# Fraud

Identity theft occurs when your personal information (like your name, social security number, birth date, or credit card information) is stolen and used without your knowledge to commit fraud or other crimes. It can destroy your credit and good name. It is one of the fastest growing crimes in the United States.

**Dos and Don'ts for Protecting Your Identity**

- Never disclose your full social security number over the phone.
- Avoid paper statements by requesting secure e-statements instead.
- Shred documents that contain sensitive information (your name, birth date, account numbers, social security number).
- Avoid paying bills (or using your sensitive information) online while using an unsecured Wi-Fi network, like one at a coffee shop or a hotel.
- Don't carry your social security card in your wallet.
- Never give out any personal information over the phone or internet unless you know who you are dealing with.
- Never click on a link in an unsolicited email. Instead, type in the web address that you know.
- Use firewalls, anti-spyware, and antivirus to protect your home computer and keep them up to date.
- Keep your personal information secure at home.
- Trust your gut!
- Think before you click!

**Passwords**

- Set a password on all of your devices. It is quick and easy and goes a long way to protect your information.
- Choose unique passwords that include a combination of letters, numbers, and symbols.
- The longer the password, the harder to crack. Phrases are a good idea.

- Don’t use obvious passwords.
- Avoid using the same passwords for different accounts.
- Never share your passwords with anyone.

**Ways Your Identity Can Be Stolen**

- **Phishing** is when identity thieves try to steal your information by pretending to be your bank or another company you deal with. They send you an unsolicited email that may appear to be legitimate to try to get you to reply and reveal your personal information. These emails are usually fake lookalikes. Only respond if you feel the email is truly authentic. If you are not sure, call the company to verify its legitimacy. Do NOT call the number in the message as it could be fake and lead you straight to the thief. Look up the company in the phone book or on www.whitepages.com.
  By the way, most businesses wouldn’t be asking you for your personal information because they should already have it from when you first set up an account with them.
- **Skimmers** use cameras or extra parts installed on an ATM to steal your information. Avoid using secluded ATMs and always cover your PIN when typing it in.
- **Dumpster Diving** is an easy way for thieves to get your information! They can go through any public trash can looking for bills or other paper documents that could reveal your information.
- Thieves can also **fill out a change of address** form for you and have your mail redirected to them. Always pay attention to when your bills normally arrive.
- **Good old fashioned stealing** is still common with identity thieves. They steal your purse or wallet, phone, mail, or checks.
- **File sharing or peer to peer (P2P) sharing** is an easy way for a thief to get your bank account information when you download their app, screensaver, or ringtone. Only use reliable sources for downloads and never turn off your antivirus software. Be extremely cautious when you receive emails or popups with a link inviting you to view “shocking videos” or read the “latest

celebrity gossip". Resist these as they are usually scams with malicious links embedded in them.

- Cyber criminals can also **use fake mobile APPs** offered through the app stores. Once you've installed them, they can intercept your passwords. Only download from a reliable source.

**How to Know If You Are Being Scammed**

- Did you receive an online commission check that seemed too easy?
- Did you win an online prize but then were asked to return a portion of the winnings?
- Do you have to pay to receive an inheritance?

Assume that any offer that seems too good to be true usually is, especially if it is from an unknown person or business.

**Detecting Identity Theft**

- Self-detection is the key to the quickest recovery possible. Victims who discovered fraud on their own experienced less damage than others. If you wait for your bank to notify you, the damage is already done.
- Electronic monitoring of your accounts can help you detect fraud 18 days sooner than other methods. Frequently check your online banking statements for unauthorized charges.
- Sign up to receive email or text alerts that notify you of your account activity or account changes.
- The law requires that everyone have access to one free annual credit report from each of the three main credit reporting agencies (Transunion, Equifax, and Experian). You can request one report from all three agencies once a year. Or you can request three reports a year showing one from each agency.
- When checking your credit report, verify that all information is correct and no accounts have been opened without your knowledge. Free credit reports are available online at AnnualCreditReport.com.

**What to Do If You Detect Identity Theft**

1) Immediately notify your financial institution if you discover your wallet, checkbook, debit/credit cards, or other sensitive information has been stolen.
2) Report this to the Federal Trade Commission using their online complaint form. You will be given the option to receive an Identity Theft Affidavit. This document is critical to reducing your damage (paired with a police report).
3) File a police report. When you file, bring a copy of the Identity Theft Affidavit. Keep copies of both forms for insurance purposes.
4) Contact the 3 major credit reporting bureaus. Have them each place a fraud alert and a security freeze on your account. This must be renewed every 90 days. This stops anyone from viewing your credit report (or trying to make a purchase) without your knowledge. If any fraudulent accounts were opened in your name or any existing accounts were tampered with, have these accounts closed and get verification that the fraudulent charges were discharged. Keep copies of your documents and records of your conversations.
5) If your social security number was stolen, contact the Social Security Administration right away.

**Helpful Resources**

- Social Security Administration www.ssa.gov
- Federal Trade Commission www.idtheft.gov
- Federal Deposit Insurance Corporation www.fdic.gov
- Free Annual Credit report www.annualcreditreport.com
  Don't be fooled by lookalikes or other "free" credit report websites.