may place another alert on your report.
  - To place an active duty alert, or to have it removed, call the toll-free fraud number of one of the three major credit reporting agencies. The agency you call is required to contact the other two.
  - The law allows you to use a personal representative to place or remove an alert.
  - When you place an active duty alert, your name will be removed from the marketing list of the nationwide consumer reporting agencies' for prescreened or "preapproved" offers of credit and insurance for two years – unless you have previously requested to be permanently removed from such lists.
- Be aware of data breaches which occur to organizations that have your personal identifiable information. If you receive a data breach notice, follow the identity theft precautions provided in the "Response Tips" section below.
- Ask and read about information privacy policies when seeking veteran, health and counseling services.

Response

- Consider placing a "Fraud Alert" or "Credit Freeze" on your credit reports, and review the reports carefully. Placing a fraud alert entitles you to additional free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.
- Close any accounts that have been tampered with or established fraudulently. Submit an ID Theft Affidavit to support your claim.
- Explain the situation to your commanding officer. You don't want your C.O. taken by surprise if contacted by creditors looking to collect on charges made by the identity thief. You may want a referral to a legal assistance office.
- File a police report. File a report with military law enforcement and the local police (if you are in the United States). Their reports will help you with creditors who may want proof of the crime.
- Report scam/fraud complaints to the special FTC site: The FTC's Consumer Sentinel/Military. This site provides a secure online database for the military community to report concerns about identity theft, deceptive lending or mortgage practices, debt collection problems, phone frauds, or other scams.

Contact information

To request your free annual credit report:

Visit: www.AnnualCreditReport.com
Call: 1-877-322-8228
Write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281

For placing a fraud alert or credit freeze, call:

- Equifax: 1-800-525-6285
- Experian: 1-888-EXPERIAN (397-3742)
- TransUnion: 1-800-680-7289

November 2009

A Product of the NYS Consumer Protection Board's Identity Theft Prevention and Mitigation Program