



Identity Theft: A Guide to Taking Action

Identity Theft: A Guide to Taking Action

How do you know if someone has assumed your identity?

- You apply for a credit card and are turned down because of a low credit score, yet you have always paid your bills on time.
- A debt collector calls to demand payment on an account that you have never had.
- You receive a credit card in the mail that you have never applied for.

If you experience any of the above, you could be the victim of identity theft: where an imposter is using your personal information to obtain credit.

This guide provides victims of identity theft with step-by-step instructions on how to act quickly and assertively to minimize financial damage.

- Step 1: Establish Fraud Alerts** *page 3*
- Step 2: Monitor Your Credit Report** *page 4*
- Step 3: Notify Credit Card Companies** *page 5*
- Step 4: Contact Financial Institutions & Obtain Online Access** *page 6*
- Step 5: Report Fraud to Law Enforcement** *page 7*
- Step 6: Monitor Monthly Bills** *page 8*
- Step 7: File a Complaint with the Federal Trade Commission** *page 9*
- Step 8: Research Additional Online Information** *page 10*
- Step 9: Complete the Check List Worksheet** *page 11*

Step 1: Establish Fraud Alerts

Immediately report the situation to the fraud unit of all three credit-reporting companies listed below (even though they say they will contact the others). When you do this you will be placing a fraud alert on your file, which means creditors will be required to call you before extending credit.

Experian:	1-888-397-3742 P.O. Box 9532 Allen, Texas 75013
Equifax:	1-800-525-6285 P.O. Box 740250 Atlanta, GA 30374
Trans Union:	1-800-680-7289 P.O. Box 6790 Fullerton, CA 92834

Under new provisions of the Fair Credit Reporting Act, you can place an initial fraud alert for only 90 days. Each credit bureau will mail you a notice of your rights as an identity theft victim. Once you receive this, contact the three bureaus immediately to request:

- A free copy of your credit report
 - An extension of the fraud alert to seven years (this can be canceled at any time)
-
- When you contact the credit bureaus, you will communicate with an automated system that will request your social security number and additional information.
 - Whenever you call one of the credit bureaus and speak with a representative, keep logs of all conversations using the outline on page 11 of this guide. Make sure to record the date of your call, the name of the person you speak with, and all details of the call.
 - Confirm all phone calls with a letter, and send all written communication by certified mail.
 - Keep a copy of all letters, documents, and receipts.
 - Keep a binder/folder with all information pertaining to your fraudulent situation in a secure location.

Step 2: Monitor Your Credit Report

Immediately after reporting your situation to the three credit bureaus, you may contact each of them directly to request a free copy of your credit report. Once you have received your three credit reports, examine each one carefully.

- Report fraudulent accounts and erroneous information in writing to the credit bureaus. Once you notify the credit bureaus about the fraudulent accounts, the bureau is required to block that information from future reports.
- Report fraudulent accounts and erroneous information to the credit issuers following the instructions provided on the credit reports. Make sure the accounts are closed, and action is taken to correct inaccuracies.

It's very important that you continue to monitor your credit report on an ongoing basis. Under federal law, you are entitled to one free copy of your credit report every twelve months from each of the credit bureaus. You may obtain these free reports by visiting www.AnnualCreditReport.com or by calling 1-877-322-8228.

It's suggested that you request a report every four months from one of the three agencies. This provides you with the ability to monitor your credit report three times a year at no charge.

Another way to monitor your credit report is to utilize a 24-hour monitoring service like Equifax's 3-in-1 Monitoring. For more information visit www.equifax.com.

Use the table below to record the date you requested your credit report and how it was requested.

	Date Report Was Requested	How Was Report Requested? Phone or Online
Experian		
Equifax		
Trans Union		

Step 3: Notify Credit Card Companies

Contact the credit card companies you have accounts with and request they make a notation on your account that you have been a victim of fraud.

- MasterCard: 1-800-622-7747
- Visa: 1-800-847-2911
- Discover: 1-800-347-2683
- AMEX: 1-800-528-4800

Name of Company and Phone Number	Last 4 Digits of Card Number	Date	Name of Person you Spoke With and Outcome of Call

Step 4: Contact Financial Institutions and Obtain Online Access

One of the best things you can do to protect your accounts is to obtain online access, and review the transactions that are posted each day. There's no need to wait for your monthly statement to review account activity. Online access lets you review transactions daily so you can make sure they are generated by you or another individual listed on the account.

