COMMON WAYS ID THEFT OCCURS:

Skilled identity thieves use a variety of methods to steal your personal information, including:

1. Dumpster Diving. They rummage through trash looking for bills or other papers containing personal information. Shred sensitive documents.

2. Skimming. Fraudsters steal credit/debit card information by using hidden devices attached to ATMs, gas pumps, or payment terminals to copy card data. Be cautious of tampered machines.

3. Phishing and Smishing. Scammers impersonate financial institutions, companies, or government agencies by sending fake emails, texts, or pop-up messages, urging you to reveal personal or financial information. Always verify the source before clicking on links.

4. Address Change Fraud. Criminals may complete change-of-address forms to divert your billing statements and important documents to another location, gaining access to your personal information. Confirm address changes with financial institutions.

5. "Old-Fashioned" Stealing. Thieves can physically steal wallets, purses, mail (including bank or credit card statements), pre-approved credit offers, new checks, and tax information. They may also bribe employees with access to personnel records or data systems.

6. Data Breaches and Hacking. Cybercriminals target businesses, financial institutions, and health care providers to steal massive amounts of personal information. Use strong, unique passwords and enable multi-factor authentication to protect your accounts.

7. Social Media Scams. Thieves may use personal information posted on social media to answer security questions or impersonate you. Limit what you share online and review your privacy settings regularly.

8. SIM Swapping. Criminals can transfer your mobile number to a new SIM card by impersonating you to your mobile carrier, allowing them access to SMS-based two-factor authentication codes. Protect your mobile account with additional security measures, such as a PIN.

Identity Theft

Office of the Chief Security Officer
Operations Security (OPSEC)

U.S. Department of Homeland Security
Office of the Chief Security Officer
Washington, D.C. 20528

Email: OPSEC@hq.dhs.gov

Homeland Security

DETER

Identity theft is a serious crime that occurs when someone steals and uses your personal information without your knowledge to obtain credit, commit fraud, or carry out other crimes. Identity theft can cost you time and money, damage your credit, and tarnish your reputation.

Deter identity thieves by safeguarding your information.

- **Shred** financial documents and paperwork with personal information before discarding it to prevent dumpster divers from accessing sensitive information.
- **Protect** your Social Security Number (SSN). Avoid carrying your Social Security card in your wallet or write your SSN on a check. Only provide your SSN when absolutely necessary or ask to use another identifier.
- **Verify** the recipient's identity before sharing personal information on the phone, through the mail, or over the Internet. Identity thieves will pose as bank representatives, service providers, and even government officials.
- **Avoid** clicking links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and antivirus software to protect your computer, and keep these programs up-to-date. Visit OnGuardOnline.gov for more information.
- **Create** strong, unique passwords. Avoid obvious passwords like your birth date, your mother's maiden name, or the last four digits of your SSN. Use a unique password for each account to enhance security.
- **Maintain** a list of all your credit card and bank account numbers with customer service contacts and store this list securely.
- **Store** your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

DETECT

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

- **Be alert** to signs that require immediate attention:
  - Bills that do not arrive as expected
  - Unexpected credit cards or account statements
  - Denials of credit for no apparent reason
  - Calls or letters about purchases you did not make
- **Regularly inspect:**
  - Your credit report. Credit reports contain details about your accounts and payment history. By law, Equifax, Experian, and TransUnion provide one free report per week upon request.
    - To obtain your report, visit AnnualCreditReport.com or call
    - 877-322-8228.
    - When reviewing your credit report, verify your personal information, check for inquiries you did not initiate, accounts you did not open, and any unexplained debts. Report any unauthorized accounts or charges to the credit bureaus immediately.
  - Your financial statements. Regularly review all financial accounts and billing statements for unfamiliar charges, as prompt action is key to mitigating unauthorized activity.

DEFEND

Defend against ID theft as soon as you suspect it.

- **Place a Fraud Alert on your credit reports.** A fraud alert notifies creditors to take extra precautions before opening new accounts in your name or making changes to existing ones. You only need to contact one of the three major credit bureaus, as they will notify the other two. Fraud alerts are free and last for one year, renewable upon request.
- **Freeze your credit.** A credit freeze restricts access to your credit report, which means you, or others, will not be able to open a new credit account while the freeze is in place. A credit freeze lasts until you remove it, and you can temporarily lift the credit freeze if you need to apply for new credit.
  - Equifax: 1-800-685-1111 equifax.com/personal/credit-report-services
  - Experian: 1-888-EXPERIAN (397-3742) experian.com/help/
  - TransUnion: 1-800-680-7289 transunion.com/credit-help
- **Close or change tampered or fraudulent accounts.** If any accounts have been compromised or opened without your authorization:
  - Contact each company's fraud or security department and follow up in writing with relevant supporting documents.
  - Request verification that the disputed account has been closed and any fraudulent charges have been removed.
  - Keep copies of all documents and records of communication.
- **File a police report.** File a report with law enforcement officials to help you with creditors who may want proof of the crime.
- **Report the theft to the Federal Trade Commission.** Your report helps law enforcement officials across the country in their investigations.
  - Online: identitytheft.gov
  - By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261