COMPLETE ID™
a part of Experian.

# Your Identity Theft Action Plan

According to the **Center for Victim Research**, 7 to 10% of the U.S. population are victims of identity fraud each year, and 21% of those experience multiple incidents. So whether you are a victim or not, it's best to have a plan. Below are the steps to take if your identity has been compromised.

- ✓ **Sign up with an identity protection provider**
- ✓ **File a claim with your identity theft insurance provider (if you have one)**
- ✓ **Check your credit report**
- ✓ **Lock or freeze your credit**
- ✓ **Scan your financial accounts for unauthorized charges**
- ✓ **Change the passwords on financial accounts**
- ✓ **Notify your Human Resources department**
- ✓ **Notify any companies involved**
- ✓ **Notify government agencies**
- ✓ **Contact local police**
- ✓ **Place a fraud alert on your credit reports**

---

1. **Sign up for identity protection:** With the rise in cybersecurity threats, millions of Americans have turned to identity protection providers, such as **Complete ID**. They offer comprehensive services, including monitoring criminal court records, the dark web, financial account alerts, and many other dangerous places your name and information might show up. If they do, Complete ID will notify you so you can take swift action to help protect yourself. Complete ID offers important customer care at 1-855-591-0202.

2. **File a claim with your identity theft insurance provider:** If you do have identity protection, it might include identity theft insurance. This can help ease some of your stress by helping to cover certain expenses associated with restoring your identity. Even if you haven't purchased coverage, it might be available through your employer.

3. **Check your credit report:** Now that you know you've been a victim of identity theft, it's time to check for any accounts you don't recognize on your credit report. You are entitled to request a free credit report from each of the three bureaus (Experian®, TransUnion® and Equifax®). Get in the habit of requesting them as often as you can to stay informed.

4. **Lock or freeze your credit:** When receiving a new application, creditors will pull the applicant's credit file to see if they are a reliable borrower. As a victim of identity theft, you can help prevent a cybercriminal from opening an account in your name by putting a lock or freeze on your credit file. Contact each bureau separately: Experian (1-888-397-3742), TransUnion (1-888-909-8872) and Equifax (1-800-349-9960).

5. **Scan your financial accounts for unauthorized charges:** Log into your bank and credit card accounts, and scrutinize every charge for things you don't recognize or remember. If you find unknown charges, call your bank or credit card company to let them know and ask to have the account locked or closed.

6. **Change the passwords on your financial accounts:** If your identity has been stolen, there's a chance that some of your account login information has been compromised – or soon will be. Changing your passwords, particularly with financial accounts, is a solid idea. Good password pointers include using upper and lowercase letters, numbers, symbols, and 10 or more characters. Password manager software can help.

7. **Notify your Human Resources department:** There are two reasons to do this. First, you may automatically be eligible for identity theft resolution services through your employee benefit plan. Second, you may need to take time off to resolve the identity theft.

8. **Notify any companies involved:** If you've received a bill from a company you don't do business with, call the number on the bill and let them know you did not authorize the transaction. If the transaction went through your credit card company, have them reissue your card and let them know which charges were fraudulent.

9. **Notify government agencies:** If your Social Security number was used to commit fraud, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490 and file a **form 14039** Identity Theft Affidavit. You'll also want to **file a report** with the Federal Trade Commission. Your report could be used by other law enforcement agencies to catch thieves and fraudsters.

10. **Contact local police:** Oftentimes the criminals are in a different country. The police report helps you establish a paper trail that can prove that fraudulent accounts and charges, or even crimes, should not be attributed to you.

11. **Place a fraud alert on your credit reports:** Contact all three major credit bureaus (Experian, TransUnion and Equifax), to place a fraud alert on your credit report. This will remain in your credit file for a year. Anyone who checks your credit (a credit card company, for example) will then know that your identity has been compromised. They might use that information to take a closer look at the applicant to ensure it's you.

*This article is provided for general guidance and information. It is not intended as, nor should it be construed to be, legal, financial or other professional advice. Please consult with your attorney or financial advisor to discuss any legal issues or financial issues involved with credit decisions.*

*Complete ID service provided by Experian®.*

---