Rebuilding Your Identity

Just found out your identity was stolen? Stay calm. Act quickly. Start here.

While it can take a while before everything gets back to normal, taking smart, deliberate actions can help you get your identity back. **Here's how, step-by-step.**

Huntington Welcome.®

Step 1:

Let anyone with your financial information on file know you suspect fraud.

You may need to change your credit cards and bank accounts.

If Someone Used Your Account

What to do:

- Determine which charges are fraudulent and then call your bank or credit card company's fraud department to report unauthorized charges and request confirmation in writing. If it's a credit or debit card account, ask for a new card with new numbers.
- Change all passwords, PINs and logins associated with the account(s).

Why:

- It can help prevent thieves making further charges or accessing other personal information.

Tips:

- Keep a written record of whom you contacted and when. Also, keep any confirmation letters from banks or businesses since you may need them to dispute credit report discrepancies.
- Make sure you understand if your bank, credit card company, or payee holds you responsible for any unauthorized charges.
- Don't forget to notify utilities, insurance and other auto-pay companies attached to the compromised account(s).
- Be prepared to complete a dispute form at your bank or credit card company's request, as well as send them copies of federal or law enforcement reports (Step 3 & 4).

If Someone Opened an Account(s) in Your Name

What to do:

- Call your bank's fraud department. Tell them your identity was stolen and ask to close or freeze the account(s). Ask for written confirmation that states:
  - That you reported you did not open the account and you did not authorize anyone else to open the account on your behalf.
  - That you reported you did not authorize any transactions on the account.
- Once the bank or credit card company has completed their review of the case and determined that you are not liable, you should receive written confirmation that you are not financially responsible for any charges incurred on the account.

Why:

- This can prevent someone from adding new charges or doing anything else on the account(s) without your permission.

Tips:

- Keep a written record of whom you contacted and when. Also, keep any confirmation letters from banks or businesses since you may need them to dispute credit report discrepancies.
- Be prepared to complete a dispute form at your bank or credit card company's request, as well as send them copies of federal or law enforcement reports (Step 3 & 4).

Step 2:

Report ID theft to credit reporting agencies.

Add a fraud alert or credit freeze to all of your credit reports.

Who to Contact

Equifax

(888) 766-0008
Equifax.com/CreditReportAssistance

Experian

(888) 397-3742
Experian.com/Fraud
Experian.com/Freeze

TransUnion

(800) 680-7289
TransUnion.com/Solution/Fraud-Detection
TransUnion.com/SecurityFreeze

What to Say

- Tell them your identity has been stolen.
- Add a short-term fraud alert if you're planning on applying for a new mortgage, car loan, student loan or other type of credit in the near future.
- Add a stronger, longer-term credit freeze if you won't be applying for new credit soon.
- Ask for a FREE copy of your credit report and review it carefully. (You'll need it for Step 5.)
- Most credit bureaus will give you a free copy when you place or renew a fraud alert.
- If you add an alert, you may be opted out of receiving pre-approved credit card and insurance offers.
- When you receive a report, make note of the unique number assigned to you since you may need it later when communicating with the credit bureau.

The Difference Between a Fraud Alert & Credit Freeze

Fraud Alert

Definition: A fraud alert is a notice placed on your credit report warning prospective lenders that you are a victim of identity theft and that they should take reasonable extra steps to verify your identity before granting credit to the person claiming to be you.

Typically, placing or renewing a fraud alert will allow you to request a free credit report from each bureau to help you monitor your credit.

For a fraud alert, consumers only need to **contact one of the three major credit reporting agencies by phone or through their website.** The law requires that the credit reporting agency notify the other two when a consumer requests a fraud alert.

Cost: A fraud alert is available at no charge.

How long it lasts: An initial fraud alert will be active for 90 days, but it could be renewed for another 90 days after the first alert expires. You also have the option to apply for an extended fraud alert that will last for seven years.

Credit Freeze

Definition: A credit freeze means that no one (including you) can access your credit file until you unfreeze it, using a PIN or passphrase. If a prospective lender can't access your credit report, they won't issue new credit, which makes it harder for identity thieves to open new accounts in your name.

To place a credit freeze, you must **contact each of the three credit reporting agencies separately at the companies' credit freeze websites.**

Cost: A freeze might be free, depending on your state and circumstances. For example, if you're an identity-theft victim and have filed a police report about the incident. Otherwise, expect to pay a small fee to initiate or temporarily lift a freeze at each credit bureau.

How long it lasts: If you place a credit freeze, you'll get a PIN number to use each time you want to freeze, unfreeze and refreeze the account. In almost all states, a credit freeze lasts until you temporarily lift it or permanently remove it. In a few states, it expires after seven years.

Step 3:

File a complaint with the Federal Trade Commission.

Generate a trail of evidence and help fight fraud, too.

Although it doesn't guarantee an immediate fix for you, you can help combat fraud worldwide by filing a complaint with the Federal Trade Commission (FTC). Credit reporting agencies, credit card companies, banks and others may require an FTC Identity Theft Report as part of their reporting process, so be sure to get (and keep) a copy of your complaint.

Online:

ftc.gov/complaint

By phone:

(877) FTC-HELP (877-382-4357)

Step 4:

Make a report with local law enforcement.

File a sworn statement to help protect yourself.

