Identity Theft

How to protect yourself against identity theft and respond if it happens.

Equifax Data Breach

Equifax, one of the three major credit reporting agencies in the U.S., announced a data breach that affects 143 million consumers. The hackers accessed Social Security numbers, birthdates, addresses, and driver's license numbers.

Equifax has launched a tool that will let you know if you were affected by the breach. Visit Equifax's website dedicated to this breach to learn if you were impacted. You will need to provide your last name and the last six numbers of your Social Security number.

If you are impacted, Equifax offers you a free credit monitoring service, TrustedIDPremier. However, you won't be able to enroll in it immediately. You will be given a date when you can return to the site to enroll. Equifax will not send you a reminder to enroll. Mark that date on your calendar, so you can start monitoring your credit as soon as possible.

If you detect suspicious activity on your credit report due to the breach, learn how to report it immediately.

The FTC also offers more information to protect yourself after a data breach. Learn how to report and recover from identity theft at IdentityTheft.gov.

Identity Theft

Identity (ID) theft is a crime where a thief steals your personal information, such as your full name or Social Security number, to commit fraud. The identity thief can use your information to fraudulently apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name. You may not know that you are the victim of ID theft until you experience a financial consequence (mystery bills, credit collections, denied loans) down the road from actions that the thief has taken with your stolen identity.

There are several common types of identity theft that can affect you:

- Child ID theft - Children's IDs are vulnerable because the theft may go undetected for many years. By the time they are adults, the damage has already been done to their identities.
- Tax ID theft - A thief uses your Social Security number to falsely file tax returns with the Internal Revenue Service or state government.
- Medical ID theft - This form of ID theft happens when someone steals your personal information, such as your Medicare ID or health insurance member number to get medical services, or to issue fraudulent billing to your health insurance provider.
- Senior ID theft - ID theft schemes that target seniors. Seniors are vulnerable to ID theft because they are in more frequent contact with medical professionals who get their medical insurance information, or caregivers and staff at long-term care facilities that have access to personal information or financial documents.
- Social ID theft - A thief uses your name, photos, and other personal information to create a phony account on a social media platform.

Prevent Identity Theft

Take steps to protect yourself from identity theft:

- Secure your Social Security number (SSN). Don't carry your Social Security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary.
- Don't respond to unsolicited requests for personal information (your name, birthdate, Social Security number, or bank account number) by phone, mail, or online.
- Contact the three credit reporting agencies to request a freeze of your credit reports.
- Collect mail promptly. Place a hold on your mail when you are away from home for several days.
- Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
- Enable the security features on mobile devices, especially if you have contacts, banking websites and applications saved.
- Update sharing and firewall settings when you're on a public wi-fi network. Consider using a virtual private network, which can give you the privacy of secured private network.
- Review your credit card and bank account statements. Promptly compare receipts with account statements. Watch for unauthorized transactions.
- Shred receipts, credit offers, account statements, and expired credit cards, to prevent "dumpster divers" from getting your personal information.
- Store personal information in a safe place.
- Install firewalls and virus-detection software on your home computer.
- Create complex passwords that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases
- Review your credit report once a year to be certain that it doesn't include accounts that you have not opened. You can order it for free from Annualcreditreport.com.
- Freeze your credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange, for free. This prevents someone from using your personal information to open a credit account or get utility services.

Report Identity Theft

Report identity (ID) theft to the Federal Trade Commission (FTC) online at IdentityTheft.gov or by phone at 1-877-438-4338.

If you report identity theft online, you will receive an identity theft report and a recovery plan. Create an account on the website in order to update your recovery plan, track your progress, and receive prefilled form letters to send to creditors. If you decide not to create an account, you need to print or save your identity theft report and recovery plan. Without an account, you won't be able to access them on the website in the future. Download the FTC's publication, Taking Charge - What to do if Your Identity is Stolen (PDF, Download Adobe Reader) for detailed tips, checklists, and sample letters.

You can also report identity theft to the FTC by phone at 1-877-438-4338. The FTC will collect the details of your situation, but won't provide you with an ID theft report or recovery plan. You may also choose to report your identity theft to your local police station. It could be necessary if:

- You know the identity thief
- The thief used your name in any interaction with the police
- A creditor or another company affected by the identity theft requires you to provide a police report.

Report Specific Types of Identity Theft

You may also report specific types of identity theft to other federal agencies.

- Medical Identity Theft - Contact your health insurance company's fraud department or Medicare's fraud office.
- Tax Identity Theft - Report this type of ID theft to the Internal Revenue Service and your state's Department of Taxation or Revenue.

Report Identity Theft to Other Organizations

In addition to federal government agencies, you should also report the theft to other organizations, such as:

- Credit Reporting Agencies - Contact one of the three major credit reporting agencies to place fraud alerts or freezes on your accounts so that no one can apply for credit with your name or social security number. Also get copies of your credit reports, to be sure that no one has already tried to get unauthorized credit accounts with your personal information. Confirm that the credit reporting agency will alert the other two credit reporting agencies.
- National Long-Term Care Ombudsman Resource Center - Report cases of identity theft that resulted from a stay in a nursing home or long-term care facility.
- Financial Institutions - Contact the fraud department at your bank, credit card issuers and any other places where you have accounts.
- Retailers and Other Companies - Report the crime to companies where the identity thief opened credit accounts or even applied for jobs.
- State Consumer Protection Offices or Attorney General - Your state may offer resources to help you contact creditors, dispute errors and other helpful resources.

You may need to get new personal records or identification cards if your identity was stolen. Learn how to replace your vital identification documents after identity theft.

Tax ID Theft

Tax-related identity theft occurs when someone uses your Social Security number to get a tax refund or a job. You may not be aware of the problem until you E-file your tax return and find out that another return has already been filed using your Social Security number. If the IRS suspects tax ID theft, they will send a 5071C letter to the address on the federal tax return. Keep in mind, the IRS will never start contact with you by sending an email, text, or social media message that asks for personal or financial information. Watch out for IRS imposter scams, when someone contacts you saying they work for the IRS.

Report Tax ID Theft

If you suspect you have become a victim of tax ID theft—or the IRS sends you a letter or notice indicating a problem—take these steps:

- File a report with the Federal Trade Commission (FTC) at IdentityTheft.gov. You can also call the FTC Identity Theft Hotline at 1-877-438-4338 or TTY 1-866-653-4261.
- Contact one of the three major credit bureaus to place a fraud alert on your credit records:
    - Equifax: 1-888-766-0008
    - Experian: 1-888-397-3742
    - TransUnion: 1-800-680-7289
- Contact your financial institutions, and close any accounts opened without your permission or that show unusual activity.
- Respond immediately to any IRS notice; call the number provided. If instructed, go to the IRS Identity Verification Service.
- Complete IRS Form 14039, Identity Theft Affidavit (PDF, Download Adobe Reader); print, then mail or fax according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- Check with your state tax agency to see what steps to take at the state level.

How to Protect Yourself

Follow these steps to prevent tax identity theft:

Do

File your income taxes early in the season, before a thief can file taxes in your name. Also, Keep an eye out for any IRS letter or notice that states:

- More than one tax return was filed using your Social Security number.
- You owe additional tax, you have had a tax refund offset, or you have had collection actions taken against you for a year you did not file a tax return.
- IRS records indicate you received wages from an employer unknown to you.

Don't

- Don't reply to or click on any links in suspicious email, texts, and social media messages. Make sure to report anything suspicious to the IRS.

Medical ID Theft

Medical identity theft can occur when someone steals your personal identification number to obtain medical care, buy medication, access your medical records, or submit fake claims to your insurer or Medicare in your name.

Report Medical Identity Theft

If you believe you have been a victim of medical identity theft, call the Federal Trade Commission at 1-877-438-4338 (TTY: 1-866-653-4261) and your health insurance company's fraud department. You can report the theft through IdentityTheft.gov to share with the FTC and with law enforcement. Also get copies of your medical records and work with your doctor's office and insurance company to correct them.

If you suspect that you have been the victim of Medicare fraud, contact the U.S. Department of Health and Human Services' Inspector General at 1-800-447-8477.

Prevent Medical Identity Theft

Take these steps to prevent medical identity theft:

- Guard your Social Security, Medicare, and health insurance identification numbers. Only give your number to your physician or other approved health care providers.
- Review your explanation of benefits or Medicare Summary Notice to make sure that the claims match the services you received. Report questionable charges to your health insurance provider or Medicare.
- Request and carefully review a copy of your medical records for inaccuracies and conditions that you don't have.

Source: https://www.usa.gov/identity-theft