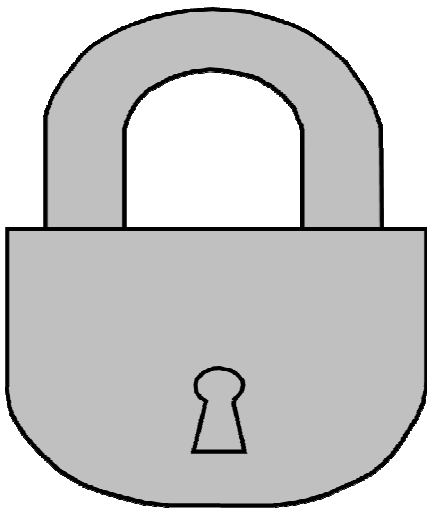


**Maryland Crime
Victims' Resource
Center, Inc.**

Identity Theft & Fraud Victim Resource Packet



1001 Prince George's Boulevard, Suite 750

Upper Marlboro, MD 20774-7427

1-877-VICTIM1

301-952-0063

www.mdcrimevictims.org

fraud@mdcrimevictims.org

One Person can make a difference and every person should try.

MARYLAND CRIME VICTIMS' RESOURCE CENTER, INC.

After their oldest daughter, Stephanie, was brutally murdered in 1982, her parents, Roberta and Vince Roper, learned they had few rights in the criminal justice system. As a result they founded the agency that bore their daughter's name, the Stephanie Roper Committee and Foundation, now known as the Maryland Crime Victims' Resource Center, Inc. (MCVRC). Today, the MCVRC is one of the most successful grassroots organizations in the history of Maryland. They have been instrumental in passing more than 70 pieces of state legislation.

Over the years MCVRC has diversified its services to include criminal justice education, court accompaniment, therapeutic counseling, support groups, community education, prevention education, legal information and assistance, direct legal representation, policy advocacy, technical assistance for allied professionals and criminal justice agencies, and faith-based referrals. As a non-profit organization, our services are free, but they rely on individual and community support to accomplish their mission: *To ensure that victims of crime receive justice and are treated with dignity and compassion through comprehensive victims' rights and services.*

Over the past decade, identity theft and fraud have become an increasing problem throughout the nation. The problem is becoming more complex, challenging, and costly. Due to the large amount of individuals affected by identity theft and fraud, Maryland Crime Victims' Resource Center, Inc., with the support of Office for Victims of Crime, will be working in conjunction with other national and local agencies to serve victims to the best of our ability. The funding awarded to MCVRC is being used to enhance its existing practice to provide free assistance to victims of identity theft and financial fraud through increasing **direct victim services, self-advocacy, and pro bono attorney development.** Our services include providing victims with legal representation on the state and federal levels.

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. Be sure to **note time spent and any expenses incurred**, in case you are able to request restitution in a later judgment or conviction. Make sure you confirm conversations in writing, and send all correspondence by certified mail, **return receipt requested.** Keep **copies of all letters and documents.**

This pamphlet is supported by Grant No. 2007-VF-GX-K033 awarded by the Office for Victims of Crime (OVC), Office of Justice Programs, U.S. Department of Justice. Points of view in this presentation and accompanying documents are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

WHERE TO BEGIN

- Get two folders, large envelopes, or other containers in which to keep documents (feel free to use folder provided).
- Label one “ORIGINALS.” In it keep the originals of all materials you compile. Do not send your original documents to anyone. Keep them safe.
- Label the second folder “COPIES.” In this folder, keep copies of EVERYTHING relevant to your identity theft/fraud case.
- Use this packet to keep track of your progress.
- Prepare yourself mentally and emotionally. Know that clearing your credit history may take many months and will take many hours of your time. You may also incur out-of-pocket expenses such as postage and copying. It is worth the effort.
- Understand that you may not be able to speak to a live person on the telephone when contacting businesses, as many companies use automated systems.
- Send all mail certified, return receipt requested. This is expensive but worth it because it allows you to prove that the addressees received your letters. Be sure to record the certified mail number on the copy of the letters you send. When you receive the postal service return card, attach it to the letter.
- Keep track of your time. Each table in this packet contains a column for you to record the time you spent working on your case. Record every minute because they add up.
- Keep track of all expenses. Keep receipts in an envelope in case you need to make copies later.
- Contact MCVRC if you need help anywhere in the process: 1-877-VICTIM1

The first thing you will be asked to do is prove who you are. You will need copies of your driver’s license of government issued ID card, your Social Security card, and most recent utility bills. You may need to prove your residence address for the last 5 years. Companies prefer to use utility bills as proof of address. Contact your utility provider and request a printout showing where you have had service for the past 5 years.

PROVING WHO I AM

My full name:

DOB:

Social Security Number:

Driver’s License Number or ID Number:

Addresses for the past 5 years:

The second thing you will be asked is, “Why do you think you are a victim of identity theft?” Make your answer as short yet as complete as possible. Answer the questions below as accurately as possible. Use the chart below as a guide when you speak to anyone about your identity theft. This will help you keep your communications consistent. You will use this information repeatedly in making reports and collecting evidence of your identity theft.

Question	Answer
<p>How did you find out your identity was stolen? Examples: I was turned down for a car loan, or I got calls from a bill collector.</p>	
<p>When did you find out that your identity had been stolen?</p>	
<p>What existing accounts were opened fraudulently using your identity? Include as much information as you have.</p>	
<p>Do you have written proof of the identity theft yet? Example: A letter from a collection agency.</p>	
<p>What existing accounts, information, or property were taken and in what amount? Include as much information as you have.</p>	

IDENTITY THEFT VICTIMS: IMMEDIATE STEPS

1. **Place a fraud alert on your credit reports** by contacting one of the credit reporting companies listed below. You only need to contact one of the three companies to place an alert, and the company you call will contact the other two, which will place an alert on their versions of your report as well.

Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your Social Security Number (SSN) will appear on your reports. Because you can get one free report per company per year, it is a good idea to stagger your report requests. Ask for a free credit report from a different company every three to four months so that you can continuously monitor your credit.

When a business sees the alert on your credit report, they must verify your identity before issuing credit in your name or SSN. As part of this verification process, the business may try to contact you directly. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

Nationwide Consumer Reporting Companies-Report Fraud

Consumer Reporting Company	Phone Number/Address	Date of Contact	Contact Person Name/Title	Comments	Date Dispute Letter Mailed	Time Spent
Equifax	1-800-525-6285 www.equifax.com					
Experian	1-888-397-3742 www.experian.com					
Transunion	1-800-680-7289 www.transunion.com					

2. **Close Compromised accounts immediately.** Call every company where an account has been tampered or opened fraudulently. Review your credit reports for additional fraudulent accounts. Close them where necessary.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. **IT'S IMPORTANT TO NOTIFY CREDIT CARD COMPANIES AND BANKS IN WRITING.** Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

Request that each fraudulently used account be closed and removed from your credit report. You should also request a copy of all applications or business transaction records relating to your identity theft; the Fair Credit Reporting Act allows you to receive this information. Your letter must include the following:

1. Proof of your identity such as a copy of your driver's license;
2. Copy of your identity theft report from police or The Federal Trade Commission (FTC) and/or an executed Identity Theft Affidavit,
3. List of each fraudulent item on your credit report.

If you follow this procedure, the credit reporting companies **MUST** remove fraudulent accounts from your credit report within 4 days unless they perform an investigation that proves the accounts to be yours, and creditors must send you copies of their records regarding accounts and transactions that are the result of identity theft. Follow this procedure for every account or transaction that is not yours. Send your letters (samples provided) by certified mail, return receipt requested and keep a copy.

We also recommend sending a business records affidavit along with your letters because records accompanied by a business records affidavit are admissible in court. This means that the state's attorney may not have to bring a live witness to court to use the records if the person who misused your identity is arrested and brought to trial.

