Avoiding Identity Theft

Your identity is one of your most valuable assets. Protect yourself by knowing where your identity is exposed and how to defend it against identity thieves. A small effort on your part to change key habits and practices could keep you from becoming a victim.

What Identity Thieves Want Most

Anything you can do to keep criminals away from your personal data helps to reduce your risk of identity theft. Here's what identity thieves covet most:

- Your name, address, and phone number
- Your date of birth
- Your Social Security number (SSN)
- Your driver's license number
- Your credit card information
- Your bank account information
- Your mother's maiden name

Your SSN

Your Social Security number is the key to cloning your identity. Therefore:

- Do not carry your Social Security card in your wallet. Avoid carrying cards that display your SSN — notably health insurance cards, unless needed to receive care.

- Never give your SSN, credit card number, or other personal data by phone unless you have an existing relationship with the business or agency AND you initiated the call using a verified phone number. Always verify the other party's authenticity.

- Avoid including your SSN on applications. Provide it only when absolutely necessary — for tax, employment, and student records, stock and property transactions, and so on.

- If a government agency requests your SSN, look for an accompanying Privacy Act notice indicating whether a SSN is required, how it will be used, and what happens if you don't provide it.

Your Bank Accounts

- Frequent monitoring of your bank accounts will help to detect and stop fraud. Research indicates that the risk and size of fraud loss for consumers who frequently monitor their accounts online is lower than those who don't monitor accounts regularly online.

- Monitor and reconcile your check activity online by viewing checks that are clearing the account.

Reduce Paper Transactions

- Use online bill pay and e-bills to remove confidential information from the mail and improve tracking of payments.

- For all your financial accounts, enroll in online statements and choose to receive your monthly account statements online instead of receiving a monthly paper statement. Research indicates 10% or more of identity theft is caused by stolen mail or trash.

Mail and Marketing Lists

- Use a secure locking mailbox or a P.O. Box.
- Never place outbound mail in an open, unlocked mailbox. Never leave mail in your car. During long absences, have mail held at the post office or have a trusted neighbor pick it up.
- Investigate immediately if expected bills or statements from financial institutions do not arrive on time. Be especially vigilant in January and April when tax documents are sent.
- Never simply discard "pre-approved" credit offers you receive in the mail. Always shred them.
- To keep pre-approved credit offers from being sent to you, remove your name permanently from the mail offer lists by visiting www.optoutprescreen.com. You can also opt out by calling 1.888.5OPT.OUT (1.888.567.8688), but only for a five-year period.
- Add your name to the National Do-Not-Call Registry at www.fcc.gov/cgb/donotcall, as well as to your state's Do-Not-Call list (if it has one). Add your name to name-deletion lists used by nationwide marketers at www.dmaconsumers.org/consumerassistance.html.
- Whenever possible, say "No" to the sharing of your data by selecting “Opt Out” with credit card companies, and insurance or investment firms.

Trash and Shredding

- Shred anything that contains your name, address, or other sensitive data before discarding, using a crosscut shredder — including invoices, receipts, statements, personalized pitch letters and envelopes, catalogs, and pre-approved credit offers.
- Don't discard sensitive documents at work unless you're sure they'll be shredded properly.
- Take your trash out immediately before it is due to be collected. Don't give identity thieves time to go through your trash.

Your Checks

- Never let merchants write your SSN on your checks. It's illegal in many states, and it puts you at risk.
- Do not have your SSN, driver's license number, or home phone number printed on your checks. If you have a P.O. Box, use that instead of your home address.
- Pick up new checks at the bank instead of having them mailed to your home address.
- Don't leave outbound envelopes containing payments in a home or office mailbox for pickup, in a car, or in any other place where they might be stolen. Checks can be altered and cashed, and provide the thief with your account information.

