Here are U.S. PIRG's identity theft and privacy tips, including descriptions of different types of ID theft; checklists for preventing, detecting, and resolving ID theft; a checklist for protecting your online privacy; and links to additional resources.

# Types of Identity Theft

There are a variety of ways stolen data can be used, depending on what was taken. Different types of ID theft and fraud include:

## Financial Identity Theft

### Existing Account Fraud

If a thief obtains a credit or debit card number, the thief can access existing bank and credit accounts for in-person transactions.

### New Account Identity Theft

With a full name and Social Security number (SSN), a thief can open new credit accounts.

## Health Care/Medical Fraud

With a full name, birthdate, SSN (and sometimes an existing health insurance account number), a thief can attempt to receive benefits and services in your name.

## Social Security Benefits Fraud

With a full name, birthdate, and SSN, a thief can try to open a “my Social Security” (MySSA) account in your name and change your direct deposit information to his or her own checking account. Coupled with other information that can easily be found online, such as place of birth, a thief can also try to claim your benefits over the phone.

## Tax Refund Fraud

With a full name, birthdate, and SSN a thief can attempt to file your taxes and claim your refund.

## Other Fraud

With a full name, birthdate, SSN, and driver's license number (which can be turned into a fake license card), a thief can attempt numerous types of fraud, such as applying for a job, getting insurance, renting a home, or even committing crimes in your name.

## Reputational & Physical Harm

Some breaches involve personal information that can be used to blackmail, stalk, or otherwise inflict reputational or physical harm against data breach victims.

## Phishing

With just a phone number or email address, a thief can use "phishing" scams to attempt to collect more information needed to commit any of the above more severe crimes.

# Protect Yourself from Identity Theft

Use these checklists to help you prevent, detect, and resolve identity theft.

## Preventing Identity Theft

The first key to protecting yourself from ID theft is prevention.

### ID Theft Prevention for Online & Electronic Activity

- ❑ Consider locking your laptop at your work desk or when you're in a public place.
- ❑ Set passwords for your computer, smartphone, and tablet. Use six digits instead of four for your smartphone password.
- ❑ Set online account passwords that include at least 10 characters and a combination of capital letters, numbers, and symbols in the middle of the password, not the beginning or end.
- ❑ Avoid using the same password for different accounts. Consider using a password manager.
- ❑ Turn on two-factor authentication for your online accounts if available. You will receive additional codes for accessing your online accounts, in addition to your passwords.
- ❑ Keep all software updated. Turn on automatic updates for all software, including antivirus programs.
- ❑ Don't show information on social networking sites that is commonly used to verify your identity, such as date of birth, city of birth, mother's maiden name, name of high school, etc. If you do, don't use that information to verify your identity.

- ❑ Turn on your laptop's firewall and turn off file sharing and "network discovery" for public Wi-Fi connections.[1]
- ❑ Turn off automatic connections to Wi-Fi networks on your electronic devices.
- ❑ Send personal information online through fully encrypted websites or apps. Encrypted websites start with **https**. The non-profit Electronic Frontier Foundation has the **HTTPS Everywhere** extension for your web browser that will make sure you're using encrypted communications on websites that support encryption.[2] In addition to using encrypted websites, online transactions are best conducted over secure encrypted Wi-Fi connections[3] or your phone's data network,[4] versus an unsecure Wi-Fi connection.
- ❑ Consider using a Virtual Private Network (VPN) when in public.[5]
- ❑ Secure your home router. Steps for doing so are available on the Federal Trade Commission's website.[6]
- ❑ Disable Bluetooth connections on devices when not in use.
- ❑ Watch out for "phishing" scams where identity thieves request personal information by pretending to be a legitimate entity, such as a bank or the IRS. Ignore unsolicited requests for personal information by email, links, pop-up windows, texts, or over the phone - and only contact entities by means you know to be legitimate. For example, if you receive a call purportedly from your bank's security department, don't give out information. Instead, call the number on your bank card and ask for the security department.
- ❑ Use credit cards instead of debit cards for all online and in-person purchases if possible. Consumers have more legal protections against fraud with credit cards and can also avoid having to wait for stolen funds from checking accounts to be replenished. Consider only carrying debit cards for trips to the ATM or cash-back transactions.
- ❑ Sign up for your "my Social Security" (MySSA) account.[7] This will help prevent a scammer from opening an account in your name and changing your direct deposit information to his or her own checking account. A credit freeze on your Equifax credit report will also block the creation of a MySSA account because the Social Security Administration uses Equifax credit reports for identity verification.
- ❑ Dispose of your old computers and mobile devices safely to keep data out of the wrong hands. You'll want to look up steps for your specific device, but below are basic steps.

