Red Flags of Identity Theft

Be aware of the following

- Mistakes on your bank, credit card, or other account statements.
- Mistakes on the explanation of medical benefits from your health plan.
- Your regular bills and account statements do not arrive on time.
- Bills or collection notices for products or services you never received.

Other ways to protect your identity

- If your mail has been stolen, report it to your local postal inspector or the U.S. postal inspector. usps.gov
- If you believe someone is using your Social Security number, report it to the Social Security Fraud Hotline. 800-269-0271
- If someone has filed for bankruptcy using your name, contact the U.S. Trustee Program in the region where the bankruptcy was filed. usdoj.gov.
- If a criminal or driving record has been created fraudulently under your name, contact the State’s Attorney’s office. You may need to consult an attorney to help resolve the problem.

Request an annual credit report:
www.annualcreditreport.com
or call 1-800-322-8228
TDD 1-877-730-4104

Opt out of credit card offers:
www.optoutprescreen.com
or call 1-888-567-8688

To report an online crime, go to:
www.IC3.gov

- Calls from debt collectors about debts that don’t belong to you.
- A notice from the IRS that someone used your Social Security number.
- Mail, email, or calls about accounts or jobs in your minor child’s name.
- Unwarranted collection notices on your credit report.
- Businesses turn down your checks.
- You are turned down unexpectedly for a loan or job.

One of the best ways to protect yourself from identity theft is to monitor your credit history!
What is Identity Theft?
The fastest growing crime in America

Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation. It takes time, money, and patience to resolve. Identity theft happens when someone steals your personal information and uses it without your permission.

Identity thieves might:
• Go through trash cans and dumpsters, stealing bills and documents that have sensitive information.
• Work for businesses, medical offices, or government agencies, and steal personal information on the job.
• Misuse the name of a legitimate business, and call or send emails that trick you into revealing personal information.
• Pretend to offer a job, a loan, or an apartment, and ask you to send personal information to “qualify.”
• Steal your wallet, purse, backpack, or mail, and remove your credit cards, driver’s license, passport, health insurance card, and other items that show personal information.

Identity theft happens when someone acquires your financial or personal information and uses it to commit fraud or theft — such as taking over accounts, obtaining loans, applying for credit cards, or purchasing items.

Protect your information
Prevent becoming a victim
• Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months. To order, go to annualcreditreport.com or call 1-877-322-8228.
• Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan. If a statement has mistakes or doesn’t come on time, contact the business.
• Shred all documents that show personal, financial, and medical information before you throw them away.
• If you use a public wireless network, don’t send information to any website.
• Don’t respond to email, text, and phone messages that ask for personal information. Legitimate companies don’t ask for information this way. Delete the messages.
• Create passwords that mix letters, numbers, and special characters. Don’t use the same password for more than one account.
• If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has “https” at the beginning of the web address; “s” is for secure.
• Use anti-virus and anti-spyware software, and a firewall on your computer.
• Set your computer’s operating system, web browser, and security system to update automatically.
• Guard your mailbox from theft. Deposit bill payments at the post office or in post office collection boxes.

If your identity is stolen...
Steps you need to take to recover

1. Make a report to the three credit bureaus
   • Ask the credit bureaus to place a “fraud alert” on your credit report.
   • Order copies of your credit reports
   • Request a victim’s statement that asks creditors to contact you prior to opening new accounts or making changes to any existing accounts.
   
   Equifax 1-800-525-6285
   Experian 1-888-397-3742
   TransUnion 1-800-680-7289

2. Contact the fraud department of each of your creditors
   Gather the contact information for each of your credit accounts (credit cards, utilities, cable bills, etc.) and call the fraud department for each creditor. Follow the phone call with a letter and any necessary documentation to support your claim. Confirm all conversations in writing.

3. Contact your bank or financial institution
   If your checks have been stolen, or if you believe they have been used, contact your bank or credit union and stop payment right away.

4. Report the incident to law enforcement
   Contact the police department and file a report. Request a copy of the police report. Some creditors will request to see the report to remove the debts created by the identity thief.