Your Wallet or Purse

At work, always store your wallet or purse in a safe place. Avoid carrying the following items:

- Your Social Security card (or your dependents')
- Your birth certificate
- Your passport
- Your military identification card
- A driver's license or insurance card with your SSN (or that of a family member)
- A list of your banking information (PINs, logins, passwords, or account numbers)
- Paychecks or pay stubs
- Deposit slips
- More than two credit or debit cards
- Receipts with your full credit card number displayed
- Any card that might store your SSN or other sensitive data on a magnetic stripe, such as a gas card, electronic hotel key, or employee ID

Credit, Debit, and ATM cards

- If a new or reissued credit card that's been mailed to you does not arrive on time, contact the issuer immediately.

- Minimize the number of credit cards you use, and carry only one or two at a time. Cancel unused accounts to reduce your exposure. However, be aware that canceling credit cards may affect your credit score adversely.

- Review your credit card statements, bank statements, and phone bills (including mobile phones) carefully each month for unauthorized use.

- Keep a list or photocopies of credit cards, bank accounts, and investments in a secure place (not your wallet or purse). Include account numbers, expiration dates, and phone numbers for customer service and fraud departments, so you can contact them quickly

Credit Reports and Credit Files

- Check your credit reports as frequently as possible, at least twice a year. Under the FACT Act, U.S. consumers are entitled to one free credit report each year from each of the three major credit bureaus. For details, visit www.annualcreditreport.com.

- Enroll in credit monitoring to track changes to your credit file. Enroll in fraud monitoring (non-credit database monitoring) to be warned of attempts to alter or acquire your identity data.

- Check your Social Security Statement each year for signs of fraud. The Social Security Administration mails this statement to adult SSN holders about three months before their birthdays.

Shopping and Application Forms

- Never toss credit card receipts into a public trash container. Always take them with you and shred them at home. Carry receipts in your wallet, not in the bag, so you don't mistakenly throw them out.

- When signing a credit card receipt, note whether your entire account number is displayed, or merely the last four digits. If the entire number shows, cross it out before leaving the signed receipt behind.

- When paying a bill with a credit or debit card, always keep the waiter, cashier, or bartender in view. Pocket-sized "skimming" devices can capture your credit card information for later use.

- When filling out applications for loans, credit, mobile phones, or other services, find out how the company stores and disposes of your data. If you aren't convinced that your information is safe, take your business elsewhere. Some auto dealerships, department stores, car rental agencies, and video stores treat customer applications carelessly.

Computers and Networks

- Install a firewall on your home computer to keep hackers out — especially if you connect to the Internet by DSL or cable modem. Install virus protection and keep it updated. Some viruses are designed to send sensitive data to identity thieves from your computer.

- Before disposing of a computer or hard drive, remove data using a strong "wipe" utility program. Do not rely on the "delete" function to remove files containing sensitive information.

- If possible, encrypt sensitive data that is sent or stored in digital form.

- Always store personal files and data securely in your home, especially if you have roommates, employ outside help, or have service work done in your home. (This applies to paper as well.)

Passwords and PINs

- Never use the last four digits of your SSN, your mother's maiden name, your birth date, your middle name, your child's name, your pet's name, or anything else that's easily discovered or guessed. If your financial institution uses the last four digits of your SSN as your default PIN, change it.

- Memorize all your passwords. Combine letters and numbers and change your passwords frequently. Don't record them on anything you carry in a wallet or purse. Ask financial institutions to add extra security to your account by requiring an additional code or password.

- Password-protect computer files that contain sensitive personal or account data.

- Shield your hand at an ATM or when making long distance calls with a phone card. Shoulder surfers may be nearby with binoculars or cameras. Avoid giving personal data by phone in a public place.

Web Sites and email

- Do not provide credit card numbers or personal information on any web site if you aren't sure the site is authentic. Choose companies with secure transactions and strong privacy and security policies.

- Never open spam and other email from unknown sources — it may contain viruses or other programs that make your computer vulnerable to intrusion.

- Never click on a link in an email claiming to come from a financial institution or business, and never provide personal or account data in response. The email may be a fake sent by "phishing" scammers.

- When entering personal information online, even on well-known web sites, watch for signs that you've been redirected to a "cloned" replica site where your data can be captured without your knowledge (a fraud technique called "pharming"). Such signs include odd error messages, unexpected page design or content, or other strange site behavior.