---

[1] "66 Ways to Protect Your Privacy Right Now", *Consumer Reports,* 21 February 2017.
[2] Electronic Frontier Foundation, *HTTPS:// Everywhere*, accessed at www.eff.org/https-everywhere, 31 August 2018.
[3] Federal Trade Commission, *Securing Your Wireless Network*, September 2015.
[4] Federal Trade Commission, *Tips for Using Public Wi-Fi Networks*, March 2014.
[5] Federal Trade Commission, *Virtual Private Network (VPN) apps*, March 2018.
[6] Federal Trade Commission, *Securing Your Wireless Network*, September 2015.
[7] 7 Social Security Administration, Create Your Personal My Social Security Account Today, accessed at www.ssa.gov/myaccount/, 31 August 2018.

For computers: Save data you want to keep and transfer, "wipe" or overwrite your hard drive many times, and keep it out of the landfill by recycling, donating, or reselling it.[8] (Deleted files can still be recovered if you don't wipe your hard drive clean many times.)

For mobile devices: Backup your phone, reset your device, remove or erase SD & SIM cards, and keep it out of the landfill by recycling, donating, reselling, or trading it.[9]

## ID Theft Prevention for Offline Activity

- ❑ Do not disclose your full nine-digit Social Security number unless absolutely necessary, and never use it as an identifier or password. Question those who ask for it. If someone calls claiming to be from your bank security department, it's best to hang up and call the number on your card.
- ❑ Lock your records and financial documents at home.
- ❑ Lock your mailbox if it is lockable.
- ❑ Shred documents containing personal information (name, account numbers, any part of your social security number, and birthdate) before throwing them away.
- ❑ Opt-out of pre-approved (pre-screened) credit & insurance offers. Credit and insurance companies buy "prescreened" lists from the credit bureaus to make pre-approved offers to prospective customers. While such offers provide consumers with information about possible credit options, identity thieves may steal these pre-approved offers and apply for them with your personal information. **Optoutprescreen.com** is the official website where by law you can opt out of receiving these offers for five years or permanently. You can also opt back in any time.[10] Note that this action only slows credit card and loan offers as only credit bureaus are subject to this rule. Airlines or retailers or others you do business with are not.
- ❑ Use the chip side of chip enabled cards, instead of the magnetic strip side, for in-person purchases whenever possible. Beware devices called skimmers[11] and shimmers[12] that criminals install on ATMs and card readers at checkout lines or gas pumps to steal your credit card information. When using ATMs and card readers, look and touch for signs of tampering, such as mismatched colors or loose parts. Always cover your hand while hand typing a PIN, and avoid using ATMs in secluded locations. ATMs at banks are the least likely to have skimmers.
- ❑ Use credit cards instead of debit cards for online and in-person purchases if possible. Consumers have more legal protections against fraud with credit cards and can also avoid waiting for stolen funds from checking accounts to be restored.
- ❑ Watch out for "phishing" scams where identity thieves request personal information by pretending to be a legitimate entity, such as a bank or the IRS. Ignore unsolicited requests for personal information by email, links, pop-up windows, texts, or over the phone - and only

---

[8] Federal Trade Commission, *Disposing of Old Computers*, September 2011.
[9] Federal Trade Commission, *Disposing of Your Mobile Device*, June 2012.
[10] OptOutPrescreen.com, accessed at www.optoutprescreen.com/, 31 August 2018.
[11] Max Eddy, "How to Spot and Avoid Credit Card Skimmers," *PC Magazine*, 15 February 2018.
[12] Brian Krebs, *ATM 'Shimmers' Target Chip-Based Cards*, 27 January 2017.

contact entities by means you know to be legitimate. For example, if you receive a call purportedly from your bank's security department, don't give out information. Instead, call the number on your bank card and ask for the security department.

- ❏ Place credit freezes on your credit reports. The "Credit Freezes: How to Prevent New Account Identity Theft" section of this report explains how to freeze your credit reports.
- ❏ File your taxes as soon as possible to help prevent tax refund fraud. A fraudster can still file taxes in your name even if you're not required to file taxes or aren't eligible for a refund. Also, some people qualify for an Identity Protection (IP) PIN that must be entered before a tax filing can be submitted. The IP PIN is available to identity theft victims and is also currently offered to all taxpayers in Florida, Georgia, and Washington, D.C., as part of a pilot program.[13]
- ❏ Protect your deceased loved ones from identity theft by notifying appropriate institutions of their deaths.[14]

## Detecting Identity Theft

- ❏ Check your monthly statements for unauthorized charges. Be suspicious of phone calls about surprise debts.
- ❏ Sign up to receive email and/or text notifications of account activity and changes to account information.
- ❏ Instead of paying for over-priced subscription credit monitoring, use your free annual credit reports as your own credit monitoring service. Every 12 months, federal law gives you the right to receive one free credit report from each of the three main credit bureaus, Equifax, Experian and TransUnion. Instead of requesting three at the same time, request one credit report from one of the bureaus every four months. Verify that the information is correct and that accounts have not been opened without your knowledge. Free credit reports are available online at **AnnualCreditReport.com**, by phone at 1-877-322-8228, or by mail.[15] There are other non-official sites that offer free reports too. Beware of sites that promise free reports and credit scores but may use trial-offer gimmicks to urge you to switch to paid credit monitoring or other services. There are some sites that offer no strings attached, free services - just expect to see ads. And know that the credit scores on those sites are most likely not FICO scores as used by most creditors.
- ❏ There are many other consumer reporting companies besides the three big nationwide credit bureaus that specialize in collecting other types of information about you, including bounced check activity, criminal and other public records, employment information, insurance claims, and tenant history.[16] Requesting free reports with these specialty bureaus every year could help

---

[13] Florida, Georgia, and Washington, D.C. were chosen for the pilot program because those locations have the highest per capita percentage of tax related identity fraud. Internal Revenue Service, Get an Identity Protection Pin (IP Pin), accessed at www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin, 31 August 2018.

[14] Sid Kirchheimer, "Protecting the Dead from Identity Theft," AARP Bulletin, accessed at www.aarp.org/money/scams-fraud/info-03-2013/protecting-the-dead-from-identity-theft.html, 31 August 2018.

[15] Federal Trade Commission, *Annual Credit Report Request Form,* accessed at www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf, 31 August 2018

[16] Consumer Financial Protection Bureau, *List of Consumer Reporting Companies*, 2018

you spot various fraudulent activities done in your name. Note that many of these companies will not have files on you at all. For example, if you've never had a bank account closed for "bounced check activity," it is likely that you won't have files at bounced check specialty bureaus.

