What To Do If Your Identity Is Stolen

With data breaches seemingly happening every week, more and more people are victims of identity theft.

Identity theft is a serious crime that wreaks havoc on your finances and credit.

A cybercriminal who steals your personal information might use it to open new accounts, make unauthorized purchases, and even file taxes in your name in hopes of stealing a refund!

As frustrating as identity theft is, you can take steps to protect yourself and minimize the damage if your identity is stolen. If you react fast, you significantly improve your chances of recovering from the crime.

How hackers get access to your data

Your data can be stolen in several ways. Many cases of identity theft today occur after:

- Your data was lost in an organization's data breach.
- A cybercriminal tricked you into entering data, clicking a bad link, or downloading a malicious attachment in a phishing attack.
- Your phone, wallet, purse, laptop or sensitive documents were stolen.

Signs of identity theft

Identity theft can happen to anyone, so it's essential to know the red flags that your identity is in the wrong hands. Some common indicators that your identity may have been stolen include:

- You receive bills or debt collection calls for accounts you don't recognize.
- You are denied credit for no apparent reason.
- You find errors on your credit report, such as accounts you didn't open or incorrect personal information.
- Important mail, such as credit card statements or bank account information, goes missing.

If you experience any of these signs, don't panic. Act immediately to protect yourself and minimize the damage.

What to do if you suspect identity theft

If your identity is stolen, you must act to mitigate the damage, report the crime, and recover your identity.

1. **Contain the damage**

If you think your identity was stolen, you should act quickly to prevent further damage to your finances and credit.

- **Place a fraud alert:** A fraud alert warns creditors to be cautious when extending credit in your name. It's a decent first step if you suspect identity theft, but it doesn't prevent new accounts from being opened (which is why you should freeze your credit). A fraud alert lasts for one year, and you can place it by contacting one of the three major credit bureaus. A hacked organization will likely offer free fraud alerts if your data is stolen due to a data breach.
- **Contact your financial institutions:** Inform your bank, credit card companies, and any other financial institutions you do business with about your identity theft. Even if there is no suspicious activity with your account, you should alert any financial institution you use to your situation. They can monitor your accounts for unauthorized activity and take steps to prevent further unauthorized transactions.
- **Freeze your credit:** A credit freeze restricts access to your credit report, making it nearly impossible for thieves to open new accounts in your name. In fact, you cannot even open a new account when your credit is frozen. Contact all three major credit reporting bureaus (Equifax, Experian, TransUnion) to initiate a freeze. We recommend keeping your credit frozen by default.

2. **Report the theft**

You will want to report being a victim of identity theft to federal and local law enforcement.

- **File a police report:** While a police report may not lead to the thief's arrest, it is an essential step in the recovery process. The report can be used to extend a fraud alert on your credit report for seven years and may be required by creditors to dispute fraudulent charges. If your local police department won't make a report, ask about filing a "miscellaneous incident" report, or go to state or federal authorities.
- **Report to the FTC:** The FTC is the federal agency that tracks identity theft. You can file a report online or by calling 1-877-438-4338. The agency will have you fill out an FTC Identity Theft Affidavit. Filing a report with the FTC helps them track the scope of identity theft and provides you with a recovery plan.

You can also report identity theft to the Identity Theft Resource Center.

3. **Recover your identity**

Once you've frozen your credit and alerted the authorities, work to recover your identity. This process will be different for every victim, but there are some general steps to follow.

- **Dispute fraudulent charges:** Contact creditors with documented evidence of fraudulent activity on your accounts. You can use the FTC's sample letter or its Identity Theft Affidavit to dispute the charges.
- **Monitor your credit report:** Every year, you are entitled to a free credit report from each of the three major credit bureaus. Review your reports carefully and dispute any errors you find. You can request your free reports at AnnualCreditReport.com). If your information was lost in a data breach, refer to the notification letter you received about how to get credit monitoring.
- **Reach out to your credit card companies and banks:** If your identity was stolen to open up a debit card, checking account, or credit card, alert the bank or credit card company to your situation. Send them your affidavit or police report if they request additional information. If you don't report that your identity was stolen quickly, you might be on the hook for some or all fraudulent charges, especially if unauthorized debit card transactions were made.

More actions to take

- **Change passwords**: Change your passwords on the accounts you suspect have fraudulent activity, or accounts where your data was affected in a data breach. If you were using those passwords, or a similar version of them, on other accounts, change those, too. Each password should be unique to the account, at least 16 characters long, and a mix of characters. Use a password manager to generate and store all your passwords.

- **Enable multi-factor authentication (MFA):** Turn on MFA for every account that permits it.
- **Think about social media:** Check the settings for every social media platform you use and consider limiting your audience or making your profiles private.
- **Use credit cards over debit cards:** Use credit cards instead of debit cards, especially when shopping online. It is much easier to dispute credit card charges than debit card charges.
- **Sign up for USPS Informed Delivery:** You can sign up for USPS Informed Delivery for free. This service emails you pictures of your expected mail each day. By tracking it, you can check if anyone is stealing your mail.
- **Consider a new Social Security number:** In extreme cases, it is possible to get a new Social Security number, but there are administrative hurdles. You typically must be a victim of identity theft more than once.

Preventing identity theft

Beyond cybersecurity basics like having strong passwords and enabling MFA, you can help prevent identity theft by keeping your credit frozen by default, not accessing sensitive accounts while using public wi-fi, and protecting your Social Security number as much as possible.

You can even freeze your children's credit, too. Cybercriminals can try to create a different name and identity using a child's Social Security number – sometimes it doesn't matter that the number doesn't belong to an adult. This fraud can happen for years, and it might be undetected until the victim turns 18! The FTC has more details.