3. **File a police report.** Contact the police in the jurisdiction where you live and file a report. You need to obtain a physical copy of this police report, NOT JUST A CASE NUMBER. This is a critical document required to clear your name. If you have a complaint report from the FTC, offer to provide a copy to the officer.

Note: Knowingly submitting false information could subject you to criminal prosecution for perjury.

You may encounter resistance. If so, be polite but firm. If you are in Maryland, you can remind the officer that under Criminal Law §8-304 law enforcement is required to prepare and file a police report.

(a) A person who knows or reasonably suspects that the person is a victim of identity fraud...may contact a local law enforcement agency that has jurisdiction over:

1. Any part of the county in which the person lives;
2. Any part of the county in which the crime occurred.

(b) After being contacted by a person in accordance with subsection (a), a local law enforcement agency shall promptly: 1. Prepare and file a report of the alleged identity fraud; and 2. Provide a copy of the report to the victim.

(c) The local law enforcement agency contacted by the victim may subsequently refer the matter to a law enforcement agency with proper jurisdiction.

(d) A report filed under this section is not required to be counted as an open case for purposes including compiling open case statistics.

Law Enforcement Authorities-Report Identity Theft

Agency/Department	Phone Number	Date	Contact Person Name/Title/Phone Number	Report Number	Comments	Time Spent

4. Report the identity theft to the Federal Trade Commission (FTC). The FTC will not investigate your case, but after making a report, your information will be entered into the Identity Theft Data Clearinghouse, a nationwide data bank that assists law enforcement in the investigation and prosecution of identity thieves.

You can file a complaint online at www.consumer.gov/idtheft. If you don't have internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (1-877-438-4338)

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

Be sure to call the Hotline to update your complaint if you have any additional information or problems.

Federal Trade Commission Complaint

Method of Contact	Date	Contact Person Name/Title	Comments	Time Spent
<input type="checkbox"/> online <input type="checkbox"/> phone				

RESOLVING SPECIFIC PROBLEMS

Bank Accounts and Fraudulent Withdrawals: Different laws determine your legal remedies based on the type of bank fraud you have suffered. Many transactions may seem to be processed electronically but are still considered "paper" transactions. If you're not sure what type of transaction the thief used to commit the fraud, ask the financial institution that processed the transaction.

Fraudulent Electronic Withdrawals: You have **60 days** from the date your bank account statement is sent to you to report in writing any money withdrawn from your account without your permission.

If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how quickly you report the loss.

- If you report the loss or theft within two business days of discovery, your losses are limited to \$50.
- If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to \$500 of what the thief withdraws.
- If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days.

If you find a fraudulent transaction, call the financial institution and follow up in writing - by certified letter, return receipt requested - so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After receiving your notification about an error on your statement, the institution generally has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that it occurred. If the institution needs more time - it may take up to 45 days to complete the investigation - but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

Fraudulent Checks and Other “Paper” Transactions: If an identity thief has passed checks in your name or using your bank accounts, notify your bank and the major check verification companies. Ask your bank to change your account number and issue new checks. Contact check verification companies to make a report of identity theft, and request that they notify retailers not to accept checks with the old account number on them.

You may be held responsible for the forgery if you fail to notify the bank in a timely matter that a check was lost or stolen.

- To request that they notify retailers who use their databases not to accept your checks, call:

- TeleCheck at 1-800-710-9898 or 1-800-927-0188

Date:

Contact Person:

- Certegy, Inc. at 1-800-437-5120

Date:

Contact Person:

Mail Theft: The United Postal Inspection Service (USPIS) is the law enforcement arm of the U.S. Postal Service, and investigates cases of identity theft. Make a report to the USPIS **only if you believe the U.S. mail was used in stealing your identity.**

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.

- USPIS

Criminal Investigations Service Center
ATTN: MAIL FRAUD
222 S. Riverside Plaza, #1250
Chicago, IL 60606-6100

1-877-876-2455
410-715-7700 (Maryland)

Online Complaint Form: <http://postalinspectors.uspis.gov/forms/idtheft.aspx>

Date Contacted:

Notes:

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.

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235

1-800-269-0271
www.socialsecurity.gov/oig

Phone Fraud: If a thief has established phone service 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. If you are having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the appropriate agency below.

- For local service, contact your state Public Utility Commission
 - Maryland: 1-800-492-0474

- For cellular phones and long distance calls, contact the Federal Communications Commission (FCC) at www.fcc.gov. The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable.
 - 1-888-CALL-FCC
 - Federal Communications Commission
Consumer Information Bureau
445 12th Street, SW, Room 5A863
Washington, DC 20554.
 - www.fcc.gov (online complaints)

Date:

Notes:

Driver's license number misuse: If you believe your name or SSN is being used by a thief to get a driver's license or a non-driver's license number, ask to substitute another number.

- Maryland Motor Vehicle Administration:
1-800-950-1682
- 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.

Date:

Notes:

- Apply for a "V" Driver's license Restriction Code: The MVA is offering a voluntary program to assist victims of identity theft by placing a "V" driver's license restriction code that will be displayed on the person's driver's license and driving record. If you have been the victim of an Identity Theft crime and would like to apply for the "V" restriction code, you must first file a report with the local law enforcement agency that has jurisdiction over:
 1. any part of the county in which the you live; or
 2. any part of the county in which the crime occurred.
- You will need to take a copy of the report to the MVA Headquarters at 6601 Ritchie Hwy, Glen Burnie, MD 21062, Investigative & Security Services Division-Room 53 and ask to speak to the Duty Chief Investigator. (410-768-7541)

- You must also take your current valid driver's license with you. After approval from a Chief Investigator, you will sign an authorization form (DL-204) granting the MVA permission to place the "V" restriction code on your driver's license and driving record. After paying the applicable fee you will then receive the driver's license displaying the "V" code.
- If someone attempts to fraudulently use your name and identifying information during a traffic stop and does not physically have the driver's license displaying the "V" code, the law enforcement officer will be alerted that you have been a victim of identity theft. The officer should then attempt to further verify the identity of the individual.

Bankruptcy Fraud: If someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where the bankruptcy was filed.

To report suspected bankruptcy fraud, please prepare a written summary that contains the following information:

- Name and address of the person or business you are reporting.
- The name of the bankruptcy case, case number, and the location of where the case was filed.
- Any identifying information you may have regarding the individual or the business.
- A brief description of the alleged fraud, including how you became aware of the fraud, and when the fraud took place. Please include all supporting documentation.
- Identify the type of asset that was concealed and its estimated dollar value, or the amount of any unreported income, undervalued asset, or other omitted asset or claim.
- Your name, address, telephone number and email address. You are not required to identify yourself, though it is often helpful to do so if questions arise.

THE LIKELIHOOD OF FURTHER INVESTIGATION AND POSSIBLE CRIMINAL PROSECUTION IS INCREASED FOR THOSE MATTERS WHERE SUPPORTING DOCUMENTATION AND SPECIFIC FACTUAL INFORMATION ARE PROVIDED. ANY INFORMATION YOU PROVIDE IS VOLUNTARY AND ITS MAINTENANCE BY THE UNITED STATES TRUSTEE PROGRAM IS AUTHORIZED BY 28 U.S.C. § 586.

You can send this information via email to: USTP.Bankruptcy.Fraud@usdoj.gov or by mail to:

Executive Office for U.S. Trustees
Criminal Enforcement Unit
20 Massachusetts Avenue, NW
Suite 8000
Washington, DC 20530

- Date:
- Notes:

Investment Fraud: If you believe that a thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the U.S. Securities and Exchange Commission (SEC).

www.sec.gov/complaint.shtml.

SEC Office of Investor Education and Assistance
100 F Street, NE
Washington, DC 20549

For answers to general questions, call 202-551-6551

Passport Fraud: If you've lost your passport, or it has been stolen, contact the United States Department of State (USDS).

www.travel.state.gov/passport/passport_1738.html

U.S. Department of State
Passport Services
Consular Lost/Stolen Passport Section
1111 19th Street, NW, Suite 500
Washington, DC 20036

1-877-4-USA-PPT (1-877-487-2778) TDD/TTY: 1-888-874-7793

Passport Information is available **24 hours, 7 days a week.**
Speak with a representative **Monday-Friday, 8 a.m. to 10 p.m., EST**, excluding federal holidays.

- Date:
- Notes:

Tax Fraud: If you have an unresolved issue related to identity theft, or you have suffered or are about to suffer a significant hardship as a result of the administration of the tax laws.

Internal Revenue Service (IRS) Taxpayer Advocate Service
www.irs.gov/advocate/

Toll-free: 1-877-777-4778

- Date:
- Notes:

CRIMINAL IDENTITY THEFT

Sometimes victims of identity theft learn that imposters using their name were arrested or had arrest warrants issued against them. If wrongful criminal violations are attributed to your name, contact the police department that arrested the person using your identity, or 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.

- File an impersonation report with the police department or the court. You will be asked to prove your identity. The police officer should:
 - Take your report;
 - Take your photograph;
 - Take a full set of fingerprints;
 - And make copies of your photo identification documents.
- To establish your innocence, ask the police to compare the prints and photographs with those of the imposter.
- 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 police department in the jurisdiction where the arrest warrant, traffic citation, or criminal conviction originated.
- The law enforcement agency should then recall any warrants and issue a “clearance letter” (if you were arrested). You will need to keep this document with you at all times in case you’re wrongly arrested again. Ask the law enforcement agency to file the record of the follow-up investigation establishing your innocence with the prosecutor’s office and/or court where the crime took place. This will result in an amended complaint. Once your name is recorded in a criminal database, it’s unlikely that it will be completely removed from the official record. Ask that the “primary name” be changed from your name to the imposter’s name with your name noted as an alias.
- 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. Clearing your name of wrongful criminal records can be challenging. You may need to hire a criminal defense attorney. Visit the Privacy Rights Clearinghouse for more help in clearing your name.

www.privacyrights.org

619-298-3396

TERMS YOU SHOULD KNOW:

- FCRA – Fair Credit Reporting Act
- FACTA – Fair and Accurate Credit Transaction Act
- FDCPA – Fair Debt Collections Practices Act: you can get a copy of this at www.ftc.gov
- SSN – Social Security Number
- CRAs – These are the 3 major Credit Reporting Agencies – Equifax, Experian, and TransUnion
- Fraud Alert – Federal law instructs credit issuers to contact you prior to approving an application. However, it is not widely enforced and not 100% reliable. ITRC has found fraud alerts to be about 65-70% effective. They don't affect your credit score but might slow down the credit issuing process for a thief!
- Security or Credit Freeze – With a freeze, a company may not look at your credit report for the purposes of establishing new lines of credit. Companies you already have an existing relationship with, i.e. a credit card, loan or utility service, may view your reports but only to review your credit-worthiness. Placing a freeze is a strong step to take and will affect your ability to get instant credit since it can take up to 3 days to thaw a report. However, it also locks out thieves, and that is the purpose. In those states with freezes, most laws state that victims with a police report get this service for free. Some states also allow the consumer to buy a freeze. You may thaw your freeze anytime you wish to apply for credit but you will need to plan ahead.
- Passwords – Your mother's maiden name should never be used as a password or a word that is easily known to you such as a pet's name. Use an unusual or made-up word such as "banapple." Place passwords on all bank accounts and credit cards as a proactive prevention action against account takeover.
- FTC – Federal Trade Commission: the governmental agency that oversees identity theft issues. All victims should report their cases to 877-IDTHEFT or to the website: www.consumer.gov/idtheft . The information the FTC collects is vital statistical information and they have a booklet that will also help guide you.
- EPTA – Electronic Transfer Act: provides consumer protection for all transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers.