MARYLAND ATTORNEY GENERAL'S OFFICE
(410) 576-6300
1 (888) 743-0023 TOLL-FREE
TDD: (410) 576-6372

200 ST. PAUL PLACE, BALTIMORE, MD 21202

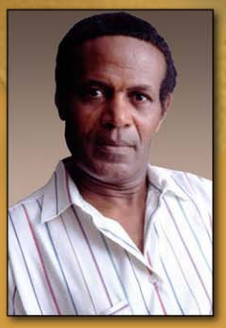
WWW.OAG.STATE.MD.US




IDENTITY THEFT: WHAT TO DO IF IT HAPPENS TO YOU

CONSUMER PROTECTION DIVISION,
MARYLAND ATTORNEY GENERAL'S OFFICE
DOUGLAS F. GANSLER, ATTORNEY GENERAL






Identity Theft: What to Do if It Happens to You

When someone else uses your name, Social Security number, bank account number, credit card number or other personal identifying information to commit fraud, it is called "identity theft." The imposter may open credit accounts, obtain a driver's license or apply for insurance benefits in your name, and create havoc with your personal finances. While identity theft is a crime that can be prosecuted, the thief is often difficult to track. It is important to act quickly and assertively to minimize the damage to your credit history. This guide provides victims a step-by-step process to address the problems caused by identity theft and instructions on how to contact the major resources.

In dealing with the authorities and financial institutions, it is very important to 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 all correspondence by certified mail, return receipt requested. Keep copies of all letters and documents.

1. Credit bureaus. Immediately place a fraud alert on your credit reports and review your credit reports. Call any one of the three major credit reporting companies (Experian, Equifax and TransUnion, numbers below). The company you call is required to contact the other two so that they can put a fraud alert on their file too. Ask to add a victim's statement to your report, such as: "My ID has been used to apply for credit fraudulently. Contact me at [your telephone number] to verify all applications."

You are entitled to a free credit report once your file has been flagged with a fraud alert. Carefully review the report for signs of ID theft, including addresses where you have never lived or accounts you did not open. Often, ID theft victims learn of the crime by finding

fraudulent account information on their credit reports. Fraud alerts are placed for 90 days, after which you can renew them for another 90 days. A victim of identity theft with a police report can also ask for an extended seven-year fraud alert.

Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. You should request a copy of your credit report every few months for a while to monitor for fraud. If you requested the extended seven-year fraud alert on your credit report, you are entitled to free credit reports within 12 months from each of the three credit reporting companies.

Ask the credit bureaus about their procedures for investigating and removing erroneous information from your report. The ID Theft Unit has sample letters you can use to dispute fraudulent accounts on your credit report. Ask them for the phone numbers and addresses of credit grantors with whom fraudulent accounts have been opened. If a credit bureau removes erroneous information in your report, ask it to send an updated report to anyone who received your report in the last year (two years for employers).

	Equifax	**Experian**	**Trans Union**
Report Fraud:	(888) 766-0008	(888) 397-3742	(800) 680-7289
Order Credit Report:	(800) 685-1111	(888) 397-3742	(800) 680-7289
Website:	www.equifax.com	www.experian.com	www.transunion.com

To access your free credit report through the federal Fair Credit Reporting Act, call 1(877) 322-8228 or go to www.annualcreditreport.com. You are also entitled to a second free copy of your credit report each year under Maryland law, which may be obtained by contacting the credit bureaus at their toll-free numbers.

If the credit bureaus are not responsive to your requests, contact the State of Maryland Division of Financial Regulation at (410) 330-6830.

2. Law enforcement. Report the fraudulent activity to your local police or sheriff's department. Under Maryland law (Criminal Law Article, § 8-304), your local police department must take a report of identity theft and provide you with a copy. Give them as much documented evidence as possible. Make sure the police report lists the fraudulent accounts and any other relevant information. Keep the phone number of the fraud investigator handy and give it to creditors and others who require verification of your case. You will need a copy of a police report to dispute fraudulent charges on existing accounts, close fraudulently-opened accounts and block fraudulent information on your credit report. If a police department refuses to take a report, contact the ID Theft Unit for help.

3. File a complaint with the Federal Trade Commission, and fill out an ID Theft Affidavit:

- www.ftc.gov/idtheft
- 1 (877) ID Theft (438-4338)

4. Credit Freezes. In addition to placing a fraud alert on your credit report, Maryland law allows you to place a "Credit Freeze"that blocks credit reporting agencies from sharing your credit report with potential creditors without your express permission. A credit freeze can help prevent identity theft. Most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and Social Security number would probably not be able to get credit in your name. Maryland law prohibits credit reporting agencies from charging more than $5 per credit freeze.

You can place a "freeze" on your credit report either by certified mail, through the credit reporting agencies' websites or, after January 2010, over the phone. Each of the credit reporting agencies requires slightly different information-- make sure to check their websites to see exactly what is required at: www.transunion.com, www.equifax.com, and www.experian.com. Generally, you will need to include your name, addresses from the past five years, Social Security number,

date of birth, a utility bill showing you at your current address, and the $5.00 fee payable by check, money order or credit card. Credit freezes are free to identity theft victims if you send a copy of your police report with the letter requesting the freeze. If you send your freeze requests via certified mail, address them to:

Equifax Security Freeze
P.O. Box 105788 Atlanta, GA 30348

- Full name, address, Social Security number and date of birth.
- A copy of your police report, or other investigative report filed with law enforcement, if you are an ID theft victim to be eligible for a free freeze.
- If you have moved in the past two years or had a name change, you should provide that prior address or name so you can be properly identified.

Experian Security Freeze
P. O. Box 9554 Allen, TX 75013

- Full name, address, Social Security number and date of birth.
- A copy of your police report, or other investigative report filed with law enforcement, if you are an ID theft victim to be eligible for a free freeze.
- If you have moved or had a name change in the past five years, prior addresses and proof of prior names are also required.

Trans Union Security Freeze
P.O. Box 6790 Fullerton, CA 92834

- Full name, address, Social Security number and date of birth.
- A copy of your police report, or other investigative report filed with law enforcement, if you are an ID theft victim to be eligible for a free freeze.
- If you have moved in the past five years, supply addresses for past five years.

5. Identity Theft Passport. One of the tools the Consumer Protection Division can offer you is an Identity Theft Passport. The Passport may help you resolve financial issues caused by identity theft and help prevent accidental arrest if a thief uses your personal identifying information during the commission of a crime. Once you have obtained a police report from your local law enforcement agency, you can apply for a Passport through the Identity Theft Unit. Contact the Identity Theft Unit at IDTheft@oag.state.md.us or by phone at 410-576-6491 for additional information and an application.

6. New Account Fraud. Immediately contact all creditors with whom your name has been used fraudulently, by phone and in writing. You may see evidence of these accounts on your credit reports. Creditors are likely to ask you to fill out a fraud affidavit. The Federal Trade Commission provides a uniform affidavit form that most creditors accept (available online at www.consumer.gov/idtheft). Ask the credit grantors to furnish you and your local law enforcement agency copies of documents such as the thief's applications for credit and the transaction records of the fraudulent transactions. You may have to formally request that fraudulent accounts be closed and the information be sent to you. You will need a copy of a police report. Contact the ID Theft Unit for sample request letters.

7. Existing Account Fraud. Credit Cards. If your existing credit accounts have been used fraudulently, get replacement credit cards with new account numbers. You should report the fraud as soon as possible in writing to your credit card company. Under federal law, you have 60 days to report the fraudulent charges to the credit card company. If you report the fraud within the time limit, the credit card company cannot hold you accountable for more than $50 worth of the charges. Monitor your mail and credit card bills for evidence of new fraudulent activity and report it immediately to credit grantors. Add passwords to all accounts.

