What to do if your identity is stolen

Identity Theft

If your identity has been stolen, the following steps should be taken as soon as possible to mitigate fraud committed in your name.

1. **Contact the companies and banks where you know identity fraud occurred.**

   Call the fraud department at the companies and financial institutions where you know the identity thief used your personal information. Part of this step may include closing or freezing your accounts that have been compromised.

2. **Contact the credit reporting agencies (CRAs) and place fraud alerts.**

   You will need to contact at least one of the three major CRAs: Equifax, Experian or TransUnion. The agency you contact is required to contact the other two and share information, but you may want to reach out to each CRA individually to be sure they are on alert as soon as possible that you've been a victim of identity theft. The CRAs collect information about you and how you use credit, as well as whether any business has turned your debt over to a collections agency or you've filed for bankruptcy.

   You'll want to request a fraud alert, which will last one year. This will make it more challenging for someone to open new accounts using your identifying information. Once a fraud alert has been placed, a business must verify your ID before issuing credit to the person requesting it. You can apply for a fraud alert by phone, online, and mail.

   If you've become a victim of identity theft, you also can request an extended fraud alert that lasts for seven years.

Equifax Alerts
800-525-6285
Equifax Consumer
Fraud Division
P.O. Box 105069
Atlanta, GA 30374

Experian Fraud Center
888-397-3742
Experian
P.O. Box 9554
Allen, TX 75013

TransUnion Fraud Alert
888-909-8872
TransUnion Fraud Victim
Assistance Department
P.O. Box 2000
Chester, PA 19016

3. **Ask for copies of your credit reports**.

   After placing the initial fraud alert, you can request a free copy of your credit report from each credit reporting agency. It's important to look at all three reports to help ensure you're not missing anything important — because each agency's report may be different. Review the reports carefully for transactions you don't recognize and follow the steps below to remedy them.

   An extended fraud alert allows you to receive two free credit reports from each of the credit bureaus within 12 months after you placed the alert.

Patriot Bank℠

What to do if your identity is stolen

4. Place a security freeze on your credit report.

If you know your identifying information has been stolen, you may want to place a security freeze on your credit report, which will prohibit a credit bureau from releasing any information in your credit report without your express approval. Because a security freeze prevents prospective creditors from accessing your credit file, this could provide an extra layer of protection by preventing a CRA from approving new credit, loans, or other services in your name without your authorization.

5. Obtain documents related to fraudulent transactions or accounts opened using your personal information.

You have the right to ask creditors or other businesses for copies of any applications or other records related to transactions or accounts connected to the use of your personal information for identity theft. You must ask for this in writing and may need to provide proof of your identity, a police report, and a Federal Trade Commission (FTC) Identity Theft Report (www.identitytheft.gov).

6. Obtain information from debt collectors.

You have the right to ask debt collectors for any information about debt incurred due to the identity theft.

7. Block the reporting of damaging information in credit reports.

You also have the right to ask CRAs to block any information in your file that is the result of identity theft. For example, an identity thief may make purchases in your name and never pay for them. If you don't ask the credit bureaus to block this information, it will remain in your credit report.

8. Prevent businesses from reporting information resulting from identity theft.

When you reach out to companies where you know an identity thief used your identifying information, ask that they stop reporting the inaccurate information to the credit bureaus, as well as report the revised, correct information. You'll need to identify what information you don't want reported and provide a copy of your FTC Identity Theft Report.

9. Report ID theft to the Federal Trade Commission.

While you don't need to report a stolen credit card to the FTC, you should report identity theft to the FTC right away. That way the FTC can create a report that you can use to prove the ID theft to businesses and financial institutions. To do this, you can fill out a report online at identitytheft.gov or call 877-438-4338.

Patriot Bank℠

10. Reach out to local law enforcement.

The FTC says you may also want to alert your local police department. When you go to your local law enforcement office, bring a copy of your FTC Identity Theft Report, a government-issued photo ID, proof of your current address, and any proof that your identity has been used for identity theft — such as collections notices. Don't forget to ask for a copy of the police report in case you need it.

You also can file an online complaint with the FBI's Internet Crime Complaint Center (www.ic3.gov), which gives victims of cybercrime a reporting mechanism that alerts authorities.

11. Contact the IRS.

Contact the IRS to make sure you aren't the victim of tax-related identity theft. Someone with a combination of your name, date of birth, and Social Security number could file a tax return in your name, hoping to receive a fraudulent refund. And make sure you respond to any notices from the IRS that may alert you to fraudulent activity.

12. Alert your health insurance company and medical care providers.

While identity theft is more often associated with financial fraud, it also can infiltrate your medical care. Contact your medical care providers to make sure the identity thief hasn't used your insurance information to receive healthcare services in your name. An identity thief who has your personal information could assume your identity when seeing a doctor, receiving prescription drugs, having surgery, or visiting an emergency room.

13. Reach out to the DMV.

An identity thief could use your driver's license or state ID number to impersonate you. They can use your driver's license number on a check, during a traffic stop, or to make a fake license. If you lose your driver's license or state ID, ask your state's DMV or licensing agency to place a flag on your license number to help put law enforcement on notice.

14. Clean up all your accounts.

You'll also need to clean up things on a more basic level. Contact your phone and utility companies, and any other places where you have accounts. Make sure you've cancelled all fraudulent accounts and, if you need them, open new accounts — with new account numbers. Remember to create strong, complex passwords for each account.

Patriot Bank℠

Additional steps for identity theft recovery

After you've taken the steps outlined above, you're on your way to responding to identity theft, but it doesn't stop there. You'll need a recovery plan to help resolve other negative effects and protect yourself going forward.

If an identity thief has sensitive personal information like your Social Security number, there are different types of ID theft they may commit. Depending on the type, you may need to take other steps such as contacting the Social Security Administration to report unauthorized use of your Social Security number, sorting through debt collector requests, or clearing your name of criminal charges.

As mentioned above, visiting the FTC's identity theft website can provide more help in creating a comprehensive identity theft recovery plan.

Resources for more information:

Equifax Alerts: www.equifax.com/personal/education/identity-theft/fraud-alert-security-freeze-credit-lock

Experian Fraud Center: www.experian.com/fraud/center.html#content-01

TransUnion Fraud Alert: www.transunion.com/fraud-victim-resource/place-fraud-alert

FTC Identity Theft Report: www.identitytheft.gov

FBI's Internet Crime Complaint Center: www.ic3.gov

5 Kinds of ID Theft Using a Social Security Number: www.lifelock.com/learn-identity-theft-resources-kinds-of-id-theft-using-social-security-number.html

Social Security Administration – Identity Theft Brochure: www.ssa.gov/pubs/EN-05-10064.pdf

Patriot Bank℠