



IDENTITY THEFT PROCEDURES

Step 1 - If you believe you have been the victim of Identity Theft, contact the following numbers and report that you may or have been a victim of Identity Theft. Instruct the rep to place a "Fraud Alert" on your credit report. A "Fraud Alert" will require an issuer of credit to first contact you by phone before any credit is extended. An initial "Fraud Alert" is only good for 90 days. To have a seven year "Fraud Alert" placed on your report, you will need to provide the credit bureaus with a police report.

For even greater security, it is recommended that you place a **SECURITY FREEZE** on your credit file. A security freeze essentially blocks any potential creditors from being able to view or "pull" your credit file; unless you affirmatively unfreeze or thaw your file beforehand. With a freeze in place on your credit file, ID thieves can apply for credit in your name all they want, but they will not succeed in getting new lines of credit in your name because few if any creditors will extend that credit without first being able to gauge how risky it is to loan to you (i.e., view your credit file). And because each credit inquiry caused by a creditor has the potential to lower your credit score, the freeze also helps protect your score, which is what most lenders use to decide whether to grant you credit when you truly do want it and apply for it.

Credit Bureaus:

- **Equifax Credit Bureau (Fraud Hotline) (800) 525-6285**
- **Experian Information Solutions (888) 397-3742**
- **Trans Union Credit Bureau (Fraud Hotline) (800) 680-7289**
- **Innovis (800) 540-2505**

Step 2 - Victims should maintain one central file that contains all relevant documentation concerning the fraud. This file is for the victims to maintain only and should be kept in a secure location.

The file should include:

- A timeline of identity theft events,
- The police report; if any,
- The identity theft affidavit,
- The victim's most recent credit report from each of the three credit reporting companies,
- The victim's Internal Revenue Service identity theft affidavit,
- Any evidence of the identity theft,
- All written or email communication with creditors, banks, financial institutions, or credit reporting companies, and
- Logs of any phone conversations, with dates, names, and phone numbers of representatives to whom the victim spoke, and notes on what information was given.

Step 3 - Report the Identity Theft to the Federal Trade Commission

Federal Trade Commission Complaint Assistant
(877) 438-4338 or www.ftccomplaintassistant.gov

- After completing the complaint process, the victim should print the identity theft affidavit created by the completion of the report.
- This affidavit will be used by local law enforcement to create a police report.
- Once completed, this report remains in the FTC's database and is entered into the Consumer Sentinel Network, which is used by agencies to track and investigate financial fraud.
- This step, while important, will not initiate a criminal investigation. The FTC does not resolve individual consumer complaints.

Step 4 - Report the Identity Theft to Law Enforcement

After receiving an identity theft affidavit, the victim may ask the local police department to create a police report documenting the identity theft allegation. If the local police will not create the report, seek out other local law enforcement or contact the local office of the Federal Bureau of Investigation.

The victim will need to bring:

- The identity theft affidavit from the FTC's Complaint Assistant,
- Government identification,
- Proof of address, and
- Any other proof of the identity theft.

Step 5 - Contact the Internal Revenue Service

Even if you do not think the identity theft is related to your taxes, it is possible that your Social Security Number could be used to file fraudulent tax returns. The IRS assists with cases involving identity theft.

IRS Identity Protection Specialized Unit (800) 908-4490

Step 6 - Contact the Social Security Administration

If you suspect your Social Security Number has been misused, you should call the Social Security Administration to report the misuse and find out if a new Social Security Number is necessary.

Social Security Administration Fraud Hotline (800) 269-0271

(866) 501-2101 (TTY)

P.O. Box 17785

Baltimore, MD 21235

Step 7 - Contact Financial Institutions:

Contact your financial institutions, credit card issuers, etc. and go over your account history. Report attempts to your institution and request added security. Consider placing a password or phrase on your account that you will remember, but that the fraudsters will not be able to guess.

Resources Available:

- Federal Bureau of Investigation
 - www.fbi.gov/about-us/investigate/cyber/identity_theft
 - Protection tips, how to report identity theft, and real-life FBI cases.

- Federal Trade Commission
 - www.consumer.ftc.gov/features/feature-0014-identity-theft
 - Types of identity theft, how to protect your identity, and a guide to assist identity theft victims.

- Identity Theft Resource Center
 - www.idtheftcenter.org
 - Educational resources, scam alerts, how to get help, and a special section for teens.

- National Identity Theft Victims Assistance Network
 - www.identitytheftnetwork.org
 - Instructions for recovery, training for professionals, and a national resource map to find local organizations, state laws, and more.

- StopFraud.gov
 - www.stopfraud.gov/protect-identity.html
 - How to protect yourself, along with a robust library of identity theft resources and publications put out by federal organizations.

- Internet Crime Complaint Center
 - www.ic3.gov
 - A partnership between the FBI and the National White Collar Crime Center

- OnGuardOnline
 - www.onguardonline.gov
 - The federal government's website to help you be safe, secure, and responsible online.

- National Crime Victim Bar Association
2000 M Street, NW, Suite 480 Washington, DC 20036
(202) 467-8716
Referral line is open from 8:30a.m. - 5:30p.m. (ET), Monday through Friday.
Questions can also be emailed to victimbar@ncvc.org