ID Safety
Protecting the *real* you, and *only* you.

In partnership with: INTERNATIONAL ASSOCIATION of CHIEFS OF POLICE Bank of America

MICHIGAN
IDENTITY THEFT RANKING BY STATE: Rank 15, 70.3 Complaints Per 100,000 Population, 7079 Complaints (2007)
Updated January 16, 2009

Current Laws: State law prohibits a person from using or attempting to use the personal identifying information of another person, with intent to defraud or violate the law, or by concealing, withholding or misrepresenting the person's identity, to obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment; or commit another unlawful act. This includes the personal identifying information of a deceased person. This also includes:

- Obtaining or possessing, or attempting to obtain or possess, personal identifying information of another person with the intent to use that information to commit identity theft or another crime.
- Selling or transferring, or attempting to sell or transfer, personal identifying information of another person if the person knows or has reason to know that the specific intended recipient will use, attempt to use, or further transfer the information to another person for the purpose of committing identity theft or another crime.
- Falsifying a police report of identity theft, or knowingly creating, possessing, or using a false police report of identity theft.

Violations are a felony, punishable by up to five years in prison and/or a fine up to $25,000.

"Personal identifying information" means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, Social Security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.
Statute: §445.65: http://legislature.mi.gov/doc.aspx?mcl-445-65

Jurisdiction: Identity theft may be prosecuted in the jurisdiction in which the offense occurred, the jurisdiction in which the information used to commit the violation was illegally used, or the jurisdiction in which the victim resides. If the person is charged with more than one violation of identity theft crimes and those violations may be prosecuted in more than one jurisdiction, any of those jurisdictions may be used for prosecution.
Statute: §762.10c: http://legislature.mi.gov/doc.aspx?mcl-762-10c

Statute of Limitations: Identity theft crimes can be prosecuted up to six years after the crime was committed or the identity of the thief was established.
Statute: §767.24: http://legislature.mi.gov/doc.aspx?mcl-767-24

Payment Cards: Financial transaction devices include electronic funds transfer cards, credit cards, debit cards, point-of-sale cards, and any instrument, device, card, account number, personal identification number, or code that can be used alone or in conjunction with another access device to obtain money, cash, credit, goods services, or any thing of value; certify or guarantee the availability of funds; or provide access to a deposit account. It is a felony to:

- Possess, control, or receive from another person a financial transaction device with the intent to use, deliver, circulate, or sell the device without the consent of the deviceholder.
  Statute: §750.157p: http://legislature.mi.gov/doc.aspx?mcl-750-157p
- Deliver, circulate, or sell a financial transaction device obtained or held fraudulently.
  Statute: §750.157q: http://legislature.mi.gov/doc.aspx?mcl-750-157q
- Knowingly and with intent to defraud, make, directly or indirectly, a false statement in writing regarding identity to procure the issuance of a financial transaction device.
  Statute: §750.157v: http://legislature.mi.gov/doc.aspx?mcl-750-157v

Scanning Devices: It is a misdemeanor, punishable by up to one year in jail and/or a fine up to $1000, to unlawfully use a device to capture personally identifiable information from a financial transaction device, by secretly or surreptitiously photographing, or otherwise capturing or recording, electronically or by other means. It is also a misdemeanor to distribute, disseminate, or transmit personal identifying information from a transaction that involves the use of a financial transaction device without the consent of the individual.
Statute: §750.539k: http://legislature.mi.gov/doc.aspx?mcl-750-539k

Social Security Numbers: State law prohibits retailers from requiring a customer to disclose his/her Social Security number as a condition to selling goods or providing a service, unless the transaction included an extension of credit to the consumer or the disclosure was required by state or federal law.
Statute: §445.903: http://legislature.mi.gov/doc.aspx?mcl-445-903

State law restricts the public disclosure of Social Security numbers (SSNs) in order to prevent identity theft. It prohibits businesses from publicly posting of all or more than four sequential digits of an employee's, student's, or other individual's SSN. It prevents businesses from using the complete SSN as a primary account number and from printing a SSN on any card or material mailed to an individual unless required by federal law. It also prohibits companies from requiring a consumer to transmit a SSN over the Internet, unless the connection is secure or the SSN is encrypted, and from requiring an individual to use his/her SSN to access the Web site, unless a password or unique personal identification number or other authentication device is also required to access the site.
Statute: §445.81 through 445.87:
http://legislature.mi.gov/doc.aspx?mcl-Act-454-of-2004

Disposal of Records: State law requires a person or agency that maintains a database that includes personal information regarding multiple individuals to destroy any data that contains personal information when that data is removed from the database. This includes destroying or arranging for the destruction of data by shredding, erasing, or otherwise modifying the data so that it cannot be read, deciphered, or reconstructed through generally available means.
Statute: §445.72a: http://legislature.mi.gov/doc.aspx?mcl-445-72a

Victim Assistance:

Mandatory Police Reports: Victims of identity theft are entitled to file a police report with a law enforcement agency in a jurisdiction where the alleged violation may be prosecuted, which includes the jurisdiction in which the offense occurred, in which the information used to commit the violation was illegally used, or the jurisdiction in which the victim resides. Victims are also entitled to a copy of the report from the law enforcement agency.
Statute: §780.754a: http://legislature.mi.gov/doc.aspx?mcl-780-754a

Denial of Credit: State law prohibits denying credit or public utility service or reducing a person's credit solely because a consumer was a victim of identity theft. A consumer is presumed to be a victim of identity theft if he provides a copy of a police report evidencing the claim, and either a properly completed copy of a standardized affidavit of identity theft or an affidavit of fact.
Statute: §445.71: http://legislature.mi.gov/doc.aspx?mcl-445-71

Security Breach: State government agencies and businesses operating in the state that collect and maintain computerized records containing consumers' personal information are required to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. A security breach occurs upon "unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals." After discovering or being notified of a breach of the security of the system, the database owner must disclose the breach to a resident whose unencrypted and unredacted personal information was accessed and acquired by an unauthorized person, or whose encrypted personal information was accessed and acquired by an unauthorized person with access to the encryption key. Notification is not required unless the business or agency determines that the breach has not or is not likely to cause substantial loss or injury to, or result in identity theft, to residents of the state.

Personal information means the first name or first initial and last name linked to one or more of the following data elements: Social Security number, driver license number or state personal identification card number, demand deposit or other financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

The disclosure must be made without unreasonable delay, consistent with legitimate needs of law enforcement. Notification can be provided to the affected persons by mail, e-mail, or telephone, depending on the existing relationship between the business or agency and consumer. If the cost

of providing regular notice would exceed $250,000 or the amount of people to be notified exceeds 500,000, substitute notice may be provided. When substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the entity's web site, and notification to major statewide media. The consumer reporting agencies must also be notified when the breach is disclosed to more than 1,000 people at a time
Statute: §445.72: http://legislature.mi.gov/doc.aspx?mcl-445-72

State Resources:

Office of the Attorney General, "Identity Theft Information for Michigan Consumers" (http://www.michigan.gov/ag/0,1607,7-164-34739_17343_18163-80479--,00.html)

"Information of Victims of Theft" (http://www.michigan.gov/ag/0,1607,7-164-34739_17343_18163-80479--,00.html#InformationForVictims)
This document directs victims to: "*Immediately file a report with either your local police department or the police where the identity theft occurred. Victims should keep a copy of the police report for their records. Credit card companies and financial institutions may require a victim to show a copy of the report to verify the crime*."

"Protecting Your Social Security Number" (http://www.michigan.gov/ag/0,1607,7-164-34739_20942-103001--,00.html)

"Security Freeze Information for Michigan Consumers (http://www.michigan.gov/ag/0,1607,7-164-17337_17291-182414--,00.html)
This site gives information to consumers about the availability of security freezes.

Michigan State Police, "Identity Theft: What to Do if You're a Victim and Tips for Protecting Your Identity" (http://www.michigan.gov/documents/ID_Theft_94764_7.pdf)
This pamphlet directs victims to: "***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*."

Department of Information Technology, "Protecting Your Computer and Your Identity" (http://www.michigan.gov/documents/cybersecurity/Protect_Your_Computer_and_Your_Identity_209955_7.pdf)
This publication contains information on identity theft, phishing, pharming, and other Internet scams.

Legislation:

2007:
Lawmakers passed several bills (**SB 298, SB 299, SB 301, HB 4517,** and **HB 4519**) to protect personal information and prevent identity theft by authorizing the registers of deeds to obscure or remove Social Security numbers (SSNs) that appear in copies of records. The bills also require the registers to reject new documents that contain SSNs and allow individuals to request that their SSNs in recorded documents be removed or obscured.

2006:
SB 309 requires that Michigan residents be notified if the security of a database containing their personal information is breached. Businesses and government agencies must notify consumers when a security breach puts personal information, including Social Security numbers, driver's license numbers, and financial information, at risk. Failure to properly notify consumers of a security breach can result in a fine of up to $750,000.

The bill also requires a person or agency that maintains a database that includes personal information regarding multiple individuals to destroy any data that contains personal information when that data is removed from the database. This includes destroying or arranging for the destruction of data by shredding, erasing, or otherwise modifying the data so that it cannot be read, deciphered, or reconstructed through generally available means.

2004:
Lawmakers passed a package of bills designed to better protect consumers from identity theft:

- **SB 792** makes it a felony to use a person's identity information without their consent, with violations punishable by up to five years in jail and/or a $25,000 fine. The bill also prohibits the denial of credit because the consumer was a victim of identity theft, and allows victims to get a certificate from a county prosecutor stating they have been the victims of identity theft.
- **SB 793** clarifies the jurisdiction in which identity theft can be prosecuted. The bill allows the prosecution of offenders in the jurisdiction in which the offense occurred; the jurisdiction in which the information used to commit the violation was illegal used; or the jurisdiction in which the victim resides.
- **SB 220** prohibits retailers from displaying more than the last four digits of a credit card account number on a sales receipt or mailing.
- **SB 657** prohibits retailers from requiring a customer to disclose his/her Social Security number as a condition to selling goods or providing a service, unless the transaction included an extension of credit to the consumer or the disclosure was required by state or federal law.
- **SB 795** prohibits employers and schools from printing Social Security numbers on an ID badge or card or using the number as an account number.
- **SB 798** prohibits the denial of consumer credit to victims of identity theft.
- **SB 1384** establishes the right of victims of identity theft to obtain a police report. Often, victims have difficulty obtaining a report because police officers are uncertain of jurisdictional issues.
- **HB 6169** establishes the sentencing guidelines for the crime of identity theft. The bill increases the maximum fine for stealing someone's identity from $10,000 to $25,000, but the maximum prison sentence remains at five years.

- **HB 6172** extends the statute of limitations for identity theft cases to six years after the crime was committed or the identity of the thief was established.
- **HB 6174** adds identity theft as an unlawful practice of trade or commerce to the Michigan Consumer Protection Act, which allows victims to bring private actions.
- **HB 6177** prohibits and creates penalties for photographing, recording, or electronically transmitting personal identifying information taken, without consent, from credit, debit, or ATM cards.