Protecting yourself from identity theft

- Destroy private records and statements. Destroy credit card statements, solicitations and other documents that contain any private information. Shred this paperwork using a "cross-cut" shredder so thieves can't find your data when they rummage through your garbage. Also, don't leave a paper trail; never leave ATM, credit card or gas station receipts behind.
- Secure your mail. Empty your mailbox quickly, lock it or get a P.O. Box so criminals don't have a chance to steal credit card offers. Never mail outgoing bill payments and checks from an unsecured mailbox, especially at home. They can be stolen from your mailbox and the payee's name erased with solvents. Mail them from the post office or another secure location.
- Safeguard your Social Security number. NEVER carry your card with you, or any other card that may have your number, like a health insurance card or school issued ID. Don't put your number on your checks; your SSN is the primary target for identity thieves because it gives them access to your credit report and bank accounts. There are very few entities that can actually demand your SSN - the Department of Motor Vehicles, for example. Also, SSNs are required for transactions involving taxes, so that means banks, brokerages, employers, and the like also have a legitimate need for your SSN.
- Safeguard your computer. Protect your computer from viruses and spies. Use complicated passwords; frequently update antivirus software and spyware. Surf the Web cautiously. Shop only at trustworthy web sites and be wary of obscure sites or any site you've never used before.
- Know who you're dealing with. Whenever you are contacted, either by phone or email, by individuals identifying themselves as banks, credit card or e-commerce companies and asked for private identity or financial information, do not respond. Legitimate companies do not contact you and ask you to provide personal data such as PINs, user names and passwords or bank account information over the phone or Internet. If you think the request is legitimate, contact the company yourself by calling customer service using the number on your account statement or in the telephone book and confirm what you were told before revealing any of your personal data.
- Take your name off marketers' hit lists. In addition to the national Do Not Call Registry (1-888-382-1222 or https://www.donotcall.gov), you also can reduce credit card solicitations for five years by contacting an opt-out service run by the three major credit bureaus: (888) 5-OPT OUT or https://www.optoutprescreen.com. You'll need to provide your Social Security number as an identifier.

- Guard your personal information. Ask questions whenever anyone asks you for personal data. How will the information be used? Why must I provide this data? Ask anyone who does require your Social Security number, for instance, cell phone providers, what their privacy policy is and whether you can arrange for the organization not to share your information with anyone else.
- Monitor your credit report. Each year, obtain and thoroughly review your credit report from the three major credit bureaus; Equifax (800-685-1111), Experian (883-397-3742) and TransUnion (800-680-4213) or at https://www.annualcreditreport.com) to look for suspicious activity. If you spot something, alert your card company or the creditor immediately.
- Review your bank and credit card statements carefully. Look for unauthorized charges or withdrawals and report them immediately. Make sure you recognize the merchants, locations and purchases listed before paying the bill. If you don't need or use department store or bank-issued credit cards, consider closing the accounts.
- Keep track of your billing dates/cycles and follow up with creditors if you don't receive bills/statements on time.
- Use random letters and numbers for passwords; don't use your mother's maiden name, your birth date, your graduation date, your social security number or any other familiar letters or numbers that can be associated with you as passwords.
- Be aware of how ID thieves can get your information. They get information from businesses or other institutions by stealing records, bribing employees with access to records, hacking into computers, rummaging through trash, posing as a landlord, employer, or someone else who may have a legal right to the information, stealing credit and debit card numbers as your card is processed by using a special information storage device ("skimming"), stealing wallets and purses containing identification and credit or bank cards, stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information or completing a "change of address form" to divert your mail to another location.

If your identity is stolen

- Contact the fraud departments of each of the three major credit bureaus. Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, along with a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts.
  1. **Equifax** To report fraud: 1-800-525-6285 (P.O. Box 740241, Atlanta, GA 30374-0241),
  2. **Experian** To report fraud: 1-888-EXPERIAN (397-3742) (P.O. Box 9532, Allen, TX 75013), and
  3. **TransUnion** To report fraud: 1-800-680-7289 (Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634)
- Contact the creditors for any accounts that have been tampered with or opened fraudulently. Speak with someone in the security/fraud department of each creditor, and follow up with a letter.

- If your Social Security number has been used illegally, contact the Social Security Fraud Hotline at 1-800-269-0271.
- File a report with Public Safety or the Police in the community where the identity theft took place. Get a copy of the police report in case the bank, credit-card company, or others need proof of the crime.
- Keep records of everything involved in your efforts to clear up fraud, including copies of written correspondence and records of telephone calls.

Computer scams

- Computer phishing is a crime. Phishers attempt to fraudulently acquire credit card details and other sensitive personal data via bogus emails or pop-up windows. It may look like a legitimate email from a legitimate institution, but beware of unsolicited requests for information.
- Financial or payment institutions will never request that you send them personal sensitive data via email or popup windows.
- If you receive a suspicious looking email from any bank, lending, or payment institution, it is best to delete and not respond. If, by coincidence, you have an account with the entity mentioned in the email, call your legitimate institution using the number on your physical bill or via the telephone book or through telephone information.
- Do not call the number that may be listed in the bogus email and do not click on any link listed in the bogus email.

Con Artists

- If a deal sounds too good to be true; it probably is.
- Be wary of any get rich quick scheme that wants you to invest money in advance.
- Never give out your credit card information over the phone unless you made the call.
- Do not buy on the spur of the moment; take time to research the company or product.
- If you are approached by a possible con artist or unauthorized solicitor, report the incident immediately to Public Safety or the Police.