Identify Theft Prevention: Tips & Resources

Protect Your Social Security Number

- Don't carry your Social Security card in your wallet and only give your Social Security Number (SSN) when absolutely necessary. Ask why a SSN is needed, who has access to it, and how it will be kept confidential.
- Don't print your SSN or driver's license number on your checks and use only the last four digits when writing checks.

Destroy Documents You Don't Need

- Shred outdated records including bank statements, credit applications, health insurance forms, prescription labels and paperwork, physician statements, etc., along with any receipts that show your credit card number.
- Find local shred-a-thon events in local media or from local/state government entities.

Safely Dispose of Old Electronics

- Make sure you have removed all of the personal information your old computer holds before you sell, donate or recycle it. For best results, use a wipe utility program that overwrites everything on the hard drive.
- Transfer phone books, contact lists, etc. to your new phone, and then wipe your old phone completely clean. Consult the owner's manual and/or your service provider for tips on how to remove all of your old data, histories, photos, etc.

Monitor Your Finances

- Limit the number of credit cards you carry and keep copies of credit cards (front and back) in a safe place in case they are lost or stolen
- Watch for missing bills and review your monthly statements carefully. Contact your creditors if a bill doesn't arrive when expected or includes charges you don't recognize.
- Review your health care bills and paperwork carefully for signs of medical identity theft. Contact your health plan if a document includes charges you don't recognize.
- Use automatic deposit for payroll and federal benefit checks. To sign up for automatic deposit of Social Security checks and other federal benefit payments, call (800) 333-1795 or visit https://fiscal.treasury.gov/GoDirect/
- Review your Social Security Earnings and Benefits Statement for errors in your yearly salary.
- "Opt out" of sharing your nonpublic personal information or credit report information with other businesses.

Watch Over Your Credit Reports

- You are entitled to one free credit report each year from each nationwide credit bureau. To get your free report, go to www.annualcreditreport.com or call 1-877-322-8228. Be careful requesting credit reports using any other addresses to avoid fees charged by commercial sites.
- To track your credit during the year, request a free report from a different credit bureau (Equifax / Experian / TransUnion) every four months.
- Consider signing up for a monitoring service which tracks your credit file daily and alerts you whenever there is a change.

Utilize Fraud Alerts and Credit/Security Freezes

- If you have lost a wallet or think your personal information may have been stolen, consider placing a fraud alert on your account. It will allow creditors to get a copy of your credit report only after they take steps to verify your identity.
- Consider placing a credit freeze, also known as a security freeze, on your credit reports. It restricts access to your credit report and makes it more difficult for thieves to open new accounts in your name.

Protect Passwords

- Don't carry your personal identification numbers (PIN) in your wallet or purse.
- Don't share PINs or passwords, even with close friends or relatives.
- When using a debit card, cover the keypad when you enter your PIN. With your debit card and PIN, someone would be able to empty your bank account.
- Avoid using easily available information for your PINs or passwords such as your mother's maiden name, yours or a family member's birth date, your SSN or phone number, or a series of consecutive numbers (i.e., 1, 2, 3, 4).
- Choose a different PIN for each account.

Protect Your Mail

- Call 1 (888) 5-OPT-OUT or visit www.optoutprescreen.com to stop pre-approved credit card applications that a thief could steal and use to get credit in your name.
- Place outgoing mail, especially paid bills, at the post office or into a locked mailbox such as a blue postal service box.
- Don't leave incoming mail sitting in an unlocked mailbox.

Protect Your Information Online

- Beware of phishing, the attempt to acquire sensitive information by someone masquerading as a trustworthy entity in an electronic communication. Sometimes emails telling you that your computer has been infected by a virus are attempts to obtain personal information.
- Never send your SSN or financial account numbers by email or transmit these numbers online unless using a secure website or encryption software.
- Shop only on secure websites, and read website privacy policies
- When you are making online transactions, watch for "https", padlock and green shading to indicate you are on the true company website and not a fraudulent copy-cat website.
- Do not respond to emails from family or friends with attachments and generic subjects such as "Hi." These attachments often contain viruses or give access to your computer.

Beware of Scams and Frauds

- Never give personal information to telemarketers who call you on the phone. To cut down on unwanted telemarketing calls, sign up for the Do Not Call Registry online at www.donotcall.gov or call (888) 382-1222.
- Be skeptical of all unsolicited offers and tell solicitors that you do not buy from (or give to) anyone who calls or visits unannounced. Request that they send something in writing.
- Double-check references for door-to-door sales, home repair offers and other products.
- Verify that charities, businesses and others who contact you are who they claim to be before you provide any personal information. If you think the request for information is legitimate, hang up and contact the company at a number you know is valid to verify the request.
- No one from the IRS will call and threaten you with police arrest, deportation or license revocation if you don't pay immediately. The IRS's first contact with taxpayers is likely to occur via US mail. If you know you owe taxes or think you may owe taxes, call the IRS at (800) 829-1040 and speak with an agent. Visit www.irs.gov for more information.
- Scammers often manipulate caller ID to reflect the name of a legitimate caller in order to obtain information. They will also contact people using two different methods or use the names of two different agencies to support bogus requests. They will use fake names and badge numbers and may even provide victims with partial account/Social Security numbers.
- Hit the clear button on gas pumps when paying with a credit or debit card. Often the last transaction on the pump is stored until another transaction is made; clearing prevents access to your card information.

Finally, be aware that you're at risk from strangers and from those closest to you. Stay involved and do not isolate yourself. If you are a victim, don't be afraid or embarrassed to talk about it because waiting could only make it worse. Call your bank or credit card company, cancel cards related to stolen accounts, reset personal identification numbers, and report abuse to law enforcement.