Each year, more than 15 million Americans have their personal information stolen, including their name, Social Security number, bank account, or credit card numbers. Scammers use this information to open credit cards or bank accounts, pay for utilities, and steal benefits such as health care or government assistance. In fact, identity thieves steal over $16 billion from unsuspecting Americans every year.

Having your identity stolen could cost you money, damage your credit score, affect your reputation, and even prevent you from getting a job. Recovering from identity theft can be frustrating, expensive, and time-consuming.

Scammers operate in a variety of ways. As Attorney General I'm committed to stopping identity theft and prosecuting anyone who perpetrates it. But the best way to fight it is to avoid it in the first place. This brochure includes tips on how to prevent identity theft, how to recognize the signs that your personal information may have been compromised, and the steps to take if you think your identity has been stolen.

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 reports, visit www.annualcreditreport.com, call 1-877-322-8228 or write to Annual Credit Report Request at P.O. Box 105283, Atlanta, GA 30348-5283.

Personal Information Compromised?

- Contact the police
- Immediately close or freeze all accounts
- Open new accounts with different pin numbers or passwords
- Report it:
  Office of Attorney General: 1-800-441-2555
  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:

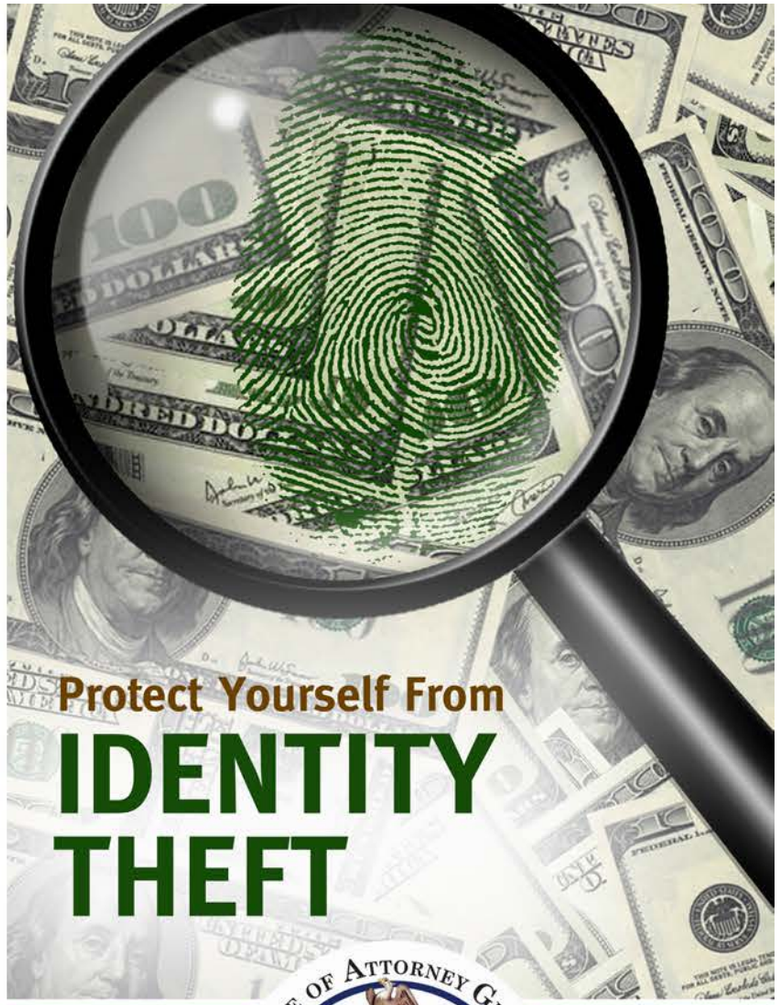
  Equifax: 1-800-525-6285, www.equifax.com
  Experian: 1-888-397-3742, www.experian.com
  TransUnion: 1-800-680-7289, www.transunion.com

Consumer Protection Helpline:
1-800-441-2555

www.twitter.com/PAAttorneyGen

www.facebook.com/PAAttorneyGen

www.attorneygeneral.gov



Protect Yourself From IDENTITY THEFT

Office of Attorney General
Commonwealth of Pennsylvania

Josh Shapiro
Pennsylvania Attorney General

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

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

Identity Theft Prevention Tips:

- **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.
- **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.
- **Shred materials with your personal information.** 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; 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 fees 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.

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.
- You receive 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.