idwatchdog®

Your Guide to Identity Theft

How It Happens, What to Watch For, and How to Better Defend Against It

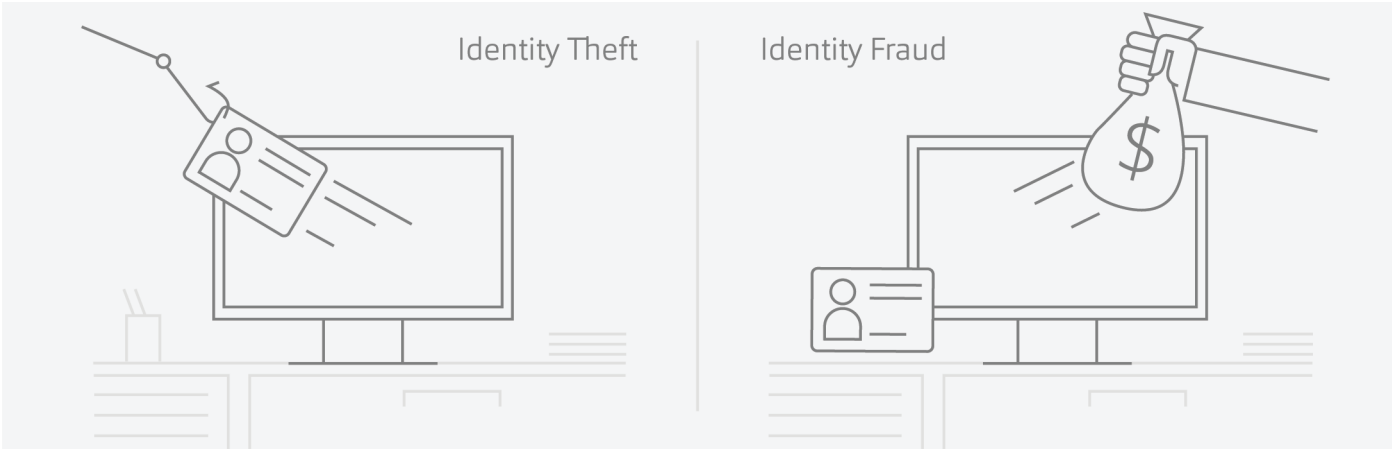
When people hear the words "identity theft," what typically comes to mind are fraudulent credit card charges or illicit bank withdrawals. But the reality of identity theft is more complex. In fact, financial identity theft is only one type of identity crime, and others can be more difficult to detect.[1]

Identity thieves can not only drain bank accounts and rack up credit card charges, but they can get medical treatment using the victim's health insurance, steal their tax refund,[2] or sell the information to other criminals.[3] In some extreme cases, a thief might even give the victim's name during an arrest and prompt a false criminal record. Identity theft victims may be unaware of the crimes until there is already substantial damage to their financial assets, credit, and reputation.[3]

This paper will explore the wide range of identity theft, including financial, tax-related, medical, employment, child, and criminal, and the impacts of identity fraud. It will also cover common warning signs and discuss how identity theft typically happens as well as steps individuals can take to better protect themselves and their loved ones.

Identity Theft vs. Identity Fraud

Though sometimes used interchangeably, identity theft and identity fraud are two different things.[4] Identity theft is when a victim's Personal Identifying Information (PII) is stolen. Stolen PII could include the victim's name, address, Social Security number, or other identifying numbers such as medical insurance or credit card accounts.[5] Identity fraud occurs when thieves use that information for illicit gain.[4]



idwatchdog®

Financial Identity Theft

New Account Fraud Jumped by 88% in 2019

According to the 2020 Identity Fraud Study from Javelin Strategy & Research, there were 13 million identity fraud incidents in 2019, totaling $16.9 billion in losses.[6]

Thieves May Open New Accounts—And They Can Be Difficult to Detect

New account fraud, in which a thief opens a brand-new account in the victim's name, jumped by 88 percent in 2019.[7] The most common types of new accounts that scammers open are online accounts such as eBay or Amazon, checking or savings accounts, and credit card accounts.[6]

According to experts, victims are much less likely to discover new account fraud on their own, and financial organizations are less likely to have a way to contact victims.[8] The most common way victims discovered new account fraud in 2018 was by notification from a credit monitoring or identity protection service.

Credit Card Fraud Still Prevalent

Credit card fraud tops the list of identity theft crimes[7] and some experts estimate that over 80 percent of credit cards currently in people's wallets have already been compromised.[9]

While microchips in credit cards have reportedly helped curb in-store fraud, experts say that mobile and online transactions are now the low-hanging fruit.[9] As a result, card-not-present fraud, a scam in which the credit card is not physically used such as for online or phone transactions,[10] has ballooned in recent years.[9]

Crooks use stolen credit card information to impersonate the cardholder and make online purchases.[9] Today's sophisticated cybercriminals may even route fake orders through a computer in the same region as the victim to avoid raising the retailer's suspicion.