If someone has taken your personal information and used it to commit fraud in your name, that is a crime and you are a victim. Filing a police report gives you documented proof that you've declared your innocence and stated you are not responsible for any crimes committed using your name.

What to Know About Filing a Police Report

Some local law enforcement agencies may allow you to file a report online; others will ask you to make a report in person. Call or visit their website for more information.

Regardless of how you file, here's what you'll need in order to make the report:

- A copy of your FTC Identity Theft Report (Step 3)
- A government-issued photo ID (driver's license, passport, U.S. military ID)
- Proof of address (mortgage statement, rental agreement, utility bill)
- Evidence of the theft (credit card statements showing fraudulent transactions, credit reports, collection letters)

Tips:

- Ask for a copy of the report to keep for your records. You may need to provide copies of this report to credit agencies or creditors.
- If local law enforcement is unable to take your report as an identity theft report, file it as a miscellaneous incident report.
- If you have trouble filing a report, contact your state Attorney General's office.

Step 5:

Submit a dispute to the credit reporting agencies.

Ask for an investigation and removal of fraudulent charges and accounts.

Although you're a victim of crime, credit reporting agencies will not automatically fix your credit report. After reviewing your credit report (Step 1) and identifying fraudulent charges, you'll need to file a dispute with each agency. Include as much detail and supporting documentation as possible, including an FTC Identity Theft Report (Step 3) and police report (Step 4). Ask that the credit agency block or remove fraudulent activity from your credit report.

Mail Your Dispute Resolution Letters

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069

(800) 525-6285

Experian

P.O Box 9554
Allen, TX 75013

(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016

(800) 680-7289

Get Up to Three Free Credit Reports Each Year

You can request a copy of your credit report at no cost to you once each year by visiting the government-approved website **AnnualCreditReport.com.** You're entitled to a free credit report from each of the three major credit reporting agencies every year, too. Since you have three reports available to you each year, mark your calendar to request one report every four months.

Step 6:

Be wary of credit repair companies.

Know that there's no quick fix for getting back to normal.

Identity theft can really disrupt your life. It takes time to get through it. Don't be discouraged. Don't rush the process. And don't be fooled by companies that claim to be able to fix your credit fast. It's not that easy—and it certainly doesn't have to cost you what they charge.

There's little that a credit repair company can do that you can't do yourself. If you've already taken Steps 1-5, you're well on your way!

Credit Repair Companies: Signs of a Scam

- The company has nothing but a website: no phone number, no physical location, no live person to talk to. You should be able to speak to a person when you call your credit repair agency as the agency should want to talk with you directly so that they can fully understand your needs and situation.
- The company insists you pay them before they do any work.
- They don't explain your legal rights when they tell you what they'll do for you.
- They insist on assigning you a credit profile number or credit privacy number, or ask that you contact the IRS for an employer identification number (EIN), instead of using your Social Security Number.
- They tell you not to contact any of the credit reporting companies yourself.
- They ask you to dispute information that's found on your credit report even if it's accurate.
- They encourage you to falsify information on credit or loan applications.

Step 7:

Adopt new habits.

Become even more proactive about keeping your identity safe.

You've already taken most of the steps to recover, but here are some other ways to help yourself.

Know your rights. Even when you've acted quickly and handled everything correctly, you still might encounter roadblocks on the way to recovering your identity. Visit the FTC's website (www.identitytheft.gov) for a list of your rights, as well as other helpful resources.

Be a responsible borrower. Continue to pay your debts in full and on time. Keep balances low on credit cards and revolving credit accounts.

Look for signs of fraud. Continually review your bank activity, credit card balances, and monthly statements to make sure all the charges shown are actually yours. Monitor your credit reports, looking for accounts you didn't open, inquiries you don't recognize, unusual payment histories and unfamiliar personal information. (See Step 5 for how to get three free copies of your credit report each year.)

Act quickly. As soon as you see something that doesn't look right, get in touch with your bank, business, utility, credit card company, etc. Repeat Steps 1-7, as necessary.

Remain vigilant. Just like panic, the other extreme—complacency—can hurt you. A common mistake of identity theft victims is assuming that once the damage is done and the clean up is over, all's well. Unfortunately, identity thieves tend to aim for the same victims again and again. To prevent repeated strikes, constantly monitor your credit, and add a fraud alert or credit freeze to your credit report.

How Theft Hurts Your Credit Score

Credit reporting agencies collect information about your financial and legal background and use it to compile a credit report. If you pay your bills on time, maintain good credit and avoid legal trouble, your credit report will reflect that.

Credit reports are sold to banks, credit card companies, employers, insurers and others who may want or need to know whether you're a good risk.

When your identity is stolen, there's a good chance your credit's been compromised, too. In a typical identity theft situation, a fraudster applies for new credit, maxes it out and fails to make payments.

When a fraudster makes several credit inquiries in your name, your credit score can drop 10-20 points. Factor in the increase in credit card debt and the "missed payments" from the fraudster, and your score can go down even more.

Keeping an eye on your credit reports can help minimize or prevent inaccuracies in your credit score due to fraudulent or inaccurate activity.

Looking out for you is what we do.

That's the kind of bank we are.

Whether you've been a victim of identity theft, fraud, phishing or other financial crime, we hope this information can help you recover and rebuild, and protect you from future harm.

Learn more about Huntington's commitment to protecting our customers' information at huntington.com/Privacy-Security.

Huntington
Welcome.®