

Identity Theft

Identity theft occurs when someone uses your name, Social Security number, credit card number, or other identifying data to commit fraud or other crimes. In this electronic age, it has become an all-too-common danger. Fortunately, there are many preventative measures you can take to substantially reduce the chance of identity theft occurring and steps you can take to minimize damage if you do become a victim. This module covers the basics of identity theft, including:

- Common Practices of Identity Thieves
- Preventing Identity Theft
- How To Recover
- Federal Laws
- Helpful Resources

Chapter 1: Common Practices of Identity Thieves

How Identity Thieves Acquire Information

Thieves use a variety of illegal techniques to procure identity information. They may:

- Steal statements or other mail containing personal information from your mailbox.
- Divert your mail to another location by filling out a change of address form.
- Search through the trash or recycling bin for documents containing financial or personal information.
- Steal your wallet or electronic device.
- Misrepresent themselves to a company that does business with you or otherwise has information about you (e.g. access your credit report by posing as a landlord).
- Hack into your computer or the computer of a company that does business with you.
- Access the information you enter online or send by e-mail.
- Pose as a legitimate company or government agency and request personal information via phone (“vishing”), email (“phishing”), or text message (“smishing”).
- Attach a skimmer to an ATM to capture the card number and PIN.
- Take advantage of a personal relationship with you. (For example, a “friend” may swipe a statement from your dresser when you are occupied.)

What an Identity Thief Can Do

After an identity thief has your personal information, he or she may use it in a variety of illegal ways. Common practices include:

- **Making charges on an existing credit card account.** Though some retailers check your identification when you pay with plastic, it is often not done – all the thief needs to do is forge your signature. It is even easier for him or her to use your account when making telephone or online purchases.
- **Opening a new credit card account.** Once a thief has your personal information, he or she can open an account in your name, but have the card and bills routed to him or her. The thief makes purchases, but the bill never arrives at your home. (And of course, the thief doesn't pay it him- or herself). You may not find about the crime until a collector tracks you down, you apply for credit and are denied, or you pull a copy of your credit report and you see the activity.
- **Taking out a loan to buy a car or other expensive items.** As with credit cards, you often won't know of the activity until you experience some type of negative credit or collection action.
- **Using an existing checking account.** The thief may write fraudulent checks or use your debit card. Having the PIN makes it easy to take cash out of the ATM, but even without it, he or she can still make purchases in a store by choosing the "credit" option and online and over the phone.
- **Obtaining government benefits or using your health insurance.** The thief may apply for such things as Social Security benefits or foods stamps with your identity or pretend to be you and provide your insurance information to pay for medical care.

Chapter 2: Preventing Identity Theft

Taking steps now to reduce the chances you will become a victim is a lot easier and less time-consuming than cleaning up the mess an identity thief leaves behind.

Review Your Credit Report

You should check your credit reports for fraudulent activity at least annually. You can receive one free copy of your credit report from each of the three credit bureaus, Equifax, Experian, and TransUnion, once year through the Annual Credit Report Request Service. (See Chapter 5 for contact information). You can obtain all three reports at once or stagger your requests throughout the year. If you believe you were a victim of identity theft, you are entitled to additional free reports. (Contact the credit bureaus directly for this.) If you are not currently eligible for free reports, you can purchase them from the credit bureaus for a fee.

When you obtain your reports, look over them carefully for balances that do not seem correct, accounts you never opened, or anything else that seems suspicious. Dispute inaccurate information with the bureaus immediately, and contact the involved creditors (discussed more in Chapter 3).

Guard Your Personal Information

When someone asks you for your information, never hesitate to ask questions or say no if you are uncomfortable. You should only provide personal data when you know how will be used, you are sure the person or company is legitimate, and you are the one who initiated contact.

Check Your Statements

Know your billing cycles, and be sure to review your statements for credit cards, utilities, checking and savings accounts, and other accounts when they are issued. If you see any charges you did not authorize, contact the company immediately. Also contact them if you don't receive your statement when you are supposed to.

Minimize and Protect Your Mail

Try to reduce the amount of mail you receive containing sensitive information. Many credit card companies, banks, credit unions, utility providers, and other institutions allow you to elect to receive electronic statements only.

Since you may not be able to completely stop the flow of mail containing personal information, be sure to empty your mailbox promptly and not let it sit there for a day or two. If you are going on vacation and there is no one available to pick up your mail, you can request a vacation hold with the post office.

Avoid a False Sense of Security

It is easy to have a sense of security in your home, work, place of worship, or other familiar spot, but keep in mind that many people are victimized by someone they know. (And of course, there may be strangers passing through as well.) Never leave your wallet, statements, or portable electronic devices out in plain sight.

Only Carry With You What You Need

If your wallet or bag is stolen, the less you have in it, the less information the thief has. There is almost never a need to carry your Social Security card with you. Most people don't need to lug around their checkbook either.

Dispose Carefully

If you are disposing of a statement or something else containing personal information, shred it – don't just don't throw it in the trash. Do the same for pre-approval offers. Better yet, opt out of receiving them. (Contact information for doing this is in Chapter 5.)

Protect Your Computer and Smartphone

Use a firewall and anti-virus/anti-spyware software to reduce your computer's vulnerability to hackers. Make all passwords hard to guess by using a complex combination of numbers and upper and lower case letters. Log off when you leave the room, and don't leave portable devices unattended. Before disposing of your computer or smartphone, be sure to delete personal information using a "wipe" utility program to overwrite the entire hard drive.

When shopping online, use a secure browser - enter personal and financial information only when there is a "lock" icon on the browser's status bar and look for the URL to read "https" versus "http." Don't send sensitive personal information via e-mail or download files or open hyperlinks sent by people you don't know.

Consider Extra Protection – Carefully

If you are exceptionally concerned about the possibility of identity theft, you may consider paying for credit monitoring or identity theft insurance – but do so only after carefully reading the fine print and weighing the cost against the benefits. Some of the businesses that offer these services are a scam themselves. Research the company's history and check the Better Business Bureau's complaint log before signing up.

- **Credit monitoring.** A credit monitoring service typically provides regular credit report updates about new inquiries, new accounts, late payments, sudden changes in your credit card balances, and other potentially suspicious activity. You may also be able to access your credit report whenever you want at no additional cost.
- **Identity theft insurance.** If you become victimized by identity theft, this type of insurance reimburses you for the out-of-pocket expenses incurred to clean it up (but not the money that was stolen) and helps you through the process of contacting creditors, writing affidavits, and filing reports.

Chapter 3: How To Recover

If you become a victim of identity theft, being proactive can minimize its impact on you. You may need to communicate with several parties, including:

- **Creditors and financial institutions.** If a credit card or checking account has been used or opened illegally, contact your creditor or financial institution immediately. If the account is not yours, it should be closed. If it is yours, you should get a new account number and card. Monitor all future account statements carefully for evidence of new fraud.
- **Legal and government agencies.** You may want to report the identity theft to the police. If you do, request a copy of the police report – a credit bureau or creditor may ask you to provide one as part of their fraud investigation. A complaint can also be filed with the Federal Trade Commission, although they do not assist with individual cases. You can contact the US Postal Inspection Service if your mail was stolen or your address was used fraudulently. (Contact information is in Chapter 5.)
- **Credit reporting bureaus.** Check your credit reports from all three bureaus. (Remember, you are entitled to additional free reports if you believe you are the victim of identity theft.) Dispute any fraudulent items – this can be done by submitting a form on-line or mailing a letter to the credit bureaus. They are required to investigate and respond within 30 days (45 days if the report was obtained through the Annual Credit Report Request Service).

Even if the fraudulent information hasn't yet appeared on your reports, be proactive and report the crime to credit bureaus now. It is a good idea to have a fraud alert placed on your credit reports. When someone applies for credit under your name, the creditor must verify that the person applying is you. The initial fraud alert only lasts 90 days. However, if you file a police report, you can extend the alert to seven years. You can also place a one-year alert on your file if you are on active duty with the military.

If you feel like a fraud alert will not provide you with enough protection, you can place a security freeze on your credit report. When a freeze is placed on your report, no creditor or other business that does not have a pre-existing relationship with you can access your report. Since most creditors will not grant credit without checking your report first, this makes it extremely difficult for a thief to get credit in your name. If you want to apply for credit yourself (or rent an apartment or do anything else that requires a credit check) you can have the freeze lifted, either temporarily or permanently, but it may slow down the application process.

Because you may be speaking with many people, it is vital to be organized. Keep copies of all letters, file paperwork promptly, and store everything in a safe and accessible place. You can use the Identity Theft Action Log on pages 9-12 to help you keep track of what you have done.

Chapter 4: Federal Laws

There are many federal laws that help in the fight against identity theft.

Fair Credit Reporting Act (FCRA)

- If you are denied credit, insurance, or employment because of what is in your credit report, you may get a free report from the bureau that supplied it within 60 days.
- You have a right to dispute any inaccuracies on your credit report. The credit bureaus must investigate the validity of disputed items within 30 days (under most circumstances).
- Derogatory information that is outdated or unverifiable cannot be reported.
- Only those with a need recognized by the FCRA (usually a creditor, insurer, employer, landlord, or other business who is evaluating an application from you) may access your file.

The Fair and Accurate Credit Transactions (FACT) Act

- You may receive a free copy of your credit report from each of the three credit bureaus once a year.
- You may receive additional free reports if identity theft is suspected.
- You may block fraudulent information from appearing on your credit report.
- You have a right to access business records, such as credit applications, that document an identity thief's fraudulent transactions.
- You have a right to place a fraud alert on your credit report if you believe you have been the victim of identity theft. Creditors must ensure that all credit requests are legitimate after a credit report has been flagged.
- Active duty military personnel may place a special alert on their files when they are deployed overseas.
- No more than five digits of a credit card number may be listed on store receipts. The card's expiration date cannot be listed either.
- Creditors must implement identity theft prevention programs.
- Debt collectors must inform a creditor of fraudulent information.

Fair Credit Billing Act (FCBA)

- Liability for a lost or stolen credit card is limited to \$50 if you notify the card issuer within 30 days.

- If there has been an error in a credit card bill, the lender must correct it, or explain why the amount is believed correct, within 90 days after being notified. (You must send the notification within 60 days of the bill containing the error being sent to you.)

The Electronic Fund Transfer Act

- You have 60 days to dispute an error in a checking or savings account statement. The financial institution must respond with 45 days (in most cases). Any disputed funds must be put back into your account within 10 business days.
- The maximum liability for a lost or stolen debit or ATM card is:
 - \$50 if you report it within 2 business days of noticing the card is lost or stolen.
 - \$500 if you report it after 2 business days but within 60.
 - No limit if you wait more than 60 days – you can lose all of the money in your account plus, if applicable, your maximum overdraft line of credit.
 - Note: Many financial institutions provide protections greater than what is required by the law.

If a creditor or credit bureau violates one of these laws, you can submit a complaint with your state's attorney general's office and the Federal Trade Commission. Violations involving a checking or savings account can be reported to the Office of the Comptroller of the Currency for national banks, the Federal Reserve Board for state banks that report to them, the Federal Deposit Insurance Corporation for other banks, the National Credit Union Administration for federal credit unions, and state financial supervisory board for state credit unions.

Chapter 5: Helpful Resources

Since contact information can periodically change, confirm addresses before sending a letter containing personal information.

Credit Reporting Bureaus/ Credit Reports

Equifax

To order a credit report: (800) 685-1111

To report fraud: (888) 766-0008

PO Box 740241, Atlanta, GA 30374

- www.equifax.com
- Dispute Form: https://www.ai.equifax.com/CreditInvestigation/jsp/ECC_Dispute_Login.jsp
- Fraud Alert Request: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

Experian

(888) 397-3742

PO Box 2104, Allen, TX 75013

- www.experian.com
- Dispute form or fraud alert request: <http://www.experian.com/disputes/>

TransUnion

To order credit report: (800) 888-4213

To report fraud: (800) 680-7289

PO Box 2000, Chester, PA 19022

- www.transunion.com
- Dispute Form: <http://annualcreditreport.transunion.com/entry/disputeonline>

Annual Credit Report Request Service

(877) 322-8228

PO Box 105281, Atlanta, GA 30348

- www.annualcreditreport.com

Government Agencies

Federal Trade Commission

(877) 382-4357

Identity theft hotline: (877) 438-4338

600 Pennsylvania Avenue NW, Washington, DC 20580

- www.ftc.gov
- Identity Theft Victim's Complaint and Affidavit: <http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf>
- Complaint Form: https://www.ftccomplaintassistant.gov/FTC_Wizard.aspx?Lang=en

U.S. Postal Inspection Service

(877) 876-2455

222 S Riverside Plaza Ste 1250, Chicago, IL 60606

- <https://postalinspectors.uspis.gov>
- Complaint Form: <https://postalinspectors.uspis.gov/forms/idtheft.aspx>

U.S. Postal Service

- Vacation Hold Request Form: <https://holdmail.usps.com/holdmail/landingView.do>

Banking Regulators

Office of the Comptroller of the Currency (national banks)

800-613-6743

1301 McKinney Street Ste 3450, Houston, TX 77010

- www.occ.treas.gov
- Complaint Form: https://appsec.helpwithmybank.gov/olcc_form/

Federal Reserve Board (state-chartered banks)

888-851-1920

PO Box 1200, Minneapolis, MN 55480

- www.federalreserve.gov
- Complaint Form: <https://www.federalreserveconsumerhelp.gov/FormComplaint.cfm?source=jump>

Federal Deposit Insurance Corporation (other banks)

703-812-1020

2345 Grand Boulevard Ste 100, Kansas City, MO 64108

- www.fdic.gov
- Complaint Form: <https://www2.fdic.gov/starsmail/index.asp>

National Credit Union Administration

1775 Duke Street, Alexandria, VA 22314-3428

(800) 755-1030

- www.ncua.gov
- For regional contact information: <http://www.ncua.gov/Resources/ConsumerInformation/Complaints/fcucomplaints.aspx>

Checking Account Verification/Monitoring Services

ChexSystems

(800) 428-9623

7805 Hudson Rd Ste 100, Woodbury, MN 55125

- www.consumerdebit.com
- Complaint Form: https://appsec.helpwithmybank.gov/olcc_form/

TeleCheck

(800) 710-9898

PO Box 4451, Houston, TX 77210

- www.telecheck.com
- Dispute Form: http://www.firstdata.com/telecheck/telecheck_dispute_form.pdf

Other

Better Business Bureau

- www.bbb.org

Pre-approved Credit Offers

To opt out of receiving pre-approved credit offers

(888) 567-8688

- www.optoutprescreen.com

Identity Theft Action Log

FINANCIAL INSTITUTIONS						
Financial Institution	Action	Yes/No	Date	Contact Person	Notes (phone, email, extension, etc.)	
	Stop payments					
	Report check fraud					
	Cancel accounts					
	Change account #'s and passwords					
	Stop payments					
	Report check fraud					
	Cancel accounts					
	Change account #'s and passwords					
	Stop payments					
	Report check fraud					
	Cancel accounts					
	Change account #'s and passwords					

CREDIT ACCOUNTS

Creditor	Action	Yes/No	Date	Contact Person	Notes (phone, email, extension, etc.)
	Report fraud				
	Send affidavit				
	Change account #'s and passwords				
	Report fraud				
	Send affidavit				
	Change account #'s and passwords				
	Report fraud				
	Send affidavit				
	Change account #'s and passwords				
	Report fraud				
	Send affidavit				
	Change account #'s and passwords				
	Report fraud				
	Send affidavit				
	Change account #'s and passwords				

CREDIT REPORTING BUREAUS

Bureau	Action	Yes/No	Date	Contact Person	Notes (phone, email, extension, etc.)
Equifax	Obtain report				
	Fraud alert				
Experian	Obtain report				
	Fraud alert				
Trans Union	Obtain report				
	Fraud alert				

LEGAL AND GOVERNMENT AGENCIES

Bureau	Action	Yes/No	Date	Report #	Notes (phone, email, extension, etc.)
FTC	Report crime				
	File Report				
Police Dept.	Report crime				
	File Report				
USPIS	Report crime				
	File Report				
DMV	Report crime				
	File Report				

