

A stylized globe with a network overlay of lines and dots. A silhouette of a world map is overlaid on the globe, with a red-to-orange gradient on the left side. The background is a light gray grid of lines and dots.

IDENTITY THEFT

PROTECTING YOUR
ASSETS IN A HIGH-TECH,
HIGH-RISK WORLD

YOU'RE STANDING IN LINE AT TARGET, and it's Armageddon as usual. As you wait for the ten customers ahead of you to scan and purchase, you check your Facebook and find the item you've been eying is finally on sale! Score. You click, log in, and since your favorite store already has your credit card information saved, your purchase is a breeze. By the time you receive your confirmation email, it's time to pull out your debit card and swipe for your Target loot. These types of multifaceted transactions are more common than ever. Convenience is at our fingertips, we have nearly constant access to the internet, and we have more ways to pay than most of us could have fathomed fifteen years ago. But with all these amazing changes have come new challenges, especially in terms of cybersecurity. Identity theft is the criminal use of an individual's personal identification information (PII). Identity thieves steal PII such as your name, social security number, driver's license information, bank and credit card accounts, and use that information to establish credit, make purchases, apply for loans, or even seek employment. Identity theft isn't a new phenomenon; in fact, recorded instances of identity theft date back to the dark ages.¹ However, the face of identity theft has changed dramatically, evolving with the technology and economic landscape that surrounds it. Understanding your exposure and staying informed of the trends and methods that thieves use to steal from you is the first step in a strong defense against identity theft.



HOW AM I EXPOSED?

This answer is simple: every time you provide PII of any kind, you're exposed. Whether you swipe your card in person, fill out your social security number on a government form, mail a check, or make a purchase online, you're putting your PII out into the world. Aside from going completely off-grid, there's genuinely no way to avoid it.

Throughout your life—even just throughout a given day—you might do the following:

- Apply for a credit card or loan
- Use a debit card or credit card in person or online
- Use public Wi-Fi
- Mail financial documents
- Write a check
- Switch service providers
- Speak with a customer service representative
- Fill out a medical form
- Use social media

It's nearly impossible to eliminate your exposure entirely, but there are measures you can take to prepare and protect yourself so that you can avoid costly and frustrating breaches of your personal information.





WHERE DO IDENTITY THIEVES GET A HOLD OF MY PII?

Getting a hold of your information isn't as complicated as you might think. In fact, much of your PII could be publicly available online or through public records such as court documents.

Here are just a few examples of how your PII can be found, taken, or stolen:

IMPOSTER SCAMS: Fraudsters may pose as a professional from a bank, the IRS, a utility company, a charity, or another reputable institution in an attempt to gather PII directly from you. These scams often rely on a sense of urgency, insisting that you must send funds immediately. Remember to take a moment when you receive a call like this and ask yourself if the urgency makes sense. Government agencies don't demand immediate payment over the phone; they communicate by the U.S. Postal Service and send multiple notices. If a Nigerian prince or foreign diplomat calls asking for an urgent loan that they'll pay back with 300% interest, ask yourself why they'd be reaching out to you for such a loan. If it sounds overly urgent or too good to be true, hang up. If you're concerned that you might owe money to a legitimate company, hang up and reach out to the company directly with information from their official website. Don't call back the number that dialed you or use any contact information given to you over the phone.

PHISHING: Similar to an imposter scam, phishing involves emails that appear to be sent from a reputable company in an attempt to gather information from you directly. A phishing email might redirect you to a form to fill out or ask you to reply with PII such as account numbers, your social security number, or other sensitive information. These emails can be difficult to spot, but they often contain vague greetings such as "dear valued customer" or "dear client." You may also spot misspellings in the web domain or the company name. **Note:** Most secure companies such as banks, utility companies, and government agencies will direct you to log in to your account rather than direct you to a strange link. When in doubt, call the company directly (don't use any phone number listed in the email) or log in directly from the official site (never use a link from the email).

PUBLIC DOCUMENTS: Your PII may be readily available in court files, county property appraiser websites, government contracts, civil records, voter registrations, or occupational licenses you hold. Although these records contain sensitive information, they can still be made public. Establishing a trust, business identity, or a P.O. Box are a few steps that can help keep your PII private. Social media posts, photos, check-ins, and tags can also be public without your knowledge or consent. Always be wary of where and what you post. A photo in front of your new home, a travel check-in, a picture of a car with your visible license plate... these are all avoidable mistakes that can cost you. Always double check your photos for privacy to ensure that your posts aren't putting you at risk.

DUMPSTER DIVING: Thieves often resort to digging through trash or intercepting mail for financial statements or anything else they might find useful. Always shred sensitive documents, medical records, expired credit cards, and identification cards. Also, consider switching your accounts to paperless statements and electronic bill pay to avoid the risk of your mail being intercepted, another common practice for stealing sensitive information.

SKIMMING: This process involves an illegitimate storage device that a thief has installed on a machine where you might process your card, such as an ATM or at a gas station pump. When you process your card, the skimmer reads the magnetic strip and stores your information. In some cases, the skimmer can also capture your PIN. Your best defense against skimming devices is using credit cards with chip technology. EMV chip cards produce a unique cryptogram for every transaction, rather than storing all the information in a reusable format as the magstripe technology does. In fact, chip technology has already reduced counterfeit fraud by 76%.²

SHOULDER SURFING: Some thieves may use a camera or binoculars to obtain your card information and PIN as you use an ATM or input information online. Covering the keypad whenever you input your PIN is a simple measure that can protect you when you use ATMs, pay for gas, or withdraw cash at the grocery store. If you often work or shop in public on your devices, investing in privacy glass is another cost-effective way to combat shoulder surfing. Privacy glass screen protectors are widely available and make your screen difficult to see from any angle other than directly in front of you.

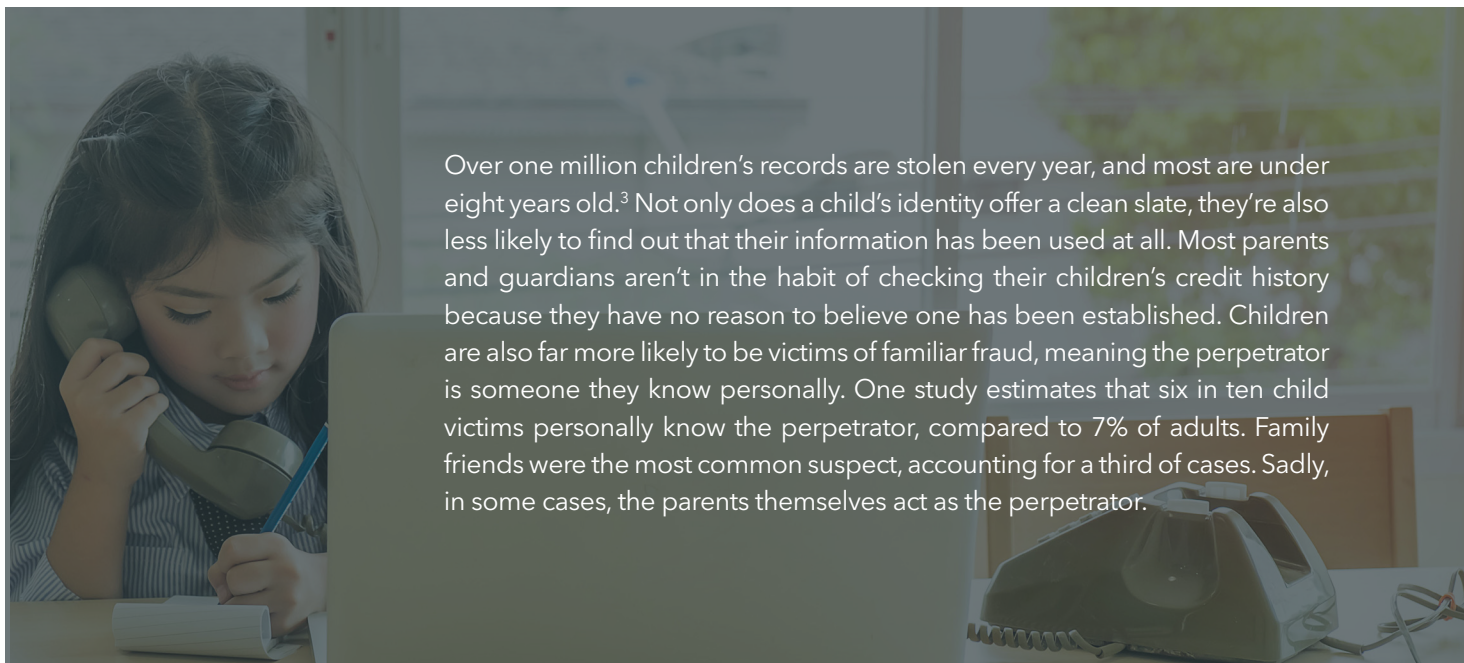
MASS BREACHES: Unfortunately, no matter what measures you take to protect yourself, the vast array of companies that store your PII can also be breached. Widespread data breaches occur when hackers gain access to personal data stored within a company's system, such as account information, names, addresses, and login and password combinations. Your best defense against data breaches is never re-using passwords across sites so that if your PII is stolen at one company, the hacker hasn't gained access to your accounts across any other platforms.

Once your PII is stolen, it can be used illegitimately in many ways: a fraudster can steal funds directly from your accounts, apply for a loan or credit card with your information, apply for a false driver's license with their picture and your name, commit crimes under your identity, redirect your mail to themselves, or sell your PII on the black market for other criminals to use. The bottom line is, once your information is stolen, it can get out of hand very quickly, costing you time and money to rectify.



I'M NOT RICH. AM I STILL AT RISK?

Many people make the mistake of assuming that if they're not "wealthy," then nobody is after them. First of all, rich is relative. You may think that your nest egg is a humble one, but it could be a pot of gold to the criminals that target you. There's also a great deal of value in good credit and a clean background. Even without a penny to your name, you have plenty to lose if you have decent credit and no criminal record. Criminals can use your clean slate to get into debt, use your medical insurance, sign a lease, and many other activities aside from directly stealing funds from your accounts. Clean slates are so valuable that minors are regularly targeted for identity theft.



Over one million children's records are stolen every year, and most are under eight years old.³ Not only does a child's identity offer a clean slate, they're also less likely to find out that their information has been used at all. Most parents and guardians aren't in the habit of checking their children's credit history because they have no reason to believe one has been established. Children are also far more likely to be victims of familiar fraud, meaning the perpetrator is someone they know personally. One study estimates that six in ten child victims personally know the perpetrator, compared to 7% of adults. Family friends were the most common suspect, accounting for a third of cases. Sadly, in some cases, the parents themselves act as the perpetrator.



HERE ARE SOME STEPS YOU CAN TAKE TO PROTECT YOUR CHILD'S IDENTITY:

KNOW WHO HAS ACCESS TO IT: Whether you enroll your child in school, summer camp, or recreational activities, keep track of the forms you've filled out that contain your child's personal information. Having a record will help you in the unfortunate event that your child's PII is compromised. Also, be sure to read privacy policies and terms when you share any personal information. Some groups may share PII with other local groups or agencies, and you may have the option to deny consent.

SEE IF YOU CAN OPT-OUT: It's understandable that when you enroll your child in little league, the league will need some PII such as name, address, contact information, and guardian. But do they really need your child's social security number? Ask them. These extracurricular groups often download forms online and may not need every field to be filled out to allow your child to participate.

RECOGNIZE THE SIGNS: If your minor child or dependent gets summoned for jury duty or receives a credit card offer in the mail, don't ignore it. It could be an indication that their PII has been used to open accounts or create an illegitimate identity. Call the institution directly, make formal inquiries, and keep track of any letters, statements, or summons for future reference.

CREDIT FREEZE: All three major credit bureaus offer credit freezes for minors. A credit freeze makes it very difficult for anyone to use your child's information to take out loans or open new accounts. This is a good option if you don't plan to monitor your child's credit and accounts regularly.

EDUCATE YOUR CHILD: Teach your kids not to share their information with anyone, especially online. If your child shops or plays games online, they might be asked to provide some of their PII. Teach them to involve you in this process so you can monitor and advise them on how to protect themselves. Once they're ready, you can have them participate in opening student bank accounts, building their credit, and monitoring their own finances properly.

The truth is anyone can be a victim of identity fraud regardless of wealth or age. Currently, Millennials are the most likely age group to become victims of identity theft,⁴ although older victims suffered greater financial losses in comparison. No matter what your age, wealth level, or online presence, identity theft is a serious threat to all you've worked for, and it shouldn't be taken lightly.

HOW CAN I PROTECT MYSELF?

1. BE DISCRETE, AWARE, AND ORGANIZED

Don't share personal information in public places over the phone or public Wi-Fi and avoid sharing any PII that isn't completely necessary.

Know where your information is stored and which companies, individuals, and institutions have access to it. Read disclosures and privacy policies to understand if and how your PII can be shared.

Avoid public computers that may contain viruses or have been tampered with.

Don't share your passwords. A 2020 survey found that 79% of Americans admit to sharing passwords despite the risks.⁵ If you share accounts such as Netflix, use a totally new password unrelated to other accounts—especially financial ones.

Don't overshare on social media. Travel details, new addresses, phone numbers, and photo identification shouldn't be posted on your profile where they're easy to find and exploit. Even check-ins can indicate that your home is empty or allow others to predict your social schedule, including when you leave your home.

2. USE STRONG AND DIVERSE PASSWORDS AND MULTI-FACTOR AUTHENTICATION

Nearly one third (29%) of hacking-related breaches took advantage of stolen passwords.⁶ Re-using passwords across multiple sites and accounts heightens the risk that one hack will expose multiple accounts to theft. Make sure all your passwords are unique, diverse, and strong.

Consider enabling multi-factor authentication for further protection. Even if your password falls into the wrong hands, multi-factor authentication offers another level of verification. This additional authentication factor could be a fingerprint, a registered device, a passcode sent to your email or phone number, a security key, or security questions.

TIPS FOR A STRONG PASSWORD:

Use a different password for each account. If it gets stolen, your other accounts can't be overtaken.

Get creative. Mix letters, numbers, and special characters. Never use names or dates that others can guess or find such as anniversaries, pets, birthdates, etc.

Use ten or more characters. A longer password is tougher to hack. Using numbers and symbols that resemble the letters they're replacing can help make your password memorable.

Change your password several times per year.

3. MAINTAIN SOFTWARE UPDATES, ANTIVIRUS, VPN, AND FIREWALLS

Outdated software is easier to hack, so make sure you keep your devices updated with the most current software available.

Invest in software that can protect you, such as VPN, antivirus, and firewalls.

Don't shop or access sensitive information over public Wi-Fi. If you frequently need access through public Wi-Fi, invest in VPN software.

Don't underestimate the sites you frequent. You may think logging onto public Wi-Fi to browse your favorite store sounds pretty harmless, but if you have your credit card information stored on that site, your PII could be exposed.

Research apps before you download them to ensure they're from a trusted source.

4. USE A PASSWORD MANAGER

Managing many unique and complex passwords can be overwhelming, especially if you change them periodically (as you should). A password manager allows you to store all your usernames and passwords in an encrypted state, while you only need to use one "master" password to access the manager. The app auto-generates strong passwords for each account and auto-fills your login fields for you.

Note: You can still enable multi-factor authentication for enhanced protection.

5. SWITCH TO PAPERLESS

Paperless statements limit the amount of mail that can be stolen or intercepted and limit the sensitive documents you have around your house, waiting to be shredded or filed. Additionally, e-statements require a login, which is much more secure than a mailbox.

Paying bills online is also more prudent than sending a check since a check can be altered and potentially used for fraud. Keep in mind that a check displays your account number, name, address, and banking institution all in one place—a great starter-kit to commit fraud.

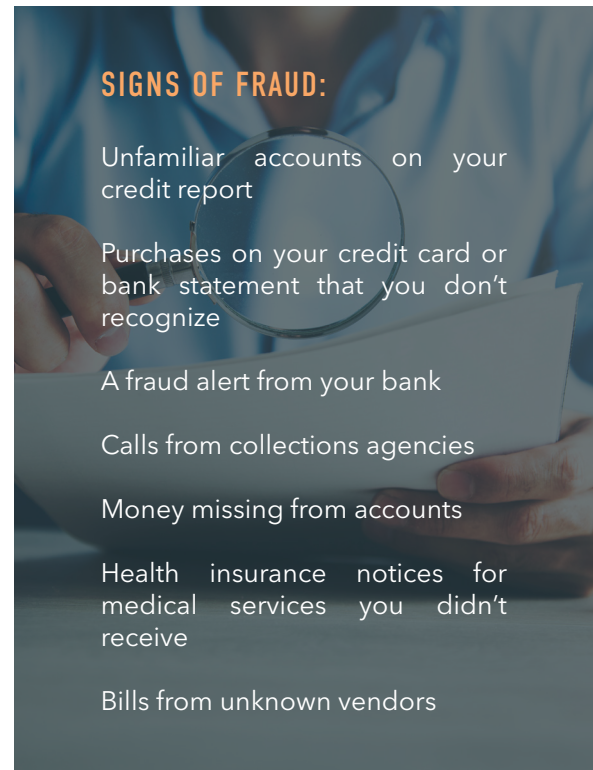
Scan and save your wallet contents so that if your wallet is stolen, you'll have a list of companies to contact when you replace your cards and report the theft. This will make it more difficult for the thief to use the stolen information. You can use this same method to keep track of any documents you bring on vacation. **Note:** Avoid taking all your cards when you travel, and make sure you submit a travel notification with your bank.

6. SCRUTINIZE MAIL, STATEMENTS, AND CREDIT REPORTS

Whether you receive your statements physically or electronically, make sure you're looking over them closely and regularly. If you see something strange, investigate. Loan offers for a minor, unfamiliar statements, bills from unknown vendors, and unfamiliar purchases could indicate that you've been compromised. Contact vendors and institutions using the information on their official website to make any inquiries.

Check your credit report regularly. You may have access to updated credit reports through your bank or a private credit reporting site. Stay abreast of any changes to ensure that you're the only person using your credit.

Be sure to file or shred any sensitive physical documents properly. Loose documents are a liability. If you can't store them securely, consider scanning them and saving them in a password-protected folder.



7. OPT-OUT OF TELEMARKETING AND UNSUBSCRIBE FROM JUNK MAIL

Unnecessary phone calls and junk mail might not put you at risk directly, but it's more difficult to spot strange calls and emails when you're inundated with unwarranted communications. When you're accustomed to only receiving calls and messages that you expect and welcome, the strange ones will stand out, allowing you to report them appropriately.

When you spot a spam email, mark it as spam so that your email provider can filter them more effectively in the future. You can also report fraudulent phishing emails to appropriate anti-phishing groups. For example, your bank likely has a dedicated fraud department where you can forward phishing emails. This helps them tighten security measures that protect their entire client base, including you.



You can opt-out of telemarketing calls by registering with the Do Not Call Registry at 1-888-382-1222. You can also call 1-888-5-OPTOUT to opt-out of credit and insurance offers.




Keep in mind that the IRS will never call you to ask for private information. Most medical providers and government agencies will contact you through the U.S. Postal Service or your secure messages via your online account. Report IRS scams and spam emails to TIGTA's IRS Impersonation Scam Reporting [treasury.gov/tigta](https://www.treasury.gov/tigta) or call 800-366-4484. You can also report them to the Federal Trade Commission's FT Complaint Assistant on [FTC.gov](https://www.ftc.gov).



8. RECOGNIZE WHEN YOU'RE BEING TARGETED


Stay abreast of current imposter and advance-fee scams. A scam that works well will often gain popularity and will continue to be used until folks come to recognize it. The "Nigerian Prince" scam, for example, has been used for over ten years. Although many people know about it and recognize it, it still costs victims over \$700,000 per year.⁷ Also, beware of scams that occur during specific times of the year, such as IRS and Social Security scams, which are popular during tax season, and student loan scams, popular in spring and summer.

HERE ARE SOME CURRENT SCHEMES AND THE RED FLAGS TO LOOK FOR

FOREIGN LOTTERY: Congratulations! You won the lottery in Haiti ( unfamiliar vendor, too good to be true). Pay taxes in advance ( advance-fee) and collect your winnings!

FAMILY EMERGENCY: Your granddaughter calls you from a strange number ( unfamiliar vendor). You can barely hear her, but she's in trouble and needs money right away—just don't tell her parents ( urgency)! The scammer may even specifically tell you not to hang up and that their regular phone isn't available ( improbable). Hang up, take a moment, and call your grandchild back on their regular phone number. You'll likely find that they're just fine. Other variations of this scheme can involve an old friend you haven't heard from in a while who urgently needs your help. Sometimes it's a phone call, but it can also come from a hacked email address or Facebook profile.

BUYER OVERPAID YOU: You're selling a collectible on eBay for \$5,000. The buyer "accidentally" sends you a \$10,000 check ( too good - or too strange - to be true). They want you to send a refund for the overpayment ( advance-fee). With online transactions, always avoid any strange deviation from the standard transaction process. If eBay's typical process is: receive payment through Paypal, ship item, receive confirmation, then don't engage in a transaction with someone that wants to deviate from that process.

VALUABLE ITEM STUCK IN CUSTOMS: A friend can't get their valuable item through customs. If you help them pay a customs fee ( advance-fee), they'll reward you later.

URGENT LOAN TO HELP A DIPLOMAT OR FOREIGN OFFICIAL:

These are variations of the Nigerian prince scam. The diplomat has millions that he can't access (Δ urgency), but if you give him a "small" loan (Δ advance-fee), he will reward you (Δ too good to be true).

ONLINE ROMANCE:

After chatting online with someone interesting and charming for a few weeks, or even months, you become more than friends. You discuss meeting in person, but your new beau doesn't have money for a ticket, can't travel for legal reasons, or has some other obstacle that can be solved with a little financial help from you (Δ advance-fee). Other variations of this scheme can involve a non-romantic friendship where your new friend has a family or medical issue and asks you to send money (Δ urgency). Most of these schemes involve a perpetrator that claims to live in another country where bizarre obstacles can be explained as cultural differences or lack of privilege that you can help with.

ONLINE DISTRIBUTION OPPORTUNITY:

You apply to a job opportunity where you can work remotely. You're hired by a company you've never heard of (Δ unfamiliar vendor), they ask you to open a bank account where funds will be deposited, and you'll be directed to distribute these funds as part of your job function (Δ too strange to be true). Ask yourself why a reputable company would trust a brand new employee with their money. These scams are designed to put you at the center of an illegal activity such as money laundering.

Risk is a part of the world we live in. We may not be able to avoid it completely, but if you stay informed and work with professionals that understand the current landscape, you can stay a step ahead. Our professionals are happy to help you implement any of the measures discussed here to ensure that you're protected.

STEPS TO TAKE IF YOU'RE A VICTIM OF IDENTITY THEFT:

Report the incident to the fraud department of the **three major credit bureaus** and ask for a hold to be placed on your credit

Contact the fraud department of each of your creditors

Contact your bank or financial institution

Report the incident to law enforcement

Download and print materials free:
www.ftc.gov/bcp/edu/microsites/idtheft

[1] <https://www.irisidentityprotection.com/blog/write-your-own-life-story/>

[2] <https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html>

[3] <https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html>

[4] <https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/>

[5] <https://www.thezebra.com/resources/home/dangers-of-sharing-passwords/>

[6] <https://www.morganstanley.com/articles/protecting-your-security-online-banking>

[7] <https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html>