

Red Flags of Identity Theft -

If you experience one or more of the following indicators, an identity theft may have occurred.

- Errors on your bank account, credit card or other account statement.
- Mistakes in the explanation of medical benefits of your health plan.
- Your regular bills or account statements don't arrive on time.
- You receive bills or collection notices for products or services you never received.
- You receive calls from debt collectors for debts that don't belong to you.
- You receive a notice from the IRS that someone used your Social Security number.
- Mail, email or calls about accounts, or jobs in your minor child's name.
- Unwarranted collection notices on your credit report.
- Businesses decline your checks.
- You're unexpectedly denied a loan or job.

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

Safeguarding your password:

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

P E N N S Y L V A N I A OFFICE OF ATTORNEY GENERAL



Combating ID THEFT



Office of Military and Veteran Affairs

www.attorneygeneral.gov

Pavets@attorneygeneral.gov

717-783-1944

BRUCE R. BEEMER
Attorney General



Combating ID THEFT

Each year more than 10 million Americans have their personal information -- including name, Social Security number, or bank account or credit card numbers -- stolen. Scammers use this information to open phony credit cards, bank or utility accounts, and sometimes to use the victim's identity to secure benefits such as health care or government assistance. Having your identity stolen can harm your finances and credit history, damage your reputation, and prevent you from getting a job. Recovering from identity theft can be a frustrating, costly and time-consuming process for consumers and businesses.

Sadly, veterans and military members are targeted by identity thieves who seek to appeal to their patriotism, pilfer their hard-earned benefits or exploit elements of a military lifestyle, like frequent travel. In fact, according to the Federal Trade Commission, ID theft was the number one complaint from military consumers.

Scammers operate in a variety of ways, and as Attorney General I'm committed to educating every Pennsylvanian about preventing ID theft and protecting citizens from those who perpetrate it. This brochure includes tips on how to prevent ID theft, recognize the signs that your personal information may have been compromised, and the steps to take if you've had your identity stolen.

Keeping your personal information secure is the most important step in combating ID theft and the Office of Attorney General is here to help.

Bruce R. Beemer
Attorney General

ID Theft Tactics

There are several methods scammers use to steal your information. Some are sophisticated, using mail, phone or online scams. Others include taking advantage of documents left unattended in open view such as taking mail from an unsecured mailbox or going through the trash. Scammers will "dumpster dive" to steal personal information. Some use old school tactics like pickpocketing, stealing records or keeping a restaurant customer's credit card information. In fact 55 percent of ID theft is perpetrated by someone the victim knows.

- Use ATMs inside banks and stores. ATMs located outside can be tampered with more easily.
- Never give out banking, credit card or Social Security numbers to people who initially contact you by phone or email. Look up the caller's information on your own to confirm the request.
- Don't complete unsolicited surveys or popups.
- Verify a charity before you donate -- in Pennsylvania, check with the Department of State.
- Caller ID displays can be manipulated by thieves; don't trust that they're correct.
- Make shredding materials with your personal information standard procedure. A crosscut shredder is best.
- Be careful of information you keep on iPads, smartphones, netbooks, laptops, etc. because they're easily stolen and compromised.
- Steer clear of public or shared photocopiers because they have a digital memory; instead use a home scanner, or if using a public copier use correction tape to cover personal data and handwrite the information on copies.
- Opt out of junk mail by logging onto www.dmachoice.org; and for unsolicited credit card offers www.optoutprescreen.com, or call 1-888-5-OPT-OUT.
- Use a mailbox that locks.
- Keep a security box in your home and affix it to a closet wall or floor so it can't be removed easily.
- Always verify websites, don't trust a link that comes in an unsolicited email.
- Never pay taxes or a fee in order to claim a prize. In fact, a random phone call, letter or email indicating you have won a prize is most likely a hoax to scam you.