10. Contact The Secretary of State: Contact your local Secretary of State office to report a driver's license number being used fraudulently. Check if a duplicate license was issued in your name. Place a fraud alert on your license. Fill out the SOS's complaint form and send supporting documents to begin the fraud investigation process.

**Documentation:** <u>Keep a log</u> 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 740250, 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 1017, Allen, TX 75013

• Order a credit report: (888) 397-3742.

TransUnion: www.transunion.com

Report Fraud: (800) 680-7289
 and write to: PO Box 6790, Fullerton, CA 92834

• Order Credit Report: (800) 888-4213

Credit Fraud victims are entitled to a free copy of their credit report. By law, a credit bureau can't charge more than \$9 per credit report.

#### **Report Fraudulent Use Of Checks:**

• CheckRite/Global Payments: (800) 638-4600 x555

• Tele-Check: (800) 710-9898

To find out if the identity thief has been passing bad checks in your name, call: SCAN (800) 262-7771

#### **Report Phone Fraud:**

888-CALL-FCC (888-225-5322) <u>www.FCC.gov</u>

#### **OPT OUT of Pre-Approved Credit Offers:**

• Call: (888) 5OPTOUT or (888) 567-8688.

#### **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 Trade Commission: Call the FTC ID Theft Hotline (877) FTC-HELP (382-4357) for help with a consumer complaint.

#### **Social Security Administration**

- Report Fraud: (800) 269-0271 or report online at www.ssa.gov/oig
- Order Earnings and Benefits Statement: (800) 772-1213

#### **State of Michigan Laws**

www.michigan.gov & www.mileg.org

MCL 750.285 – Obtaining Personal Identity Information With Unlawful Intent, a 5 yr Felony

MCL 750.219e – Prohibited Conduct; Application For Loan or Extension of Credit, 4 yr Felony

MCL 257.903 - False Certification with S.O.S., a Felony

MCL 750.248(1)(2) – Forgery, 14 yr Felony MCL 750.157a – Conspiracy, a Felony

ALSO: MCL 750.219f, MCL 750.157n, MCL 750.157p, MCL 750.157q, MCL 750.157w

#### **Additional Useful Web Sites:**

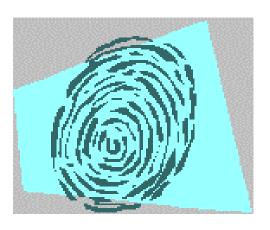
Michigan State Police <a href="www.michigan.gov/msp">www.michigan.gov/msp</a>
Federal Trade Commission (FTC): <a href="www.ftc.gov">www.ftc.gov</a>
FTC Consumer's Page: <a href="www.consumer.gov/idtheft">www.consumer.gov/idtheft</a>
US Postal Service <a href="www.usps.com">www.usps.com</a>
Id Theft Resources Center Privacy Rights Clearinghouse <a href="www.idtheftcenter.org">www.idtheftcenter.org</a>
<a href="www.michigan.gov/msp">www.ftc.gov</a>
<a href="www.michigan.gov/msp">www.ftc.gov</a>
<a href="www.michigan.gov/msp">www.ftc.gov</a>
<a href="www.michigan.gov/msp">www.ftc.gov</a>
<a href="www.michigan.gov/msp">www.ftc.gov</a>
<a href="www.michigan.gov/msp">www.ftc.gov</a>
<a href="www.michigan.gov/idtheft">www.ftc.gov</a>
<a href="www.usps.com">www.usps.com</a>
<a href="www.usps.com">www.usps.com</a>
<a href="www.idtheftcenter.org">www.idtheftcenter.org</a>
<a href="www.privacyrights.org">www.privacyrights.org</a>
<a href="www.privacyrights.org">www.privacyrights.org</a>
<a href="www.privacyrights.org">www.privacyrights.org</a>

American Expresswww10.americanexpress.comDiscoverwww.discovercard.com/discover/dataMastercardwww.mastercard.com/education/fraudVisawww.usa.visa.com/personal

# IDENTITY



## What To Do If You're A Victim & Tips For Protecting Your Identity





#### **MICHIGAN STATE POLICE**

This guide provides victims of identity theft with the major resources to contact. Victims themselves have the ability to assist greatly with resolving their case. It is important to act quickly and assertively to minimize the damage.

#### **IDENTITY THEFT:**

Unlawful use of your identifying information (Name, Date of Birth, Social Security Number, Credit Card Numbers, Etc) to obtain goods, services, credit, open fraudulent bank accounts or to facilitate other criminal activity.

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

The 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 & review your credit report yearly.

Review financial and credit card statements monthly for unauthorized activity.

Shred or tear up discarded 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, 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 <a href="mailto:and">and</a> 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 <u>notarized</u> affidavit to creditors. A written statement and supporting documentation should be enough.

3. Make a Police Report. Report the crime to the law enforcement agency with jurisdiction for your case. 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.

Some police departments have been known to resist taking reports on such crimes due to jurisdictional lines and inexperience with the Identity Theft Law. Michigan's Law, MCL 750.285, became effective on Apr. 1, 2001. Be persistent!

- 4. File A Complaint With The Federal Trade Commission (FTC): Call 1-877-IDTHEFT (877-438-4338) or visit <a href="www.consumer.gov/idtheft">www.consumer.gov/idtheft</a>. Consumer complaints help make the FTC database a better resource for law enforcement officers. You may download the comprehensive guide "ID Theft: When Bad Things Happen To Your Name" 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 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. Find out where the mail is being fraudulently sent. Notify the local Postmaster to forward all mail in your name from that address to your own address. www.usps.com/postalinspectors.
- 7. Contact The Social Security Administration: Call the Social Security Fraud Hotline 800-269-0271 to report the fraudulent use of your social security number. 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 check 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.