

## IDENTITY THEFT

### 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.

### How to Protect Your Information

- 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](http://annualcreditreport.com) or call 1-877-322-9228.
- 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.
- 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.
- If you use a public wireless network, don’t send information to any website that isn’t fully encrypted.
- Use anti-virus and anti-spyware software, and a firewall on your computer.

- Set your computer's operation system, web browser, and security system to update automatically.

## **If Your Identity is Stolen...**

### **• Flag Your Credit Reports**

- Call one of the nationwide credit reporting companies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days.
  - Equifax: 1-800-525-6285
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289

### **• Order Your Credit Reports**

- Each company's credit report about you is slightly different, so order a report from each company. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company.

### **• Create an Identity Theft Report**

- An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report:
  - File a complaint with the FTC at [ftc.gov/complaint](http://ftc.gov/complaint) or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
  - Take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report
  - The two documents comprise an Identity Theft Report.

## **Red Flags of Identity Theft**

- 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 don't arrive on time
- Bills or collection notices for products or services you never received
- Calls from debt collectors about debts that don't belong to you

- Mail, email, or calls about accounts or jobs in your minor child's name
- Unwarranted collection notices on your credit report
- You are turned down unexpectedly for a loan or job