- ❏ Sign up for your "my Social Security" (MySSA) account. Even if you don't receive social security benefits yet, checking your MySSA account can help you spot changes to your personal information that might indicate thieves trying to claim your benefits over the phone.[17]
- ❏ Request your driving record to help spot traffic violations committed in your name.
- ❏ Sign up for online accounts with your health care and insurance providers to monitor any fraudulent services on your statements.
- ❏ Be alert to notices about a tax return already filed, additional taxes you owe, refund offsets, collection for a year you didn't file, or records showing income from an employer for whom you did not work.
- ❏ Check if your online accounts have been hacked. Have I Been Pwned is a free tool you can use to check whether your online accounts may have been compromised in data breaches.[18]

## Resolving Identity Theft

- ❏ Take the following steps to resolve new account identity theft:

  **Step 1**: Notify your financial institutions. If you discover that your wallet, checkbook, credit card, or other sensitive information has been lost or stolen, immediately notify the issuing bank, credit card issuer, or relevant institution to close all existing accounts.

  **Step 2**: Get copies of your credit reports and place fraud alerts on them. If you haven't already, it's time to get freezes.

  **Step 3**: File an Identity Theft Report. If you suspect identity theft, report it to the Federal Trade Commission using the online complaint form at identitytheft.gov or by calling 1-877-ID-THEFT.

  **Step 4:** You might decide to file a police report.

- ❏ Visit **Identitytheft.gov**, the government's official website that will walk you through clear checklists of actions you can take to recover from new account identity theft and other types of fraud.[19]

---

[17] Social Security, *Create your personal my Social Security account today,* accessed at https://www.ssa.gov/myaccount/, 31 August 2018

[18] Troy Hunt, *Have I Been Pwned*, accessed at haveibeenpwned.com/, 31 August 2018.

[19] Federal Trade Commission, *Report identity theft and get a recovery plan,* accessed at https://www.identitytheft.gov/, 31 August 2018.

# Credit Freezes: How to Prevent New Account Identity Theft

Defense against any kind of identity theft starts with vigilance about protecting your personal information by taking steps such as creating secure passwords, keeping your social security number private, and shredding personal documents.

However, if and when someone does steal your information, there are a variety of ways it can be used, depending on what was taken. One of those uses is known as new account identity theft, where someone opens a new account in your name and then proceeds to rack up a ton of debt. New account identity theft can be prevented by getting security freezes, also known as credit freezes.

## What Are Credit Freezes & Why Should I Get Them?

A credit freeze blocks potential creditors such as a credit card company, a cell phone company, or a lender from viewing your credit report, which shows your credit history. Most creditors will not issue new credit to a customer if they cannot see that customer's credit report or the credit score derived from it from at least one of the three big nationwide consumer reporting agencies - Equifax, Experian, and TransUnion. (Consumer reporting agencies are also known as credit bureaus.) By blocking creditors from accessing your credit report, you're stopping identity thieves who apply for new accounts in your name with your stolen Social Security number.

Credit freezes do not affect your ability to use existing credit you already have, such as a credit card or loan. Nor do freezes affect your credit score. In fact, freezes help protect your score by preventing your credit from being negatively scored if someone racks up debt in your name.

You can easily remove a freeze or "thaw" your credit report when you want to apply for new credit. Freezes can be temporarily or permanently removed when you want.

Because creditors run credit checks with any one or a combination of the three big credit bureaus, you need to block access to your reports with all three.

## What Are the Differences Between Credit Freezes, Credit Locks, Credit Monitoring, and Fraud Alerts?

**Credit locks** offered by the credit bureaus appear to block access to credit reports the same way that credit freezes do. Therefore, freezes and locks both deny thieves the ability to open fake accounts in your name.

However, freezes are a right mandated by law, while locks are conditional on terms of use agreements that are set by the credit bureaus and could change at any time. Your rights as a consumer are on stronger ground with freezes. Whether you chose to get freezes or locks, remember you'll need to get them at all three national credit bureaus.

**Fraud alerts** don't block access to your credit reports, but they do notify creditors that they should try to verify your identity before opening a new account in your name. If you choose not to block access to your reports at the three main credit bureaus, you should at least place fraud alerts on your reports.[20]

**Credit monitoring** alerts you to changes to your credit reports, which can help you spot unauthorized credit accounts opened in your name. Credit monitoring can only help *detect* new account identity theft after it has already occurred, not prevent it.

