

10. Contact The Secretary of State (SOS): Contact your local Secretary of State office to check if a duplicate license was issued in your name. If someone applied for a duplicate license, fill out the SOS's fraud report form and send in supporting documents to begin the fraud investigation process. If tickets are placed on your driving record that you did not receive, place a fraud alert on your driver's license. Contact the court where the ticket was issued to have it removed.

Documentation: *Keep a log of all conversations, including dates, times, names, and phone numbers. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.*

Resources

Credit Bureaus:

Equifax: www.equifax.com

- Report Fraud: Call (800) 525-6285
and write to: PO Box 740256, Atlanta, GA 30374
- Order a credit report: (800) 685-1111

Experian: Formerly TRW www.experian.com

- Report Fraud: Call (888) 397-3742
and write to: PO Box 2002, Allen, TX 75013
- Order a credit report: (888) 397-3742.

TransUnion: www.transunion.com

- Report Fraud: Call (800) 680-7289
and write to: PO Box 6790, Fullerton, CA 92834
- Order Credit Report: (800) 888-4213

By law, a credit bureau cannot charge more than \$9.50 per credit report. Credit Fraud victims are entitled to a free copy of their credit report.

Free Annual Credit Report:

You are entitled to one free credit disclosure in a 12 month period. To request this free credit report, visit Central Source at www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request form and mail to Annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348-5281.

Report Fraudulent Use Of Checks:

- CheckRite/Global Payments: (800) 638-4600 x555
- Tele-Check: (800) 710-9898

Social Security Administration

- Report Fraud: (800) 269-0271
- Order Earnings and Benefits Statement: (800) 772-1213

OPT OUT of Pre-Approved Credit Offers:

- Call: (888) 5OPTOUT or (888) 567-8688.
- www.optoutprescreen.com

Remove Your Name From Mail and Phone Lists:

- Direct Marketing Association
-Mail Preference Service, PO Box 9008,
Farmingdale, NY 11735
-Telephone Preference Service, PO Box 9014
Farmingdale, NY 11735

Federal Resources:

- Federal Government Agency Information Center: (800) 688-9889
- Federal Trade Commission: Call the FTC ID Theft Hotline (877) FTC-HELP for help with a consumer complaint.

State of Michigan Laws:

- Laws pertaining to Identity Theft may be referenced at www.michiganlegislature.org
- **Identity Theft Protection Act** – Act 452 of 2004
MCL 445.61 through 445.67

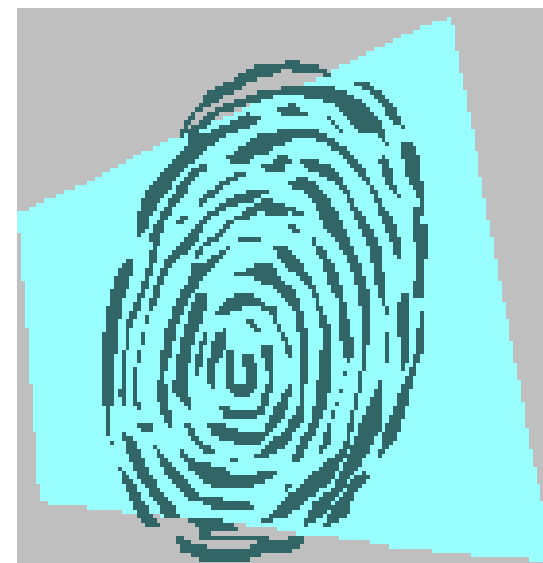
Useful Web Sites:

Michigan State Police www.michigan.gov/msp
MSP ID Theft Team www.michigan.gov/identity-theft
Federal Trade Commission (FTC): www.ftc.gov
FTC Consumer's Page: www.consumer.gov/idtheft
US Postal Service www.usps.com
Central Source www.annualcreditreport.com
Consumer Action www.consumeraction.gov

IDENTITY

THEFT

**What To Do If You're A Victim
and
Tips For Protecting Your Identity**



MICHIGAN STATE POLICE

www.michigan.gov/identity-theft

This guide provides information pertaining to the prevention of identity theft and what steps to follow if you become a victim. A victim of identity theft has the ability to assist greatly with resolving their case, through use of the enclosed information. It is important to act quickly and assertively to minimize the damage to your personal information..

WHAT IS IDENTITY THEFT?

When someone uses your identifying information (Name, Date of Birth, Social Security Number, Credit Card Numbers, etc) to obtain goods, services, credit, or open fraudulent bank accounts.

Every 79 seconds, a thief steals someone's identity, opens an account in the victim's name and goes on a spending spree.

A victim can spend anywhere from six months to two years and \$1400 recovering from identity theft.

TIPS FOR PREVENTING ID THEFT:

Never give out identifying information in response to unsolicited offers by phone, mail, internet, or in person unless you initiate the contact.

Order and review your credit report yearly.

Review financial and credit card statements monthly for unauthorized activity.

Cross shred paperwork containing personal identifiers (i.e. receipts, insurance forms, bank & credit card statements, cash advance checks) before discarding.

Protect your mail by removing it from your mailbox as soon as possible. Place your mail delivery on hold at the post office while you're away on vacation.

Be aware of where your personal identification is kept and who has access to it – at work and at home.

Protect your wallet/purse and don't leave them unattended. Limit the number of credit cards carried, and don't carry your PIN or social security card in your wallet/purse.

Treat checkbooks, ATM cards, credit cards & credit card offers as if they were cash. Cancel unneeded credit cards.

Don't put your social security number (SS#), phone number or date of birth on your checks.

When using the internet to make purchases, look for the "s" in the address (https) to ensure a secure site.

IF YOU'RE AN IDENTITY THEFT VICTIM, YOU SHOULD:

1. Contact The Credit Bureaus. Immediately call the fraud units of the three major credit reporting companies – Experian, Equifax, and Trans Union (phone numbers provided on back of pamphlet). Request that a "fraud alert" be placed on your account. Add a victim's statement to your report, i.e. "My ID has been used to apply for credit fraudulently. Contact me at (telephone number) to verify all applications." Ask how long the fraud alert will be posted on your account, and how to extend it if necessary. *Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter.* Request, in writing, to receive a free copy of your credit report every few months to monitor it. Request the names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask that all inquiries that have been generated due to the fraudulent access be removed. Request the credit bureaus to notify those who have received your credit report in the last six months (two years for employers) to alert them of the disputed and erroneous information.

2. Contact Creditors. Immediately contact, by phone and in writing, all creditors with whom accounts were created or used fraudulently. Get replacement cards with new account numbers for existing accounts that you suspect were used fraudulently. Request that old accounts be processed as "account closed at consumer's request." This is better than "card lost or stolen" which can be interpreted as blaming you for the loss. Monitor your mail and credit card bills for evidence of new activity.

Fraud Affidavit: Banks and credit grantors may ask you to complete a notarized fraud affidavit, which could become costly. The law does not require you to provide a notarized affidavit to creditors. A written statement and supporting documentation should be enough. A police report or complaint number may also be necessary.

3. File a Police Report. Report the crime to your local law enforcement agency. Provide as much documentation as possible. Get a copy of your police report and keep the report number handy to give to creditors and others who require verification. Credit card companies and banks may require you to show the report to verify the crime.

Violations of the Identity Theft Protection Act may be prosecuted in any one of the following jurisdictions:

- The jurisdiction in which the offense occurred
- The jurisdiction in which the information used to commit the violation was illegally used
- The jurisdiction in which the victim resides

4. File A Complaint With The Federal Trade Commission (FTC): Call 1-877-IDTHEFT (877-438-4338) or visit www.consumer.gov/idtheft. Consumer complaints help make the FTC database a better resource for law enforcement officers. You may download the comprehensive guide "**Take Charge: Fighting Back Against Identity Theft**" from the FTC website. The guide helps consumers guard against and recover from identity theft.

5. Contact Your Financial Institutions: Report stolen checks, stolen or compromised ATM cards or fraudulent bank accounts to the appropriate financial institution. Place a "stop payment" on outstanding checks. Close your checking and/or savings accounts and obtain new account numbers. Create new passwords avoiding common numbers and names; i.e. last 4 digits of social security number, telephone number, birth date or mother's maiden name.

6. Contact The Local Postal Inspector: Notify the local Postal Inspector if you suspect a change of address was filed with the post office or mail was used to commit fraud. Notify the local Postmaster, find out where mail is being fraudulently sent & forward all mail in your name from that address to your own address.

7. Contact The Social Security Administration(SSA): Call the Fraud Hotline at (800) 269-0271 to report the fraudulent use of your SS#. The SSA will only change your SS# as a last resort if you fit their fraud victim criteria. Order your Earnings and Benefits Statement and review it for accuracy.

8. Contact The Passport Office: Notify the Passport office in writing to watch for anyone ordering your passport fraudulently.

9. Contact Your Phone Company: Contact your phone company to report stolen calling cards, fraudulent charges and fraudulent accounts. Cancel the account and open a new one.