ATM cards. If your ATM or debit card has been stolen or compromised, report it to your bank immediately and request a fraud affidavit. Get a new card, account number and password. Do

not use your old password. Monitor your account statement. Under federal law, you are afforded more protection for your credit cards than your ATM or debit cards. We recommend using a credit, not debit, card for online purchases. If an ID thief uses your debit card for fraudulent transactions and you report it within two business days, you are liable for up to $50. If you report the problem between two and 60 days after it occurs, you are liable for up to $500. If you do not notice and report the problem within 60 days, you could be responsible for all unauthorized charges.

PayPal and other escrow services: Read any user agreement carefully before signing up to see what security and privacy steps the company takes to protect your information, and review the company's fraud recovery provisions. For example, if you notify PayPal of a fraudulent charge within 60 days of discovering it, they will not hold you financially liable. Close any accounts related to the service to avoid further fraud and report the charges to your bank or credit card company.

8. Phone and utility services. If a thief has established phone or other utility services in your name or you discover fraudulent charges on your bill, contact the service provider immediately to cancel the account and open a new one. Provide a password that must be used any time the account is changed. You can dispute charges on your existing utility account or fraudulently opened accounts the same way you can for other new accounts (see #6, above).

9. Debt Collectors. If debt collectors demand that you pay the unpaid bills on fraudulent credit accounts, ask for the name of the collection company, the name of the person contacting you, phone number and address. Tell the collector that you are the victim of fraud and are not responsible for the account. Ask the collector for the name and contact information for the referring credit issuer, the amount of the debt, account number and dates of the charges. Under federal law, you are entitled to receive all information about the debt that you would be entitled to see if the debt were actually yours. The collector must inform the creditor that you are a victim

of identity theft. Once a creditor is notified that a debt is the work of an identity thief, it cannot sell that debt or place it for collection. Ask the collector if they need you to complete their fraud affidavit form or if you can use the Federal Trade Commission form. Follow up in writing to the debt collector explaining your situation. Ask that they confirm in writing that you do not owe the debt and that the account has been closed.

10. Stolen checks and fraudulent bank accounts. If a thief has stolen checks or written counterfeit checks on your account, notify your bank. The bank should provide you with a fraud affidavit. Stop payment on the checks, close your checking and saving accounts and open new ones with new account numbers. Set a password for the new accounts. Ask the bank to notify the check verification service with which it does business so that retailers will be alerted not to accept those checks. If someone has opened an account using your information, notify that bank. If your checks have been stolen and you know where the thief has used them, contact the verification company that the merchant uses:

- CheckRite: 1 (800) 766-2748
- ChexSystems: 1 (800) 428-9623 (closed checking accounts)
- CrossCheck: 1 (800) 552-1900
- Certegy, Inc. (previously Equifax Check Systems): 1 (800) 437-5120
- National Processing Co. (NPC) - 1 (800) 526-5380
- TeleCheck: 1 (800) 710-9898

To find out if the identity thief has been passing bad checks in your name, call:

- SCAN: 1 (800) 262-7771

11. Fraudulent change of address. Notify the U.S. Postal Inspection Service (in Maryland, call 410-715-7700) if you suspect an identity thief has filed a change of your address with the post office or has used the mail to commit credit or bank fraud. 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.

12. Social Security Number (SSN) misuse. The Social Security Administration's Office of the Inspector General investigates cases that involve the use of your SSN to fraudulently obtain Social Security benefits. Report this fraud to the Social Security Administration at 1 (800) 269-0271.

13. Driver's license number misuse. You may be able to change your driver's license number if someone is using yours as identification on bad checks. Call the Maryland Motor Vehicle Administration at 1 (800) 950-1682 to see if you qualify to be issued a new number. You can also find out if a replacement license has been issued in your name and ask to have a fraud alert put on your license.

14. 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 of your local State's Attorney's Office or the Office of the Attorney General for further information on how to make your voice heard in the legal proceedings.

15. False bankruptcies. If someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A list of the U.S. Trustee Program's Regional Offices is available on the U.S. Department of Justice Web site at www.usdoj.gov/ust. You may need to hire a lawyer to help convince the bankruptcy court that the filing is fraudulent.

16. Criminal Identity Theft. Criminal identity theft includes a person fraudulently using your personal information in the commission of a crime. Sometimes victims of identity theft learn that imposters using their name were arrested or had arrest warrants issued against them. If criminal violations are wrongfully attributed to your name, contact the police department that arrested the person using your identity, or the court agency that issued the warrant for

the arrest. Explain that this is a case of misidentification and that someone is using your personal information. You may need to file an impersonation report to confirm your identity. If the arrest warrant is from a state or county other than where you live, ask your local police department to send the impersonation report to the appropriate police department. In addition to correcting your record in criminal justice databases, you'll also want to clear your name in court records. Contact the State's Attorney's office in the county where the case was prosecuted. To contact the State's Attorney's office in the jurisdiction where the warrant was issued, go to www.mdsaa.org for a listing of all State's Attorneys offices.

Clearing your name of wrongful criminal records can be challenging. The Privacy Rights Clearinghouse (www.privacyrights.org or 619-298-3396) has a helpful fact sheet, "Criminal Identity Theft." You may need to hire a criminal defense attorney to help you clear your name. Contact your local bar association for help in finding an attorney.

17. Legal help. You may want to consult an attorney to determine legal action to take against creditors and/or credit bureaus if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor. Call the local Bar Association, a Legal Aid office in your area (for low-income households), or the National Association of Consumer Advocates (www.naca.net) to find an attorney who specializes in consumer law, the Fair Credit Reporting Act and the Fair Credit Billing Act.

18. Don't give in. Do not pay any bill or portion of a bill which is the result of identity theft. Do not cover any checks which 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.

19. Keep all records and write everything down. You will need many of the documents you receive over the course of the recovery process, keep them together in a safe place. Keep a log of all phone conversations (names, phone numbers, dates) and follow up in writing. Use certified mail, return receipt requested for all correspondence.

Other Useful Resources

- ***Federal Trade Commission***
  The FTC offers a universal fraud affidavit and an in-depth guide for recovering from identity theft. Victims can also file a complaint with the FTC that may help law enforcement investigate and prosecute identity thieves.
  www.consumer.gov/idtheft
  (877) ID-THEFT (438-4338)

- ***Privacy Rights Clearinghouse***
  The Privacy Rights Clearinghouse offers information on identity theft and privacy issues.
  www.privacyrights.org
  619-298-3396

- ***Identity Theft Resource Center***
  The Identity Theft Resource Center is a non-profit organization dedicated to the understanding and prevention of identity theft.
  http://www.idtheftcenter.org/
  PO Box 26833
  San Diego, CA 92196
  858-693-7936
  Mon-Fri 9:00 A.M.-4:30 P.M. Pacific Time

In Maryland, it is a crime to obtain a person's identifying information or assume another person's identity in order to obtain any benefit or thing of value, to avoid the payment of a debt, or to avoid prosecution for a crime. A person convicted of this crime is subject to a fine up to $25,000 or up to 15 years in prison or both. The court may also order the person to make restitution to the victim for reasonable costs incurred, including attorney's fees for clearing the victim's credit history or as the result of any civil proceeding that arose because of the crime.

Consumer Protection Division
Office of the Attorney General

200 St. Paul Place
Baltimore, MD 21202

Toll-free: 1 (888) 743-0023
Consumer complaint hotline: 410-528-8662

Identity Theft Unit:
idtheft@oag.state.md.us
www.oag.state.md.us/idtheft
410-576-6491

Revised 07/08

Notes: