

How to Report Identity Theft

What Happens To You

This guide provides victims of identity theft with the major resources to contact. Unfortunately, at this time victims themselves are burdened with resolving the problem. You must act quickly and assertively to minimize the damage. In dealing with the authorities and financial institutions, keep a log of all conversations, including dates, names, and phone numbers. Note time spent and any expenses incurred, in case you are able to request restitution in a later judgment or conviction against the thief. Confirm conversations in writing. Send correspondence by certified mail, return receipt requested. Keep copies of all letters and documents.

Credit Bureaus - Immediate Action!

If you feel that you are a victim of Identity Theft, you only need to contact one number to notify all three major credit bureaus: 877-ID-THEFT ((877) 438-4338)

To contact the three major credit bureaus individually, call or contact the fraud units at:

Trans Union: Report fraud at P.O. Box 6790, Fullerton, CA 82834 or call (800) 680-7289. For more information visit www.transunion.com

Equifax: Report fraud at P.O. Box 740241, Atlanta, GA 30348 or call (888) 766-0008. For more information visit www.equifax.com

Experian (formerly TRW): Report fraud at P.O. Box 2002, Allen, TX 75013 or call (888) 397-3742. For more information visit www.experian.com

Report the theft of your credit cards or numbers and request a credit report (free to identity theft victims). Ask that your file be flagged with a fraud alert. Add a victim's statement to your report ("My ID has been used to apply for credit fraudulently. Contact me at [your phone number] to verify all applications"). Ask how long the fraud alert is posted on your file, and how you can extend it if necessary.

Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Request a free copy of your credit report every few months so you can monitor any new fraudulent activity. Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers). When you provide your police report to the credit bureaus, they must remove the fraudulent accounts from your credit report (Law Enforcement below).

Remember, you are entitled to a free credit report if you are a victim of identity theft, if you have been denied credit, if you receive welfare benefits, or if you are unemployed.

Creditors

Contact all creditors immediately with whom your name has been used fraudulently, by phone and in writing. You may be asked to fill out fraud affidavits (No law requires these to be notarized at your own expense). Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request" (better than "card lost or stolen" because it can be interpreted as blaming you). Monitor your mail and bills for evidence of new fraudulent activity. Report it immediately to creditor grantors.

Law Enforcement

Report the crime to your local police or sheriff's department. You might also need to report it to police departments where the crime occurred. Give them as much documented evidence as possible. Make sure the police report lists the fraud accounts. Get a copy of the report. Keep the phone number of your investigator handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime. It is a violation of federal law (18 USC 1028) and the laws of many states to assume someone's identity for fraudulent purposes. Some police departments do not write reports on such crimes, so be persistent! Also, report this to the Federal Trade Commission at (877) IDTHEFT.

Stolen Checks

If you have had checks stolen or bank/credit union accounts set up fraudulently, report it to the appropriate check verification companies (see below). If check numbers are known, put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses.

To report fraudulent use of your checks:

Chexsystems: (800) 428-9623
CrossCheck: (800) 843-0760
TeleCheck: (800) 710-9898

ATM Cards

If your ATM or debit card has been stolen or compromised, report it immediately. Get a new card and Personal Identification Number (PIN). Do not use your old PIN. When creating a PIN, do not use common numbers like the last four digits of your SSN or your birth date. Monitor your account statement. You may be liable if fraud is not reported quickly.

Visit a branch near you or call (870) 862-5121 for our Electronic Banking Department.

Fraudulent Change of Address

Notify the local Postal Inspector if you suspect an identity thief has filed a change of your address with the post office or has used the mail to commit fraud (Call the U.S. Post Office to obtain the phone number). Find out where fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the mail carrier.

Social Security Number (SSN) Misuse

Call the Social Security Administration to report fraudulent use of your SSN. Order a copy of your Personal Earnings and Benefits Statement and check it for accuracy. The thief might be using your SSN for employment purposes.

Social Security Administration - Report fraud: (800) 269-0271.
Order Earnings & Benefits Statement: (800) 772-1213.

Passports

Whether you have a passport or not, write the passport office to alert them to anyone ordering a passport fraudulently.

Driver's License Number Misuse

You may need to change your driver's license number if someone is using yours as ID on bad checks or for other types of fraud. Call the state office of the Revenue Department of Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local Revenue Department or DMV to request a new number. Fill out a complaint form to begin the investigation process. Send supporting documents with the completed form to the nearest office for investigation.

Victim Statements

If the imposter is apprehended by law enforcement and stands trial, write a victim impact letter to the judge handling the case. Contact the victim-witness assistance program in your area for further information on how to make your voice heard in the legal proceedings.

Don't Give In

Do not pay any bill or portion of a bill that is a result of identity theft. Do not cover any checks that were written and/or cashed fraudulently. Do not file for bankruptcy. Your credit rating should not be permanently affected, and no legal action should be taken against you. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills. Report such attempts to government regulators immediately.

Opt-Out or In

To opt-out or in of pre-approved offers of credit for all three bureaus, call (888) 5OPTOUT ((888) 567-8688), you may choose a five year opt-out period or permanent opt-out status. Remember, you are entitled to a free credit report if you are a victim of identity theft, if you have been denied credit, if you receive welfare benefits, or if you are unemployed.