Identity Theft

Identity (ID) theft happens when someone steals your personal information to commit fraud.

The identity thief may use your information to fraudulently apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name.

Warning Signs of ID Theft

You may not know that you're the victim of ID theft immediately. You could be a victim if you receive:

•Bills for items you didn't buy

•Debt collection calls for accounts you didn't open

•Denials for loan applications

Potential Victims of ID Theft

Children and seniors are both vulnerable to ID theft. Child ID theft may go undetected for many years. Victims may not know until they're adults, applying for their own loans.

Seniors often share their personal information with doctors and caregivers. The number of people and offices that access seniors' information put them at risk.

Types of ID Theft

There are several common types of identity theft that can affect you:

•Tax ID theft - Someone uses your Social Security number to falsely file tax returns with the IRS or your state

•Medical ID theft - Someone steals your Medicare ID or health insurance member number. Thieves use this information to get medical services or send fake bills to your health insurer.

•Social ID theft - Someone uses your name and photos to create a fake account on social media

Take steps to avoid being a victim of identity theft. Secure your internet connections, use security features, and review bills. Read more about how you can prevent identity theft.

Prevent Identity Theft

Keep these tips in mind to protect yourself from identity theft:

•Secure your Social Security number (SSN). Don't carry your Social Security card in your wallet. Only give out your SSN when necessary.

•Don't share personal information (birthdate, Social Security number, or bank account number) because someone asks for it.

•Collect mail every day. Place a hold on your mail when you are away from home for several days.

•Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.

•Use the security features on your mobile phone.

•Update sharing and firewall settings when you're on a public wi-fi network. Use a virtual private network (VPN), if you use public wi-fi.

•Review your credit card and bank account statements. Compare receipts with account statements. Watch for unauthorized transactions.

•Shred receipts, credit offers, account statements, and expired credit cards. This can prevent “dumpster divers” from getting your personal information.

•Store personal information in a safe place.

•Install firewalls and virus-detection software on your home computer.

•Create complex passwords that identity thieves cannot guess. Change your passwords if a company that you do business with has a breach of its databases

•Review your credit reports once a year. Be certain that they don't include accounts that you have not opened. You can order it for free from Annualcreditreport.com.

•Freeze your credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange for free. Credit freezes prevent someone from applying for and getting approval for a credit account or utility services in your name.

Report Identity Theft

Report identity (ID) theft to the Federal Trade Commission (FTC) online at IdentityTheft.gov or by phone at 1-877-438-4338.

Report ID Theft Online to Get a Recovery Plan

If you report identity theft to the FTC online, you will receive an identity theft report and a recovery plan. Create an account on the website to:

•Update your recovery plan

•Track your progress

•Receive prefilled form letters to send to creditors

If you don't create an account, you won't be able to access the report or letters later. Download the FTC's publication (PDF, Download Adobe Reader) for detailed tips, checklists, and sample letters.

If you report identity theft by phone, the FTC will collect the details of your situation. But it won't give you an ID theft report or recovery plan.

When to Report ID Theft to the Police

You may choose to report your identity theft to your local police station. A creditor or another company may require you to provide a police report. It could also be necessary if:

•You know the identity thief

•The thief used your name in an interaction with the police

Report Specific Types of Identity Theft

You may also report specific types of identity theft to other federal agencies.

•Medical Identity Theft - Contact Medicare’s fraud office, if you have Medicare.

•Tax Identity Theft - Report tax ID theft to the Internal Revenue Service.

Report Identity Theft to Other Organizations

You can also report the theft to other organizations, such as:

•Credit Reporting Agencies - Contact one of the three major credit reporting agencies to place fraud alerts or freezes on your accounts. Also get copies of your credit reports, to be sure that no one has already tried to get unauthorized credit accounts with your personal information. Confirm that the credit reporting agency will alert the other two credit reporting agencies.

•National Long-Term Care Ombudsman Resource Center - Report cases of identity theft due to a stay in a nursing home or long-term care facility.

•Financial Institutions - Contact the fraud department at your bank, credit card issuers and any other places where you have accounts.

•Retailers and Other Companies - Report the crime to companies where the identity thief opened credit accounts or even applied for jobs.

•State Consumer Protection Offices - Some states offer resources to help you recover from identity theft.

You may need to get new personal records or identification cards if you're the victim of ID theft. Learn how to replace your vital identification documents after identity theft.

Medical Identity Theft

Medical identity theft happens when someone uses your name, Social Security number, insurance plan number, or other personal information to get:

•Medical care

•Medication

•Access to your medical records

•Coverage under your name from your insurance company or Medicare

Report Medical Identity Theft

Report the theft online at IdentityTheft.gov or by phone at 1-877-438-4338 (TTY: 1-866-653-4261). Also, report it to your health insurer's fraud department.

If you suspect that you have been the victim of Medicare fraud, contact the U.S. Department of Health and Human Services' Inspector General at 1-800-447-8477.

Prevent Medical Identity Theft

Take these steps to prevent medical identity theft:

1.Guard your Social Security, Medicare, and health insurance identification numbers. Only share them with your health care providers.

2.Review your explanation of benefits or Medicare Summary. Report questionable charges to your health insurance provider or Medicare.

3.Request your medical records. Review them for incorrect information.