## How Much Do Freezes Cost And When Do They Become Free Nationwide?

**A federal law eliminated fees for getting and removing credit freezes across the country at all big three credit bureaus on September 21st, 2018.**

## Do I Need to Freeze My Report with Other Credit Reporting Agencies?

As the Consumer Financial Protection Bureau lists, there are many other consumer reporting companies besides the three big nationwide providers of consumer reports.[21] Some websites have recommended getting freezes with Innovis and ChexSystems, but as far as we know, their reports are not used by creditors for credit approvals.

However, some news outlets have reported fraudulent accounts being opened by cell phone companies using credit reports provided by the National Consumer Telecommunications & Utilities Exchange

---

[20] Federal Trade Commission, *Place a Fraud Alert*, September 2017.
[21] Consumer Financial Protection Bureau, *List of Consumer Reporting Companies*, 2018.

(NCTUE).[22] **We therefore also recommend freezing your credit report at NCTUE, in addition to at the big three credit bureaus.**

## How to Freeze (and Unfreeze) Your Credit Reports

- ❏ You can place freezes online, over the phone, or in writing (info provided below)
- ❏ You will receive a PIN for your credit freeze with each bureau. You will use this PIN when you want to unfreeze your credit report to apply for new credit.
- ❏ If you want to temporarily lift a freeze because you are applying for credit, try to find out which credit bureau the business uses to check credit reports. You can save some money and time by only lifting your freeze for that credit bureau.
- ❏ You can temporarily lift a freeze for a particular creditor or for a specific period of time, from one day to one year.
- ❏ Make sure to account for the time it can take to thaw your report. In most cases if you request a thaw online or over the phone, your report can be unfrozen within 15 minutes. However, it can take longer if you don't have your PIN that was assigned to you when you froze your report, so make sure to keep your PIN in a safe, memorable place where you can quickly retrieve it when needed. It can also take up to three days of receipt of your request if you make it via postal mail.

**Equifax**

Online: https://www.equifax.com/personal/credit-report-services/

Phone: 1-800-349-9960 (automated), 1-888-298-0045 (live operator)

Mail: Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348

**Experian**

Online: https://www.experian.com/freeze/center.html

Phone: 1-888-397-3742

Mail: Experian Security Freeze, P.O. Box 9554, Allen, Texas 75013

[22] Kathy Kristof, "This Equifax credit database can boost your risk of phone fraud," *Moneywatch,* 16 May 2018.

Experian includes a potentially confusing three paragraph "Security Freeze Warning." They are just explaining that you will need to unfreeze your credit report before applying for credit if you ever wish to do so in the future.

**TransUnion**

Online: https://www.transunion.com/credit-freeze/place-credit-freeze

Phone: 888-909-8872

Mail: TransUnion LLC, P.O. Box 2000, Chester, PA 19016

**National Consumer Telecommunications & Utilities Exchange**

Online: https://www.exchangeservicecenter.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Phone: 1-866-349-5355

Mail: NCTUE Security Freeze P.O. Box 105561 Atlanta, GA 30348

# Protect Your Online Privacy

Although protection from identity theft is largely about data security, privacy also plays an important role. Data security and privacy often go hand-in-hand with each other. Privacy generally refers to the control or choice you have over how your personal information is used or shared. Data security refers to the measures put in place to protect that control and make sure data is used as intended.[23]

Use this checklist to help you control how your personal information is used or shared online.

- ❏ Cover the camera on your laptop to prevent hackers from watching and recording you.
- ❏ Consider your options for blocking websites, advertisers, and others from tracking your online activity on your computer, including: adjusting your cookies settings on your browser, installing a tracking blocker for your web browser, or opting out of targeted advertising.[24] Note that "private browsing" settings by themselves still allow your activity to be communicated to third-parties *during* a browsing session.

[23] Laura Moy, Center on Privacy & Technology at Georgetown Law, *Statement Before the Financial Services Committee Hearing on Continuation of Hearing Entitled Examining the Equifax Data Breach*, 25 October 2017, 18.
[24] Federal Trade Commission, *Online Tracking*, June 2016.

- ❑ Consider your options for blocking advertisers from tracking your online activity on your mobile device, including turning off ad tracking and resetting "device identifiers."[25] You can also research ways of controlling ad tracking on your other smart devices, such as internet connected entertainment systems.
- ❑ Check the privacy settings on your mobile device to control the access that different apps have to your personal information, including location, personal contacts, photos, calendar, and health data.[26] Many apps have the ability to track your location **even when you're not using them**.
- ❑ Check your privacy and other settings in your Facebook account to control tools such as face recognition, location history, and ad preferences.[27]
- ❑ Check your privacy settings in your Google account to control tools such as the collection of your web searches and other activity and the ads you see.[28]
- ❑ Check your privacy settings in your other apps and social media accounts.

# Identity Theft & Privacy Resources

- AnnualCreditReport.com (Phone and mail options available.[29])
- Consumer Federation of America's IDTheftInfo.org[30]
- Consumer Reports' "66 Ways to Protect Your Privacy Right Now"[31]
- Electronic Frontier Foundation's HTTPS:// EVERYWHERE[32]
- Facebook's privacy and security page[33]
- Google's privacy and security page[34]
- Have I Been Pwned[35]
- Krebs On Security[36]
- OptOutPrescreen.com[37]

---

[25] Ibid.
[26] Federal Trade Commission, *Understanding Mobile Apps,* February 2017.
[27] Facebook, *Tools to Help You Control Your Privacy and Security on Facebook,* accessed at www.facebook.com/privacy/, 31 August 2018.
[28] Google, *Privacy*, accessed at privacy.google.com, 31 August 2018.
[29] See "Free Credit Reports," FTC Fact Sheet, available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports
[30] Consumer Federation of America, *IDTheftInfo.org*, accessed at idtheftinfo.org/, 31 August 2018.
[31] Consumer Reports, *66 Ways to Protect Your Privacy Right Now*, 21 February 2017.
[32] Electronic Frontier Foundation, HTTPS:// Everywhere, accessed at https://www.eff.org/https-everywhere, 31 August 2018.
[33] Facebook, *Privacy,* accessed at https://www.facebook.com/privacy/, 31 August 2018.
[34] Google, *Control, protect, and secure your account, all in one place*, accessed at https://myaccount.google.com/, 31 August 2018.
[35] Have I Been Pwned, accessed at https://haveibeenpwned.com/, 31 August 2018
[36] Brian Krebs, Krebs on Security, accessed at krebsonsecurity.com, 29 August 2018.
[37] Opt Out of Prescreen, accessed at https://www.optoutprescreen.com/, 31 August 2018.

- Privacy Rights Clearinghouse[38]
- The Federal Trade Commission's IdentityTheft.gov website[39] & Online Security tips[40]
- The Identity Theft Resource Center[41]
- The Social Security Administration's "my Social Security" website[42]
- U.S. PIRG's Identity Theft & Privacy Checklists[43]

[38] Privacy Rights Clearinghouse, accessed at www.privacyrights.org/, 31 August 2018.
[39] Federal Trade Commission, *Report identity theft and get a recovery plan,* accessed at https://www.identitytheft.gov/, 31 August 2018.
[40] Federal Trade Commission, *Online Security*, accessed at https://www.consumer.ftc.gov/topics/online-security, 31 August 2018.
[41] Identity Theft Resource Center, accessed at www.idtheftcenter.org/, 31 August 2018.
[42] Social Security, *Create your personal my Social Security account today,* accessed at https://www.ssa.gov/myaccount/, 31 August 2018.
[43] U.S. Public Interest Research Group, *Identity Theft and Privacy Checklists,* 3 August 2018.