How Stolen PII Is Used for **Financial Fraud** and the Potential Impact

- Impersonate the victim to make online purchases the victim may have to pay for or resolve with their financial institution
- Open new online accounts, checking accounts, or credit card accounts the victim may be responsible for

idwatchdog®

Tax Identity Theft

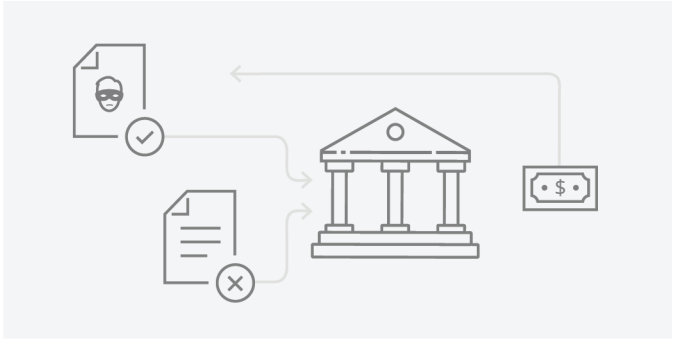
Thieves Aim to File a Fake Tax Return Before the Victim Does

According to the IRS, tax-related identity theft is one of the most common tax scams.[11] Tax identity theft occurs when a criminal uses the victim's Social Security number to file a fraudulent tax return.[12] Victims may not know the crime has happened until the IRS rejects their tax return as a duplicate filing.[13]

Experts Recommend Filing Taxes Early

In recent years, the IRS has advised taxpayers to file as early as possible—and with good reason.[14]

The IRS accepts only one tax return per Social Security number, so if a taxpayer can file their authentic tax return before a potential criminal can file their fraudulent one, they may be able to beat an identity thief to the punch.[15] On the other hand, if a criminal succeeds in filing their fraudulent return first, it could take months for the victim to resolve the issues.[16]



...if a criminal succeeds in filing their fraudulent return first, it could take months for the victim to resolve the issues.

How Stolen PII Is Used for **Tax Fraud** and the Potential Impact

- File a fraudulent tax return in the victim's name and collect their refund before they have a chance to file
- Cause the victim's own tax filing to be rejected, resulting in delays and issues with the IRS

idwatchdog®

Medical Identity Theft

Fictitious Medical Information Could Plague the Victim for Years

According to the World Privacy Forum, medical identity theft can cause great harm to its victims, as it often results in falsified information being entered in the victim's medical records that can plague their medical and financial lives for years.[17]

101% Increase in Medical Identity Theft in 2019

Medical identity theft is when a criminal submits fraudulent claims to the victim's health insurance or Medicare[18] or uses the victim's information to get treatment, prescription drugs, medical devices, or other benefits.[19] It can lead to tens of thousands of dollars in damages.[20]

One reason why fraudsters may target healthcare data is that it can have a longer shelf life than financial information and is more difficult for the victim to change or cancel.[21] The FTC reported a 101 percent increase in medical identity theft cases in 2019.[19]

The More Costly and Least Understood Type of Identity Theft

Medical identity theft is one of the most difficult types of identity theft to repair,[22] and it can cost far more than financial identity theft.[19] Federal law generally limits consumers' liability for fraudulent credit card charges to $50, but there are no such protections for a stolen medical identity.[19]

If a criminal gets treatment in the victim's name, erroneous medical records could cause treatment delays, incorrect prescriptions, or misdiagnoses.[19] It could even affect the victim's ability to get medical care and insurance benefits in the future. Despite this risk, experts say that medical identity theft is the least studied and most poorly documented of identity theft crimes.[17]

How Stolen PII Is Used for **Medical Fraud** and the Potential Impact

- File erroneous medical claims the victim has to pay
- Use insurance for medical diagnoses that the victim does not have and could result in future misdiagnoses, treatment delays, or incorrect prescriptions
- Max out insurance payout which cancels the policy, leaving the victim without insurance and potentially making it more difficult to get new insurance

idwatchdog®

Employment Identity Theft

Opposing Goals: Thieves Seeking Employment—Or Unemployment Benefits

In employment identity theft cases, scammers may file fraudulent unemployment claims,[23] or alternatively, they may use a falsified or stolen ID to get a job using the victim's identity.[24] Victims may learn of employment fraud when their employer asks why they have applied for jobless benefits[25] or receive a W-2 or 1099 from an unfamiliar employer.[24]

Employed or Not—Anyone Can Be a Victim

In many cases, fraudulent unemployment payments are deposited into bank accounts controlled by the scammers.[26] However, suppose payments are sent to the victim's legitimate bank account instead. In that case, the criminals may contact the victim by phone, email, or text message and impersonate an unemployment official in an attempt to get them to transfer the funds.

According to the Internet Theft Resource Center (ITRC), anyone can be a victim of unemployment benefits fraud, and individuals both with and without a current position have been impacted.[25]

According to the Internet Theft Resource Center (ITRC), anyone can be a victim of unemployment benefits fraud...

How Stolen PII Is Used for **Employment Fraud** and the Potential Impact

- File fraudulent unemployment benefits claims that the victim has to resolve with their employer or the IRS
- Use the victim's identity to get a job, which could lead to problems resolving misreported income

idwatchdog®

Child Identity Theft

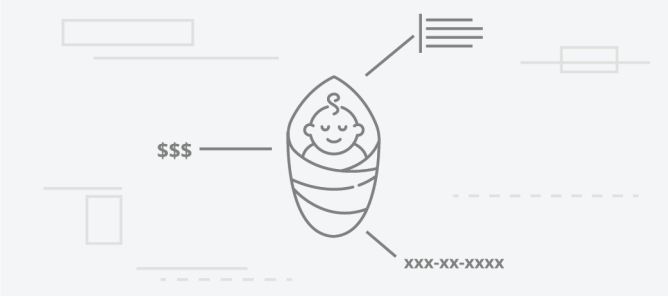
Children Can Be the Perfect Mark for Identity Thieves

Many parents assume that their children are safe from identity theft because of their young age and lack of credit history. However, for identity thieves, children can be the perfect mark.[27] While thieves may target adults for the money in their accounts, a child represents a clean slate for opening new lines of credit.

Child Identity Theft Can Go Undetected for Years

The identity theft of a child can go undetected for years—or even decades.[28] And the consequences can be devastating.[29] When the child becomes a young adult and seeks independence, they may have problems with banks, landlords, utility companies, and potential employers due to their negative credit history.

While thieves may target adults for the money in their accounts, a child represents a clean slate



Identity thieves only need a Social Security number to commit synthetic identity theft, in which a victim's real Social Security number is combined with a fake name, address, and date of birth to apply for credit or commit other types of fraud.[30] Synthetic identity theft—and especially its use in stealing children's identities—can negatively affect young people in the future.[31]

In many cases, identity theft of a child takes place in the child's own home—or close to it. It's estimated that 60 percent of child identity fraud victims personally know the perpetrator.[32]

How Stolen PII Is Used for **Child Identity Fraud** and the Potential Impact

- Open new lines of credit or loans that go into collection or default and remain on the child's credit
- Damage a child's credit and make it difficult for them to qualify in the future for student loans, get credit cards, or rent a place to live

Criminal Identity Theft

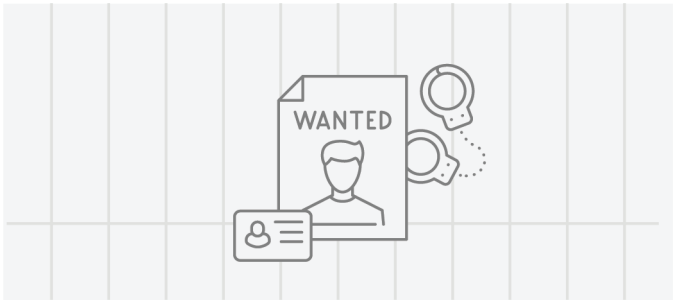
An Identity Thief's Crimes Can Become the Victim's

Though rare, criminal identity theft can occur when someone cited or arrested for a crime uses the victim's name and identifying information, resulting in a criminal record in the victim's name.[33] Criminals may steal a victim's identity to commit a crime, enter a country, get special permits, hide their own identity, or commit acts of terrorism.[22]

Victims May Be Unaware They Have a Criminal Record

An identity thief, using the victim's name or personal information, may sign a citation or be required to appear in court.[34] When neither thief nor victim appear in court, the judge may issue an arrest warrant, or a criminal record may be created in the victim's name.

The victim is often unaware that they have a criminal record until they are arrested because of an outstanding warrant, are denied employment, or fired from their current job after a criminal background check.[34] It can be difficult to resolve criminal identity theft because the victim often appears to be the criminal.[22]



The victim is often unaware that they have a criminal record until they are arrested because of an outstanding warrant...

How Stolen PII Is Used for **Criminal Identity Fraud** and the Potential Impact

- Use the victim's name during an arrest, potentially leading to a criminal record the victim isn't aware of
- Cause the victim to be denied employment or fired from a job after criminal activity appears during a background check

idwatchdog®

What Are Common Warning Signs of Identity Theft?

There were over 3.2 million reports of fraud in 2019 according to the FTC, and people filed more reports about identity theft, in all its various forms, than any other type of fraud.[7] Fortunately, some common warning signs of identity theft can help victims identify the issues and begin to resolve them,[35] including:

- Noticing unfamiliar credit card charges or bank withdrawals
- Not receiving expected bills or other mail
- Finding unknown accounts on a credit report
- Receiving unrecognized medical bills or having a medical claim rejected because of reaching the benefits limit for unfamiliar services
- Having a health plan rejected because of inaccurate medical records
- Having an e-filing rejected, or receiving an IRS notice about a suspicious tax return [36]
- Getting an unexpected IRS notice that an online account has been created, accessed, or disabled
- Discovering IRS records with wages or income from an unfamiliar employer
- Being notified of a data breach[35]
- Receiving calls from debt collectors

Warning signs that **a child may be a victim** of identity theft include:[30]

- Receiving credit card or loan offers in the child's name
- Receiving an IRS notice that the child owes unpaid taxes
- Getting collection calls for a debt in the child's name
- Receiving bills for products or services in the child's name that the parent or guardian didn't order
- Having government benefits declined under the child's Social Security number

How Does Identity Theft Happen?

Phishing
Scammers often use phishing emails to trick victims into providing personal or financial information.[37] Phishing emails can be deceiving in that they may appear to come from a known or trusted company, such as a bank or an online retailer, and use various tactics to get the victim to click a link or open an attachment.[37]

Smishing
Scammers may also target victims via text message—a crime called smishing.[38] Similar to phishing attacks, criminals may impersonate trusted organizations or even friends to trick victims into divulging information.[39] Smishing may be increasing as more people trust text messages over phone calls and emails.

Vishing
Fraudsters can also use phone calls, also known as voice phishing or vishing, to target potential victims.[40] Phone scammers sometimes use promises, like the offer of a prize, or threats, such as the risk of not getting a tax refund, to prompt victims into giving up personal information. Scammers will also use spoofing to send falsified information to a caller ID.[41] A spoofed call looks like it's coming from a local number or a trusted organization when it could be originating anywhere in the world.

Skimming
Skimming occurs when a criminal steals information as the debit or credit card is swiped.[22] Scammers may tamper with the electronic card reader so that it captures card data, place a recording device at an ATM, or recruit a crooked salesperson to steal customers' card data.

Fake Websites
Fake websites often look like legitimate and trustworthy sites to make people more apt to provide their personal information.[22] Some online shopping scams use a bogus website or mobile app that mimics a trusted retailer, including a familiar logo and similar URL.[42] Purchases made on these fraudulent sites will likely never arrive, or worse, scammers may seed the website with malware that infects the victim's device and harvests personal or financial information.

Impersonation Scams or Confidence Fraud
Confidence fraud occurs when a criminal deceives a victim into believing they have a trusted relationship—as a family member, friend, or romantic interest—to convince the victim to send money, provide information, make purchases, or even launder money.[43] One way thieves steal taxpayer information is through IRS impersonation scams. Scammers call their victims claiming to work for the IRS or send fraudulent emails that look like official communications.[44]

Data Breaches
A data breach is the intentional or unintentional release or theft of information, whether it is due to a cyberattack or simply the improper disposal of physical documents.[45] If an individual is notified of a breach, their financial or personal information may have been exposed. The theft of usernames and passwords from data breaches may also fuel credential stuffing attacks in which criminals use stolen username and password combinations to hack into other accounts.[46]

Public Wi-Fi and USB Charging Stations
Many public Wi-Fi networks are vulnerable to threats from hackers,[47] making it possible for thieves to eavesdrop on users' private information.[1] Scammers may also employ a USB charging scam, called juice jacking, in which malware infects the user's device when connected to an airport USB charging station or hotel USB port.[48]

Purchase of Information on the Dark Web
The dark web, or dark net, is a part of the internet that serves as a highly profitable marketplace where criminals can purchase stolen personal information.[49] Private photos, medical records, and financial information have all reportedly been stolen and shared on the dark web.[50] Security researches have reported a concerning trend that cybercriminals have begun targeting children—even infants—and advertising their stolen information for sale on the dark web.[28]

Theft by a Family Member or Friend
An identity could be stolen by a family member or friend, such as a parent who uses a child's information to get a credit card or loan, or someone who uses their spouse's information without permission to open an account.[51] According to one report, 51 percent of new account fraud victims stated that they personally knew the individual who committed the fraud.[52]

Theft of a Wallet, Mail, or Even Trash
Personal and financial information can also be stolen using low-tech methods, such as a criminal going through the victim's mail or even their trash.[22]

Steps to Better Protect Yourself and Your Loved Ones from Identity Theft

Secure Devices and Accounts

- **Create strong passwords** - Experts recommend creating strong passwords[36]—for example, a long memorable phrase such as a song lyric or quote that mixes characters and numbers.[53] It's best to create a different password for each account.[36] Individuals should change their password if they are notified of a data breach by a company they do business with.[12]
- **Use multi-factor authentication when available** - Some online accounts or apps offer multi-factor authentication, which is an extra layer of security that requires two or more credentials to log in[37]— often a unique code sent to the user via text message.[54] Multi-factor authentication can make it harder for scammers to hack the victim's accounts, even if they have the victim's username and password.[37]
- **Update software regularly** - It's best to regularly update software, as criminals try to exploit known vulnerabilities before they can be fixed.[55] The FTC advises updating antivirus or firewall programs, as well as the operating system, internet browsers, and apps.
- **Implement security software** - The IRS advises using security software, including virus/malware protection and a firewall, and ensuring that they are set to update automatically.[36] It's also recommended to use encryption programs to protect sensitive digital data.
- **Protect data by backing it up** - The FTC advises individuals to back up data stored on all devices using an external hard drive or cloud storage and to make sure those backups aren't connected to the home network.[37]

Shop and Surf Online More Safely

- **Verify the legitimacy of websites** - It is advised to look for the presence of "https" in the URL and the lock icon, which often indicate the web traffic is encrypted and that visitors can share data safely.[56] Consider also checking for misspellings or wrong domains within a link (for example, an address that should end in ".gov" but instead ends in ".com").
- **Use caution on public Wi-Fi networks** - The Department of Homeland Security advises individuals not to connect to unsecured public Wi-Fi networks, especially for banking or online shopping.[57] It's advised to connect to public Wi-Fi using a Virtual Private Network (VPN) or the user's own cell phone hotspot instead.[58]
- **Examine for skimming devices** - Skimmers may be placed on the regular credit card swipe, so if anything looks off, it's best to go elsewhere.[61] Things to look for at ATMs, gas stations, and checkout lines include obvious signs of tampering, a different color or material, and graphics that aren't aligned correctly.[62]
- **Stick with reputable online retailers** - Experts advise online shoppers to look for products and services first on trusted and known web retailers.[59] It's best to use apps provided directly by the retailer as well. The FTC recommends researching unfamiliar retailers by typing the name of the company or product into a search engine with terms like "review," "complaint," or "scam."[60] Experts advise confirming the retailer's physical address and working phone number in case there are problems with the transaction.[59]
- **Use a credit card over a debit card when possible** - The FTC advises paying with a credit card, as credit card transactions are protected by the Fair Credit Billing Act, which allows consumers to dispute charges under certain situations.[60] Additionally, because a debit card draws money directly from a bank account, unauthorized charges could leave the victim with insufficient funds.[57] It's advised to never pay by wire transfer, money order, or gift card, as sellers that request these types of payments are often scammers.[42]

Avoid Impersonations or Confidence Scams

- **Beware of unsolicited emails, texts, and calls** - Scammers may attempt to target victims through email, text, phone calls, or even social media messages, so it's wise to be suspicious of any unsolicited communication,[3] even if they appear to come from a trusted company.[1] It's advised instead to contact the company directly using their main customer service line.
- **Know who you are dealing with** - It's recommended to search online for the contact information (name, email, phone number, and address) of individuals or businesses who contact you, as others may have shared information about previous scam attempts.[63] In addition, a reverse image search can help determine if a profile picture has been used elsewhere on the internet and on which websites.[43]
- **Don't give money or information to someone you meet online** - The FBI advises that individuals should never send money to someone they meet online, especially via wire transfer.[43] The agency advises consumers to never share credit card numbers or bank account information with another person without verifying their identity.
- **Beware of money mule scams** - The FBI advises individuals not to send or receive money on behalf of people or businesses for which they are not responsible, and to be wary of online job postings and messages promising easy money for little to no effort.[64]
- **Resist the pressure to act quickly** - Scammers often try to create a sense of urgency to produce fear and lure victims into immediate action.[63] The FTC advises that individuals talk to someone they trust before providing money or personal information.[65]

Stay Vigilant During Tax Time and Year-Round

- **File taxes as early as possible** - Experts advise taxpayers to file as soon as they have collected all of the necessary documents, such as W-2s, 1099s, and mortgage interest statements.[14] Use a secure internet connection to file electronically, or mail the return directly from the post office.[13] Taxpayers should follow the advice of their retained financial or tax professional.[16]
- **Research tax preparers** - Research tax preparers thoroughly before giving them personal information.[13]
- **Know how the IRS contacts taxpayers** - The IRS typically initiates contact with taxpayers through regular mail delivered by the United States Postal Service.[66] According to the IRS, its agency will not: initiate contact with taxpayers by email, text, or social media to request personal or financial information; call taxpayers with threats of lawsuits or arrests; or call, email, or text to request taxpayers' Identity Protection PINs.[36]

Safeguard Information - Personal, Financial, Medical, and Insurance

- **Protect your information** - Experts advise caution when sharing personal or financial information, such as date of birth, Social Security number, or bank account number, as well as medical information, such as health insurance number and Medicare number. [12] It's recommended not to carry a Social Security card in a wallet or purse and to only provide a Social Security number when absolutely necessary.[12]

- **Initiate contact with medical or insurance professionals** - It's recommended not to share medical or insurance information by phone or email unless you initiated the contact and are sure you are speaking with the right organization.[67] Experts advise not to provide any personal information in response to calls or emails from someone who claims to be from an insurer or healthcare provider.[68] Instead, it's better to contact the doctor or insurer directly or log in to the patient portal to verify the request.

- **Safeguard your mail** - It's recommended to collect mail daily to reduce the potential for mail fraud.[1] For vacations, consider requesting a hold from the post office or asking a trusted person to collect mail. Consider reducing the number of documents with sensitive information that arrive by mail by requesting electronic statements. Outgoing mail containing personal data should be taken directly to the post office or a secure collection box.

- **Shred important documents** - Experts recommend shredding receipts, credit offers, account statements, expired credit cards,[12] outdated insurance forms, physician statements, prescription paperwork, and other documents containing personal information.[19]

Protect Children

- **Consider a child credit freeze** – Consider locking or freezing your child's credit, until he or she is old enough to use it.[29] A credit freeze or credit lock restricts access to a child's credit file, making it harder for identity thieves to open new accounts in the child's name.[69]

- **Check their credit** - Experts advise checking your child's credit report if you suspect fraud or identity theft.[30] If a child's credit report contains errors due to fraud or misuse, parents will have time to correct it before the child applies for a job, needs a loan for tuition or a car, or attempts to rent an apartment.

- **Be aware of events that may put a child's information at risk** - It's recommended to pay particular attention to certain circumstances, such as having an adult in your household who might be tempted to use a child's identity to start over[51] or being notified of a data breach at the child's school, doctor's office, or another location.[70]

- **Talk about what information can be shared—and what shouldn't** - Children often like to share personal details online, including pictures, videos, plans, and their location. Experts advise talking with children about what types of information should never be shared, such as their Social Security number, street address, phone number, and financial information.[71]

Keep Up General Maintenance

- ✓ **Pay attention to bills and transactions** - Review bank account and credit card statements regularly to look for unexplained withdrawals, charges, and accounts.[3] If bills don't arrive on time, follow up with creditors as it's possible that scammers changed the address associated with the account. It's also a good idea to set up automatic alerts on accounts to receive a notification when a transaction is made.

- ✓ **Review EOB statements and other medical correspondence** - Experts recommend carefully reviewing Explanation of Benefits (EOB) statements, bills, and other correspondence from insurers and medical providers.[19] Anything suspicious, such as an unfamiliar doctor's name or treatment date, should be reported immediately to the insurer.

- ✓ **Review credit reports annually** - Experts advise that individuals review their credit reports for suspicious activity once a year.[12] Credit reports can be ordered for free from Annualcreditreport.com. Individuals can also consider freezing their credit, which prevents someone from applying for and getting approval for a credit account or utility services in their name.

- ✓ **Request access to medical records** - Consider periodically reviewing medical records for red flags.[20] It's a patient's right under the Health Insurance Portability and Accountability Act to request copies of health information. Some healthcare providers may have an online patient portal to view records, or patients may be able to request the information from the office directly, sometimes for a small fee. At least once a year, it's recommended to ask your insurer for a full list of benefits paid in your name.[19]

- ✓ **Take appropriate action if you receive a breach notification** – The FTC provides a checklist for individuals whose information may have been exposed during a data breach.[72] If you receive a notification that your health insurance or health plan number was compromised, notify the insurer so they can note it in their records and flag the account number.[73]

How to Report an Incident

According to the FTC, if you or a loved one believe you have been the victim of identity theft, report it immediately at IdentityTheft.gov, the federal government's resource for identity theft victims. Below are additional steps to report other specific types of identity theft.

- For possible tax identity theft, the IRS recommends responding immediately to any IRS notice.[36] If an e-filed return was rejected because of a duplicate filing, or if the IRS instructs you to do so, complete IRS Form 14039, Identity Theft Affidavit (PDF).

- For possible medical identity theft, the US Department of Health and Human Services recommends contacting their fraud hotline and Medicare.gov's web page on reporting fraud.[74]

- For possible employment identity theft, report it to your employer and the state unemployment benefits agency.[75]

- For a possible confidence or romance scam, report it to the Internet Crime Complaint Center and local FBI field office.[43]

Sources Cited

[1] U.S. News & World Report, "Credit Card Fraud vs. Identity Theft: What's the Difference?" (https://creditcards.usnews.com/articles/credit-fraud-vs-identity-theft-whats-the-difference)

[2] Federal Trade Commission IdentityTheft.gov, "Warning Signs of Identity Theft" (https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft)

[3] Better Business Bureau, "BBB Tip: Identity Theft" (https://www.bbb.org/article/news-releases/16951-bbb-tip-identity-theft)

[4] TechRadar, "ID Fraud vs Identity Theft vs Credit Card Theft: What Is the Difference?" (https://www.techradar.com/news/id-fraud-vs-identity-theft-vs-credit-card-theft-what-is-the-difference)

[5] U.S. Department of Labor, "Guidance on the Protection of Personal Identifiable Information" (https://www.dol.gov/general/ppii)

[6] Javelin Strategy & Research, "2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis" (https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis)

[7] Federal Trade Commission, "Consumer Sentinel Network Data Book 2019" (https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf)

[8] Forbes, "Credit Card Fraud Is Down, But Account Fraud That Directly Hurts Consumers Remains High" (https://www.forbes.com/sites/tomgroenfeldt/2019/03/18/credit-card-fraud-is-down-but-account-fraud-which-directly-hurts-consumers-remains-high/#6130466f20bf)

[9] Green Sheet, "Credit cards surging in 2019—fraud too" (http://www.greensheet.com/emagazine.php?article_id=6186)

[10] Investopedia, "Card-Not-Present Fraud" (https://www.investopedia.com/terms/c/cardnotpresent-fraud.asp)

[11] IRS, "Identity Theft Remains on IRS' 'Dirty Dozen' List Despite Progress" (https://www.irs.gov/newsroom/identity-theft-remains-on-irs-dirty-dozen-list-despite-progress)

[12] USA.gov, "Identity Theft" (https://www.usa.gov/identity-theft)

[13] Federal Trade Commission, "Tax Identity Theft Awareness" (https://www.consumer.ftc.gov/features/tax-identity-theft-awareness)

[14] Consumer Reports, "4 Reasons to File Taxes Early and Electronically, Especially This Year" https://www.consumerreports.org/taxes/reasons-to-file-taxes-early/)

[15] Federal Trade Commission, "Tax-Related Identity Theft" (https://www.consumer.ftc.gov/articles/tax-related-identity-theft)

[16] Investopedia, "Reasons to File an Early Tax Return" (https://www.investopedia.com/taxes/file-early-tax-return/)

[17] World Privacy Forum, "Medical Identity Theft" (https://www.worldprivacyforum.org/category/med-id-theft/)

[18] U.S. Department of Health and Human Services, "Medical Identity Theft" (https://oig.hhs.gov/fraud/medical-id-theft/index.asp)

[19] AARP, "Medical Identity Theft" (https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html)

[20] CNBC, "Here's How to Avoid Medical Identity Theft" (https://www.cnbc.com/2019/06/07/how-to-avoid-medical-identity-theft.html)

[21] Fraud.org, "Medical Identity Theft" (https://www.fraud.org/medical_id_theft)

[22] National Association of Insurance Commissioners, "Identity Theft" (https://content.naic.org/cipr_topics/topic_identity_theft.htm)

[23] BenefitsPro, "U.S. Unemployment Systems Are Under Attack, Secret Service Says" (https://www.benefitspro.com/2020/05/21/u-s-unemployment-systems-are-under-attack-secret-service-says/)

[24] Michigan Department of Treasury, "Types of Identity Theft" (https://www.michigan.gov/treasury/0,4679,7-121-1755_73555-511247--,00.html)

[25] MarketWatch, "What To Do If Someone Else Is Fraudulently Claiming Your Unemployment Benefits" (https://www.marketwatch.com/story/what-to-do-if-someone-else-is-claiming-your-unemployment-benefits-2020-06-08)

[26] Federal Trade Commission, "Is a Scammer Getting Unemployment Benefits in Your Name?" (https://www.consumer.ftc.gov/blog/2020/06/scammer-getting-unemployment-benefits-your-name)

[27] CNBC, "How to Protect Your Child From Identity Theft" (https://www.cnbc.com/2019/07/12/how-to-protect-your-child-from-identity-theft.html)

[28] TheNextWeb, "The Worrying Trend of Children's Data Being Sold on the Dark Web" (https://thenextweb.com/podium/2019/02/23/children-data-sold-the-dark-web/)

[29] State of California Department of Justice, "How to 'Freeze' Your Child's Credit Files" (https://oag.ca.gov/idtheft/facts/freeze-child-credit)

[30] U.S. News & World Report, "How to Check Your Child's Credit Report" (https://creditcards.usnews.com/articles/how-to-check-your-childs-credit-report)

[31] Investopedia, "Synthetic Identity Theft" (https://www.investopedia.com/terms/s/synthetic-identity-theft.asp)

[32] Javelin Strategy & Research, "2018 Child Identity Fraud Study" (https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study)

[33] State of California Department of Justice, "Criminal Identity Theft" (https://oag.ca.gov/idtheft/criminal)

[34] Georgia Department of Law, "Identity Theft: Criminal Identity Theft" (http://www.consumer.ga.gov/consumer-topics/identity-theft-criminal-identity-theft)

[35] Federal Trade Commission, "Warning Signs of Identity Theft" (https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft)

[36] IRS, "Taxpayer Guide to Identity Theft" (https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft)

[37] Federal Trade Commission, "How to Recognize and Avoid Phishing Scams" (https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams)

[38] FBI, "2019 Internet Crime Report Released" (https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120)

idwatchdog®

[39] Consumer Reports, "Smishing: A Silly Word for a Serious Fraud Risk" (https://www.consumerreports.org/scams-fraud/smishing-silly-word-serious-fraud/)

[40] CSO, "Vishing Explained: How Voice Phishing Attacks Scam Victims" (https://www.csoonline.com/article/3543771/vishing-explained-how-voice-phishing-attacks-scam-victims.html)

[41] Federal Trade Commission, "Phone Scams" (https://www.consumer.ftc.gov/articles/0208-phone-scams)

[42] AARP, "Online Shopping Scams" (https://www.aarp.org/money/scams-fraud/info-2019/online-shopping.html)

[43] FBI, "Cyber Actors Use Online Dating Sites to Conduct Confidence/Romance Fraud and Recruit Money Mules" (https://www.ic3.gov/media/2019/190805.aspx)

[44] IRS, "Tax Scams/Consumer Alerts" (https://www.irs.gov/newsroom/tax-scams-consumer-alerts)

[45] IRS, "Data Breach: Tax-Related Information for Taxpayers" (https://www.irs.gov/identity-theft-fraud-scams/data-breach-information-for-taxpayers)

[46] Identity Theft Resource Center, "2019 End-Of-Year Data Breach Report" (https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf)

[47] Reader's Digest, "How Bad Is It to Use Public WiFi?" (https://www.rd.com/article/dangers-of-public-wifi/)

[48] The New York Times, "Stop! Don't Charge Your Phone This Way" (https://www.nytimes.com/2019/11/18/technology/personaltech/usb-warning-juice-jacking.html)

[49] Forbes, "The Market That Will Sell You a $20,000 Bank Loan for $30" (https://www.forbes.com/sites/daveywinder/2019/10/15/the-market-that-will-sell-you-a-20000-bank-loan-for-30/#2ed575745743)

[50] Investopedia, "Dark Web" (https://www.investopedia.com/terms/d/dark-web.asp)

[51] The Balance, "Dealing with Identity Theft by a Friend or Relative" (https://www.thebalance.com/dealing-with-identity-theft-by-a-friend-or-relative-2386237)

[52] Forbes, "Credit Card Fraud Is Down, But Account Fraud That Directly Hurts Consumers Remains High" (https://www.forbes.com/sites/tomgroenfeldt/2019/03/18/credit-card-fraud-is-down-but-account-fraud-which-directly-hurts-consumers-remains-high/#8482d9020bfc)

[53] Google Account Help, "Create a Strong Password & A More Secure Account" (https://support.google.com/accounts/answer/32040?hl=en)

[54] PCMag, "Two-Factor Authentication: Who Has It and How to Set It Up" (https://www.pcmag.com/how-to/two-factor-authentication-who-has-it-and-how-to-set-it-up)

[55] Federal Trade Commission, "Update Your Software Now" (https://www.consumer.ftc.gov/blog/2019/06/update-your-software-now)

[56] FBI, "Cyber Actors Exploit 'Secure' Websites in Phishing Campaigns" (https://www.ic3.gov/media/2019/190610.aspx)

[57] U.S. Department of Homeland Security, "Holiday Online Shopping" (https://www.cisa.gov/sites/default/files/publications/19_1125_cisa_Holiday-Online-Shopping-Tip-Sheet.pdf)

[58] National Cybersecurity Alliance, "Online Shopping" (https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/)

[59] PCMag, "14 Tips for Safe Online Shopping" (https://www.pcmag.com/how-to/14-tips-for-safe-online-shopping)

[60] Federal Trade Commission, "FTC: Fashion Nova Failed to Deliver the Goods" (https://www.consumer.ftc.gov/blog/2020/04/ftc-fashion-nova-failed-deliver-goods?utm_source=govdelivery)

[61] The Balance, "How to Prevent Credit Card Fraud" (https://www.thebalance.com/ways-avoid-credit-card-fraud-960797)

[62] PCMag, "How to Spot and Avoid Credit Card Skimmers" (https://www.pcmag.com/how-to/how-to-spot-and-avoid-credit-card-skimmers)

[63] FBI, "Perpetrators Use Various Methods to Deceive and Defraud Elderly Victims for Financial Gain" (https://www.ic3.gov/media/2019/190919.aspx)

[64] FBI, "COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic" (https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic)

[65] Federal Trade Commission, "10 Things You Can Do to Avoid Fraud" (https://www.consumer.ftc.gov/articles/0060-10-things-you-can-do-avoid-fraud)

[66] IRS, "IRS Continues Warning on Impersonation Scams; Reminds People to Remain Alert to Other Scams, Schemes This Summer" (https://www.irs.gov/newsroom/irs-continues-warning-on-impersonation-scams-reminds-people-to-remain-alert-to-other-scams-schemes-this-summer)

[67] Federal Trade Commission, "Medical Identity Theft" (https://www.consumer.ftc.gov/articles/0171-medical-identity-theft)

[68] The Washington Post, "Hackers Want Your Medical Records. Here's How to Keep Your Info From Them." (https://www.washingtonpost.com/national/health-science/hackers-want-your-medical-records-heres-how-to-keep-your-info-from-them/2018/12/14/4a9c9ab4-fc9c-11e8-ad40-cdfd0e0dd65a_story.html)

[69] Federal Trade Commission, "Credit Freeze FAQs" (https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs)

[70] State of California Department of Justice, "Child Security Breach First Steps" (https://oag.ca.gov/idtheft/child-security-breach)

[71] Federal Trade Commission, "Net Cetera: Chatting with Kids About Being Online" (https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/netcetera_2018.pdf)

[72] Federal Trade Commission, "When Information is Lost or Exposed" (https://identitytheft.gov/databreach)

[73] State of California Department of Justice, "First Aid for Medical Identity Theft: Tips for Consumers" (https://oag.ca.gov/privacy/facts/medical-privacy/med-id-theft)

[74] U.S. Department of Health and Human Services, "Medical Identity Theft & Medicare Fraud" (https://oig.hhs.gov/fraud/medical-id-theft/OIG_Medical_Identity_Theft_Brochure.pdf)

[75] Federal Trade Commission, "Is a Scammer Getting Unemployment Benefits in Your Name?" (https://www.consumer.ftc.gov/blog/2020/06/scammer-getting-unemployment-benefits-your-name)