You will also want to contact the financial institutions where you have accounts and let them know about the fraud you have experienced. Ask them if they have a process in place to flag your account.

Name of Institution and Phone Number	Date	Accounts	Name of Person you Spoke With and Outcome of Call	Registered for Online Access (Y/N)

Step 5: Report Fraud to Law Enforcement

Report the crime to your local police or sheriff's department immediately.
Please note the following:

- Prove as much documented evidence as possible.
- Make sure the police report lists the fraudulent accounts.
- Get a copy of the report. Credit card companies, credit bureaus, and other financial institutions may require you to show this report in order to verify the crime.

Date of Initial Contact: _____

Contact Phone Numbers: _____

Date of Meeting with Officer: _____

Location of Meeting with Officer: _____

Time of Meeting: _____

Officer's Name	Badge Number
_____	_____
_____	_____
_____	_____
_____	_____

Incident (Report) Number: _____

Request a Copy of Police Report: _____

Time of Police Departure: _____



Step 6: Monitor Monthly Bills

Make a list of all statements you receive:

- Electric/Gas Bill
- Water Bill
- Telephone (Cell Phone)/Cable Bill
- Insurance Bills
- Credit Cards
- Loan Payments
- Medical Bills
- Other Utilities

Make a check mark below when bill arrives

Company Name	Phone Number	Date monthly bill arrives							

Step 7: File a Complaint with the Federal Trade Commission

The FTC serves as the federal clearinghouse for complaints reported by victims of identity theft. Every identity theft case reported helps the FTC investigate fraud, and can lead to law enforcement action. Include your police report number.

You have three options to choose from when reporting your situation:

Complete an online form:

[https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z_ORG_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03)

Call to report:

1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261

Mail to:

Identity Theft Clearinghouse, Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

What to include in your complaint:

- All your personal information:
 - Name
 - Address
 - Phone Numbers
 - Social Security Number
 - Date of Birth
 - E-mail address
- The types of identity theft you have experienced:
 - Credit Cards
 - Checking/Saving Accounts/Loans
 - Phone/Utilities
 - Internet/E-mail
 - Government Documents
 - Securities/Other Investments
- A full detailed description of your complaint:
 - When did you become aware of your ID theft?
 - When did the first incident occur?
 - How many accounts were opened?
 - How much have you had to pay?
- Any information you have discovered about the identity thief.
- What steps you have already taken:
 - Reported with all three credit bureaus?
 - Fraud alert placed on reports?
 - Ordered credit report?
 - Any problems with credit bureaus?
 - Contacted the police? (provide your police report number)
 - Problems with any financial institution or other organization?

Step 8: Research Additional Online Information

This document contains what we believe to be current best practices, however, there are additional information sources you might consider accessing. We have listed a few resources below, however there are many available. When researching information online it's critical that you access reputable sources. This will help you avoid scam artists who have a legitimate looking web site, but are waiting to take advantage of individuals who are seeking information on identity theft and fraud.

1st Source Bank Infosource:

<https://www.1stsource.com/infosourceonline/index.jsp>

Experian:

<http://www.experian.com/>

Equifax:

<http://equifax.com/>

Trans Union:

<http://www.transunion.com/index.jsp>

Free Credit Report – Sponsored site of the 3 reporting agencies:

<http://www.freecreditreport.com/>

Federal Trade Commission – National Resource for ID Theft:

<http://www.consumer.gov/idtheft/>

Social Security Online:

<http://www.ssa.gov/pubs/idtheft.htm>

Identity Theft Resource Center:

<http://www.idtheftcenter.org/alerts.shtml>

Step 9: Complete Identity Theft Checklist

The check list below is a way for you to keep track of the action steps you have taken to protect yourself against identity theft.

- Establish Fraud Alerts
- Monitor Your Credit Report
- Notify Credit Card Companies
- Contact Financial Institutions and Obtain Online Access
- Report Fraud to Law Enforcement
- Monitor Monthly Bills
- File a Complaint with the Federal Trade Commission
- Research Additional Online Resources
- Monitor Your Credit Report on an Ongoing Basis

