




Protecting Yourself Against Identity Theft

Sometimes called a “Silent Crime,” the rise in Identity Theft in the United States is staggering. Nearly 60 million Americans have been affected by identity theft according to a 2018 online survey by The Harris Poll. Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.



The crime takes many forms from making fraudulent charges on a credit card all the way through renting an apartment, obtaining a credit card, or even establishing a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector.



Here are some tips regarding identity theft and how you can protect yourself and your information.

How do thieves steal an identity?

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.

Skilled identity thieves may use a variety of methods to get hold of your information, including:

- **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
- **Skimming.** They steal credit/debit card numbers by using a special storage device when you process your card at places like gas stations.
- **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
- **Changing Your Address.** They divert your account statements to another location by completing a change of address form.

- **Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel record, or bribe employees who have access.
- **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.
- **Obituaries.** Scammers look at obituaries for names and addresses, then buy social security numbers and other personal data for the deceased individual.
- **Document Forgery.** Forgers obtain signed checks and alter the payee and/or dollar amount. To avoid this problem, always use a gel pen for your checks.
- **Gift card scams.** There are many varieties of scams related to gift cards. An email from an unknown address (but personal contact) asks someone to “procure” gift cards to be sent to a certain address.
- **“Tech” Support.** Scammers claim to be representatives of a software firm – sometimes going as far as spoofing a caller ID so that your phone displays the name of your trusted company. They may ask you to install applications that give them access to your computer.
- **IRS Notices.** Scammers take advantage of people’s fear of the IRS to scare them into providing sensitive information or money by phone, email, or snail mail.



3 Ways to Protect - and Defend - Your Identity



1. Deter identity thieves by safeguarding your information.

- Shred financial documents and paperwork with personal information before you discard them
- Protect your Social Security number. Don't carry your card in your wallet or write on a check.
- Don't give out personal information over the phone, internet or mail. Don't respond to emails directing you to a site to confirm your user name or password, even if it looks legitimate. Call or use the website you know to be legitimate to verify their authenticity.
- Use firewalls, anti-spyware and anti-virus software to protect your home computer and keep them up-to-date.

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

Be alert to signs that require immediate attention, such as:

- Bills that do not arrive as expected
- Unexpected bills or account numbers
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make
- Inspect your credit report

The law requires the major nationwide consumer reporting companies—Equifax, Experian, and TransUnion—to give you a free copy of your credit report each year if you ask for it. Visit www.AnnualCreditReport.com or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.



3. Defend against ID theft as soon as you suspect a problem.

Place a free "Fraud Alert" on your credit reports, and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:

- Equifax: 1(800) 525-6285
- Experian: 1(888) EXPERIAN (397-3742)
- TransUnion: 1(800) 680-7289

Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. An initial alert stays on your reports for at least 90 days. An extended alert is available if you have been a victim of credit theft and submit an Identity Theft Report.

Freeze your credit. A freeze cuts off access to your credit reports unless and until you lift the freeze with a password-protected credit bureau account or a PIN. A fraud alert requires that creditors verify your identity. One lesson we learned from the 2017 Equifax data breach is how freezing your credit at each of the three major credit reporting companies could protect you in the event of identity theft. Contact each of the nationwide credit reporting companies to get started:

Contact each of the nationwide credit reporting companies to get started:



Equifax: 1 (800) 349-9960

<https://www.freeze.equifax.com/Freeze>



Experian: 1 (888) 397-3742

<https://www.experian.com/freeze/center.html>



TransUnion: 1 (888) 909-8872

<https://www.transunion.com/freeze>

You will need to provide your name, Social Security number, and other personal information. Fees are minimal and vary based on where you live. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. When and if you eventually chose to lift the freeze, you will definitely need this information. Taking the step to freeze your credit makes it more difficult for identity thieves to obtain new credit in your name.



Be aware, however, that a freeze will also prevent you from getting anything else that might require a credit check without contacting the credit agencies first and putting a temporary lift on the credit freeze. When you request the security freeze the agencies give you an 8 to 10 digit pin that is used when you want to lift the freeze. It can take 24 to 48 hours for this to go into effect and you can usually specify the lift for either a period of time or for a specific lender/retailer.

One other small drawback is that it costs, on average, \$10 per credit agency to put the credit freeze on and then each time you choose to temporarily lift it. Also, a credit freeze cannot stop someone who manages to get ahold of enough personal information to use your existing credit cards. But it will stop them from opening up new credit cards, or lines of credit.

How To Lift A Credit Freeze

To lift your freeze, contact the bureau used by the institution requiring your credit information and provide your PIN to lift the freeze—either temporarily or permanently. You can do this over the phone or online. A credit reporting company must lift a freeze no later than three business days after receiving your request. Again, fees will vary based on where you live.

Close accounts. Close any accounts that have been tampered with or established fraudulently.

- Call the security or fraud departments of each company where an account was opened or changed without your approval. Follow up in writing, with copies of supporting documents.
- Use the ID Theft Affidavit at [ftc.gov/idtheft](https://www.ftc.gov/idtheft) to support your written statement.
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Keep copies of documents and records of your conversations about the theft

What To Do If Your Identity Is Stolen

File a police report. File a report with law enforcement officials to help you with creditors who may want proof of the crime. Here is a link to get you started online: <https://www.bankrate.com/finance/credit/steps-for-victims-of-identity-fraud.aspx>

Report the theft to the Federal Trade Commission. Your report helps law enforcement officials across the country in their investigations.

To learn more about ID theft and how to deter, detect, and defend against it, visit ftc.gov/idtheft or call 1(877) ID-THEFT (438-4338) or TTY, 1(866) 653-4261. You may also request copies of ID theft resources by writing to:

Consumer Response Center
Federal Trade Commission
600 Pennsylvania Ave., NW, H-130
Washington, DC 20580

It's important to always be vigilant about fraud and phishing attempts from scammers. A helpful rule of thumb: if something seems out of the ordinary, use your intuition and ask questions before engaging with an unknown party or vendor.



Learn More:
www.privateocean.com