IDENTITY THEFT

Identity Theft

Some Facts About Identity Theft:

- According to FBI Internet Crime Report, identity theft victims lost $160,305,789 in 2019.
- Only 3 in 5 of Americans have checked their credit report.
- 2 in 3 Americans who have checked their credit scores have had to take action to correct inaccuracies.
- 13 was the average number of corrections to their credit reports for those who noticed inaccuracies.
- 60 percent of Americans report that they or an immediate family member have ever been the victim of a scheme to defraud them. This includes letters, emails or phone calls impersonating the IRS, theft of an existing credit card number, new lines of credit opened in their name, or tax return fraud.
- 62 percent of parents of minors don't know children are at risk. In 2018, nearly 1 in 4 children had experienced identity theft. It affected over 13 million.

How You Can Help Protect Yourself from Identity Theft

There's no surefire way to protect yourself from identity theft. But there are many steps you can take to reduce the chances of someone stealing your identity.

The first part of this booklet explains the best practices for protecting your identity.

The second part of this booklet has steps you can take if you find yourself a victim of identity theft.

The Basics:

Never give out or write down your Social Security number

Make sure your social security number is not on your checks or IDs. If asked, always request to provide a different form of identification.

Carry only the cards you need in your wallet

This includes medical cards that may have your sensitive information. Leave extra credit cards and your Social Security card locked up safely at home.

When in doubt, opt out

Read privacy notices from your financial institutions. Then, follow the instructions to opt out of sharing your information. Stop unsolicited credit card offers by calling 888-5OPT-OUT or visit www.optoutprescreen.com.

At Work:

Keep your purse or wallet locked up at work.

Workplace theft is more rampant than most people realize. Ask your employer for a safe place to lock your purse or wallet if they don't already provide one.

Ask your employer about security procedures for personnel files

Make sure your employer locks up files and that there is a policy in place to prevent theft. Many cases of identity theft started at work because coworkers stole personal data.

Don’t log onto personal financial accounts from work

In addition, don’t set work computers to remember personal passwords automatically. Finally, don’t store personal information in your desk or on work computers.

At Home:

Use a locked mailbox, if possible, to receive mail

Thieves can pluck bills or other mail from your mailbox and use that information to commit fraud. Send any sensitive mail from the post office or using an official USPS mailbox.

Never have new checks sent to your home

You should only receive checks if your mailbox is secure. If not, ask your bank to hold them for you at your local branch and pick them up instead.

Buy an inexpensive shredder

Shred any mail or documents with sensitive information before you throw them away.

Keep track of when your credit card bills normally arrive

If one is missing, contact your lender immediately. Don’t just assume you get to skip a month’s payment or that your creditor forgot to mail it!

Keep your personal information in a locked room or filing cabinet at home

This is especially important if you have frequent visitors, a housekeeper, or others who may be in your home.

Check your credit report at least once a year

Consider a credit monitoring service if you want to keep close tabs on your credit report. Early detection of fraud can save hours of time and hassle later.

When you receive a benefits statement from the SSA, check it carefully for errors or possible fraud

If you see signs of either, call the Social Security Administration as soon as possible.

On the Internet:

Use a virtual private network

Be sure to use a VPN if you use public Wi-Fi. This technology hides your identity, online activity, and communications from unwanted eyes. Install a VPN on your phone as well.

Use a firewall on your home computer

These are often inexpensive and well worth it. If you are constantly connected to the Internet via a cable modem or fiber connection, it's especially important to protect yourself.

Choose good passwords and usernames

Don't use your Social Security number, address, or family birth dates. The best passwords use letters, numbers and special characters. The best usernames don't give away valuable information.

Beware of phishing

Scammers can use email or fake websites to collect personal information from consumers. Thousands of consumers have fallen victim to the “PayPal” email scam where consumers receive emails that seem to be from the company. The emails ask them to update their personal information, but that info goes straight to the scammers. Fraudsters operate fake sites, but they look real. Always log into financial sites from the homepage you usually use.

Think twice before providing sensitive personal information online

Consumers have been duped into applying for loans on fake websites designed only to gather consumer information. In other cases, companies sell consumer information to outside companies without their permission. Make sure a website is reputable before you enter your personal data.

Shop carefully

Only deal with reputable merchants that have secure websites. For maximum protection, always use a credit card rather than a debit or check card when dealing with a new merchant online.

Teach your children about online privacy

Make sure they understand they should not give out any personal information without your permission.

Before you trash a computer, clear the hard drive

Make sure your information is no longer available to someone who may pick it up from the trash or a charity. Wipe your computer clean or physically destroy the hard drive. Simply deleting files may not be enough.

What to Do if ID Theft Happens to You

If you become a victim of identity theft, you'll want to take these steps immediately:

File a police report

You'll need this to report the theft. Keep the original and make copies for others who need it.

Notify the credit bureaus

Report the fraud immediately to the three major credit reporting agencies – Equifax, Experian and TransUnion. One company should notify the other two, but be sure to ask. Ask them to place a fraud alert on your file.

Get a recovery plan from the Federal Trade Commission

Visit www.identitytheft.gov for the forms, affidavits, and letters you will need to start the recovery process.

Order your credit report and investigate new accounts

By law, fraud victims are entitled to one free copy of their credit report. Review your credit reports, preferably from all three major bureaus. Contact all unknown creditors listed under "New Accounts" or "Inquiries." Explain that you are an ID-theft victim and ask them how you can file a report. They'll likely want a fraud affidavit, proof of your identity, and a copy of the police report.

Contact your issuers

If you suspect that someone used your current accounts (especially credit cards) or stole your information, contact your creditors and ask them to cancel those accounts. This also applies to your ATM card or debit cards.

Contact the Social Security Administration if you think someone used your SSN fraudulently

Even if you aren't sure, review your annual benefits and earnings statement to ensure it's accurate. Think twice about requesting a new Social Security number. Doing so can create more problems than it solves. You can report fraud to the SSA at 1-800-772-1213 or visit www.ssa.gov.

Check your address

Check with the United States Postal Inspection Service (www.uspis.gov) to see if anyone filed a change of address. Also notify them if you suspect the imposter used the U.S. mail in their crime. (For example, if they have mailed change-of-address notices or credit applications.)

Check your checks

If you suspect that a thief fraudulently used your checks, contact the major credit verification bureaus to file a fraud alert.

- ChexSystems is the largest check company that provides this type of service. Contact them at www.chexsystems.com and click on the "Security Alert" under the "Identity Theft" menu or call 1-800-428-9623.
- Telecheck is smaller but it may also be helpful to contact them at www.getassistance.telecheck.com/index.html or 1-800-366-2425.

Double-check your driver's license

If you suspect someone misused it, contact your state's Department of Motor Vehicles to place a fraud alert on your driver's license. Recent investigative reports show it is very easy for imposters to get new driver's licenses using other people's information.

Check your passport

Alert the passport office to make sure no one orders a passport with your information (either a replacement or a new one). Visit www.travel.state.gov/content/travel.html or call 1-877-4USA-PPT (1-877-487-2778).

Talk to an attorney

Under the current credit reporting law, you only have two years to bring a lawsuit if you discover misuse of your personal information. You may want to talk with an attorney if you run into roadblocks with either credit reporting agencies or creditors. Contact the National Association of Consumer Advocates at www.consumeradvocates.org to locate an attorney in your area. They should have experience with the Fair Credit Reporting Act and identity theft cases.

What if you know the thief?

Many times, consumers know the thief that stole their information. It may be a coworker, friend, or even a relative or loved one. This can create additional problems since the victim is afraid of getting the thief in trouble with the law. Identity theft is a serious crime, and if you don't handle the situation appropriately, you may be stuck facing the consequences for years to come. For helpful guidelines on what to do when you know the criminal, visit the Identity Theft Resource Center at www.idtheftcenter.org.

How Consumer Credit Laws Protect You

In 2003, Congress passed a law updating the federal Fair Credit Reporting Act. It contains an entire section of requirements that make resolving fraud cases easier. The following information outlines some of the highlights:

Identity Theft Fraud Alerts

If you think you may have been, or are about to be, a victim of identity theft, credit reporting agencies must place a fraud alert on your credit report if you request it. There is a system in place so you should only have to make one phone call to initiate placing an alert. You will need to fill out a fraud affidavit and provide proof of your identity.

Members of the military on active duty may request that bureaus place an alert on their file indicating they are on active duty. For those with fraud alerts on their credit files, creditors will have to take reasonable steps to make sure they verify a consumer's identity before opening any new account.

Identity Theft Prevention

Federal banking agencies, the National Credit Union Administration, and the Federal Trade Commission worked together to develop guidelines for anyone who uses credit report information to prevent identity theft. They also require financial institutions or other credit report users to notify the Federal Trade Commission if there has been any security breach of consumer information.

In addition, they established rules so if a credit issuer receives a request for a new or replacement card from a consumer less than 30 days after receiving a change of address, the issuer must take additional steps to verify that the request is valid.

You can also ask the credit bureaus not to disclose the first five digits of your Social Security number when they supply your credit report to any requester.

If Your Identity Has Been Stolen

If you become a victim of identity theft, you can request a copy of any application and transaction records that were made by the imposter. For example, you can request copies of the application form from a credit card company that opened an account for the thief in your name. You will need to provide proof of your identity and, if the business requests it, a copy of a police report and an identity theft affidavit. The business must supply the information within 20 days.

Within four business days of notifying a credit reporting agency of identity theft, the bureau must block the information that the consumer reports and notify the creditor reporting the information that the consumer believes it's fraudulent.

Identity theft victims are entitled to two free credit reports in that year, as well as blocking their file from prescreened credit offers. Creditors are also required to follow certain procedures to make sure that information that has been blocked or removed can't be resubmitted to the credit bureau again. The goal is to keep information legitimately related to identity theft off the consumer's report. Creditors generally can't sell or transfer accounts that consumers claim are due to identity theft – especially not to collection agencies.

Debt collectors who are notified that a debt may be related to identity theft must notify the creditor from whom they received the debt that it may be fraudulent.

Additional Resources

Several websites provide additional helpful information for both preventing and dealing with identity theft:

Federal Trade Commission (Identity Theft Site): www.identitytheft.gov

Identity Theft Resource Center: www.idtheftcenter.org

Privacy Rights Center: www.privacyrights.org