REDUCING THE RISK OF IDENTITY THEFT

FRM - KM.011

Reducing the Risk of Identity Theft

By Kelly May
Family Finance and Resource Management

Identity theft is often the most reported type of fraud complaint that the Federal Trade Commission (FTC) and other enforcement agencies receive. With identity theft occurring so frequently, it is important to take steps to reduce your risk.

Typically, credit card fraud tops the FTC's list of identity theft types. However, in 2020, government documents or benefits fraud exceeded credit card fraud, according to FTC Consumer Sentinel Network data. This type of fraud occurs when someone's information is misused to apply for a government document or benefit, such as unemployment insurance. In 2020, there were 406,375 reports of government documents or benefits fraud and 393,207 reports of credit card fraud. Those two categories alone made up more than half of the year's 1.3 million total identity theft reports, according to FTC data. Other types of identity theft included in the report were loan or lease fraud, employer or tax-related fraud, phone or utilities fraud, and bank fraud.

WHAT IS IDENTITY THEFT?

As the fraud report data shows, identity theft comes in many forms. But what exactly is identity theft? According to USAGov, identity theft happens when someone steals your personal information to commit fraud. Usually this means the identity thief impersonates you in some way for personal gain.

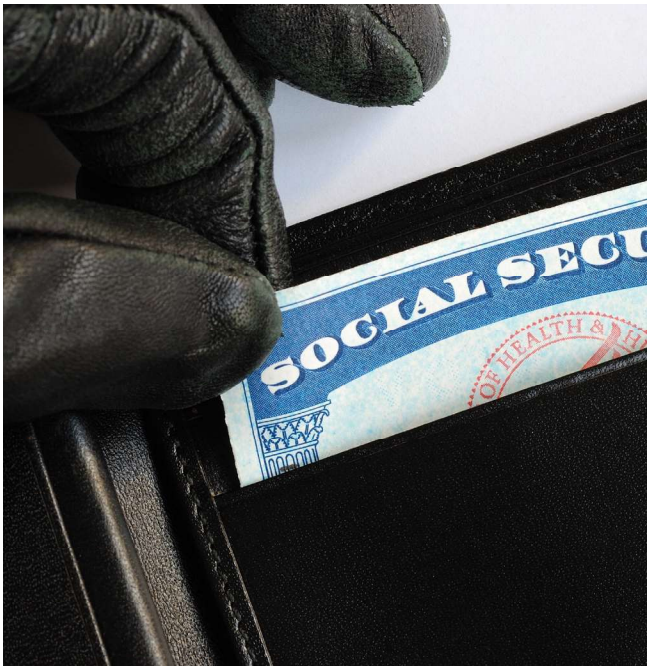
Identity thieves can do many things with your stolen information:

- Withdraw money from an ATM or bank account,
- Use your credit card account to make purchases,
- Open new credit or utility accounts in your name,
- Use your health insurance to get medical services,
- Claim your tax refund by filing in your name,
- Claim a government benefit in your name, or
- Falsify an identity (such as on a job application or during a police arrest).

If any of these incidents happen, it can cost you time and money to remedy. Sometimes it could damage your credit file, credit report, or credit score. You might be liable for charges if you do not report the identity theft in a timely manner.

Identity theft can happen several different ways – most of which the victim may not know about immediately. It could happen through a physical theft. For example, a thief could steal financial, employee, or medical records from home or business trash. The thief could steal or reroute mail. Or someone could take your information from a lost or stolen purse or wallet.

Identity theft also can happen online. *Phishing*



occurs when someone sends an email that appears to come from a legitimate company in an attempt to trick you into sharing sensitive information. *Spoofing* is a similar tactic that disguises caller ID to trick you over the phone. The thief could obtain personal information through a data security breach or through malware installed on a home or work computer. *Malware* is malicious software that damages a computer or makes it vulnerable. In a *data security breach*, a cybercriminal retrieves sensitive information from a company, government office, or other data source. Some data breaches may occur in places where you choose to share your information, such as stores where you shop. Other data breaches may occur at places that house your information without your choice. *Skimming* occurs when a thief attaches a device to a credit card terminal, such as on a gas pump or ATM, that captures your information when you swipe your card. Sometimes the thief can piece together information from what you share on social media. Identity theft also may occur if the thief intercepts banking, shopping, or other information shared over unsecured Wi-Fi.

HOW CAN I PROTECT MYSELF FROM IDENTITY THEFT?

Companies exist that sell "identity theft protection services." However, these companies actually offer monitoring and recovery services. There are free actions you can take on your own rather than paying for a service. For more information on these services, visit http://bit.ly/IDtheftProtectionInfo.

The truth is, identity theft cannot be prevented entirely. Fortunately, you can take several steps to reduce your risk of identity theft.

1. **Shred documents you no longer need, and take other steps to keep your personal information private.**

Protect your physical data by filing your important papers in a safe place and shredding any sensitive information you no longer need. Keep your Social Security and Medicare cards stored in a safe or fireproof box, rather than in your wallet. Retrieve your mail promptly from your mailbox.

While out doing business, keep your purse or wallet close to you. Use credit or debit cards by inserting the chip rather than swiping the card, since the chip offers more security features. Don't give your card to clerks, waiters, or others you are conducting business with who might write down the information when you can't see them. If the payment method is a concern, consider paying in cash or using a gift card. Don't share your PIN. Cover keypads with your other hand while entering your PIN, so no one watching can steal it.

When doing business online, make sure you are using secure Wi-Fi on a device that has security software installed. If you are shopping or banking, make sure the site is secure – look for "https" and/or the "lock" symbol in the web address. Use strong passwords that are unique, long, and unusual. The goal is to make it difficult to guess. Consider using a phrase rather than a word, and add numbers

and symbols. Don't set your device to "remember" passwords; use a two-step process to log in to your most sensitive accounts. Don't give out your personal information over phone or email. Be wary of opening email attachments that may contain malware. Think carefully before posting on social media, so that you don't give away clues to your security questions.

2. **Monitor account statements regularly for unusual activity.**

Whether you receive paper statements or online copies, make sure you review them carefully each month. On bank account and credit card statements, make sure you recognize the transactions. Know your due dates and contact the institution if you do not receive an expected bill. Many financial institutions will allow you to sign up for email or text alerts to notify you of activity on your accounts.

Also, review insurance statements, such as an explanation of benefits, to ensure you recognize the services listed.

3. Check your credit reports.

You can monitor your own credit for free by checking your credit report. The three major credit bureaus – Equifax, Experian, and TransUnion – each offer access to at least one free credit report annually. The credit bureaus compile data about you that they receive from creditors. Since creditors might only report to one bureau, you should check all three.

Request free credit reports online at www.annualcreditreport.com. Beware of fake sites with similar addresses or companies that ask you to pay or subscribe. You also may request your free report by phone at 877-322-8228 or by mail at Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. When you request your report, you must verify your identity by answering several personal credit questions.

Generally, your report is free, but your score is not. Your report includes your personal information, details on your credit accounts, collection items, and public records such as foreclosures and bankruptcies. It will show how much you owe and whether you pay your bills on time. It also will show which companies have inquired about access to your report.

As you review your report, look for any incorrect information. Also, be alert for any accounts that you didn't authorize. You can dispute any incorrect details with the credit bureau, which will keep your report clean and accurate.

WHAT DO I DO IF MY IDENTITY IS STOLEN?

If you haven't taken the precautions listed here, it could be a while before you discover identity theft. You might not know it has happened until you see withdrawals or purchases you cannot explain. You might stop getting certain bills, or suddenly get a bill for a service you didn't purchase. It can be frustrating if you get a call from a debt collector about a debt that isn't yours, or if a merchant refuses your checks. Your health plan might refuse to cover you because your records show you've reached your benefits limit. Alternately, maybe the IRS notifies you that your return has already been filed or shows that you have income from an unknown employer. Note that children or the elderly also may be vulnerable to identity theft. Share with them these steps to protect themselves, or, as caregiver, take precautions for them.

REPORT IDENTITY THEFT. If you suspect identity theft, visit identitytheft.gov, the FTC's resource for victims. The website guides you through three steps to getting a recovery plan. First, you report the identity theft and give details about what happened. Then, you receive a recovery plan personalized to your situation. If you choose to create an account, the FTC will walk you through the steps of your plan and help pre-fill forms and letters for you to use.

You can get additional identity theft information from the Kentucky Attorney General at http://bit.ly/IDtheftKyAG. Also, you can report it to the Kentucky Identity Theft Hotline at 800-804-7556.

As you work through the process, it may help to keep a log of who you talk with and when. Make a file and keep copies of documents you receive or provide.

OTHER STEPS. You might need to take some steps immediately, besides reporting it to the FTC. Identity theft victims can file a report with the local police department and contact the companies where the fraud happened. Review your statements and all three of your credit reports to find out if any other identity theft has occurred.

PLACE AN ALERT OR FREEZE. You might consider placing a one-year fraud alert, an extended fraud alert, or credit freeze on your credit report. Note that these only prevent new accounts from being opened in your name. It is a good idea to check your credit reports and account statements regularly to watch for fraud on your existing accounts.

FRAUD ALERT. If you place a fraud alert on your report, a business may access your report, but must verify your identity before issuing new credit. A fraud alert stays on your report for one year. It entitles you to one free copy of your credit report from the bureau you contact.

Anyone can place a fraud alert, even if you're only concerned about identity theft due to a theft or data breach but haven't yet become a victim. To place a free fraud alert, contact one of the three major credit bureaus. That bureau will notify the other two about your alert.

- **Equifax** – 800-685-1111, Equifax.com/personal/credit-report-services
- **Experian** – 888-397-3742, Experian.com/help
- **TransUnion** – 888-909-8872, TransUnion.com/credit-help

EXTENDED FRAUD ALERT. If you are a victim of identity theft and you have a police report, you can request an extended fraud alert. The extended alert lasts seven years. It entitles you to two free credit reports within 12 months from each of the three bureaus.

CREDIT FREEZE. Another option is to place a credit freeze on your credit report. A credit freeze, also known as a security freeze, restricts access to your credit report. To place the freeze, contact each of the three bureaus and provide the requested information. Each bureau will provide a PIN or password that you will need to lift the freeze in the future. It is free to freeze and unfreeze. If you need to apply for new credit in the future, you will need to temporarily lift the freeze then place it again when you are finished accessing your credit.

If there have been new accounts opened in your name, you may need to close them. Ask that they be reported as closed "at customer request." You can work to remove incorrect charges from your accounts and correct your credit report as needed. Remember, if you close checking accounts that have automatic payments or direct deposit set up, you will need to direct those to the new account.

While it may be difficult to eliminate the risk of identity theft completely, taking the precautions listed here can help reduce your risk. Not all data is in your control, but you can keep a great deal of your personal information safe with prevention practices. If you find that your identity is stolen, report it immediately and take steps to correct the fraud and protect yourself.

References

- Federal Trade Commission's Consumer Sentinel Network. "All Identity Theft Reports." Data as of Dec. 31, 2020. (Retrieved Feb. 9, 2021) https://public.tableau.com/profile/federal.trade.commission#!/vizhome/FraudandIDTheftMaps/IDTheftbyState
- USAGov. "Identity Theft." Dec. 7, 2020. (Retrieved Feb. 9, 2021) https://www.usa.gov/identity-theft#item-206115
- Federal Trade Commission. "Avoiding Identity Theft." (Retrieved Feb. 23, 2021) https://www.consumer.gov/articles/1015-avoiding-identity-theft#!what-it-is
- Federal Trade Commission. "Credit Freeze FAQs." September 2019. (Retrieved Feb. 26, 2021) https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs