

WISCONSIN

IDENTITY THEFT RANKING BY STATE: Rank 15, 175.9 Complaints Per 100,000
Population, 9852 Complaints (2007)
Updated January 16, 2009

Current Laws: It is unlawful to intentionally use or attempt to use any personal identifying information or personal identification documents of an individual without that individual's consent; by representing that he/she is the individual; acting with the authorization or consent of the individual; or that the information or document belongs to him/her in order to:

- Obtain credit, money, goods, services, employment, or any other thing of value or benefit.
- Avoid civil or criminal process or penalty.
- Harm the reputation, property, person or estate of the individual.

Violations are a class H felony, punishable by up to six years in prison and a \$10,000 fine.

Personal identifying information includes any of the following: an individual's name, address or telephone number; driver's license number; Social Security number; employer, employee number, or place of employment; taxpayer ID number; DNA profile; mother's maiden name; depository account number, credit card number, ATM card password, telephone service identifier, or any other account number, password or electronic identifier that can be used to obtain money, goods, services, an account transfer, or anything else of value or benefit; or fingerprint, voiceprint, retina iris image, or any other unique physical characteristic.

A personal identification document includes any of the following: a document containing personal identifying information; an individual's card or plate, if it can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value or benefit, or if it can be used to initiate a transfer of funds; or any other device that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled.

Statute: §943.201:

<http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=stats&jd=943.201>

It is also a class H felony to use an identification document or identifying information of an entity, such as a business, charity, union, or any other organization, without its consent, to obtain credit, money, goods, services, employment, or any other thing of value or benefit; or to harm the reputation, property, person, or estate of the entity.

Statute: §943.203:

<http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=stats&jd=943.203>

Payment Cards: It is unlawful for any person to:

- Obtain a financial transaction card, such as a credit card or debit card, from another without the cardholder's consent.
- Knowingly make a false statement respecting his/her identity for the purpose of procuring the issuance of a financial transaction card.
- Receive an illegally obtained financial transaction card with intent to use it or sell it or transfer it to another person. If a person possesses financial transaction cards issued in the names of two or more other persons, it is prima facie evidence the person acquired them in violation of this law.
- Receive a financial transaction card that the person knows to have been lost, stolen, or delivered by mistake to the wrong cardholder, and retain possession of the card with intent to use it, sell it, or transfer it to another person other than the issuer or cardholder. Possession of such a card for more than seven days is prima facie evidence that this law has been violated.
- Sell a financial transaction card other than the user.
- Buy a financial transaction card other than from the issuer.
- Obtain control over a financial transaction card as security for a debt with intent to defraud the issuer or any other person.
- Receive a financial transaction card issued in the name of another person which he or she has reason to know was obtained in violation of this law.

Violations are a Class A misdemeanor, punishable by up to nine months in jail and/or a fine up to \$10,000. However, a person who receives a financial transaction card issued in the name of another person that he or she has reason to know was obtained illegally is guilty of a class I felony, punishable by up to three years and six months in prison and/or a \$10,000 fine.

Statute: §943.41:

<http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=stats&jd=943.41>

It is illegal for a person, with intent to defraud the issuer, a person or organization providing money, goods, services or anything else of value, or any other person to:

- Use a financial transaction card obtained fraudulently, or which the person knows is forged, expired, or revoked
- Represent without the consent of the cardholder that the person is the holder of a specified card.

Violations are a Class A misdemeanor if the value of the money, goods, services or property illegally obtained does not exceed \$2500. If the value is between \$2500 and \$5000 in a single transaction or within six months, it is a Class I felony. If the value is between \$5000 and \$10,000, it is a class H felony, and a Class G felony (punishable by up to ten years in prison and/or up to a \$25,000 fine) if it is over \$10,000.

Any person who represents that he or she is a financial or representative of a financial institution for the purpose of obtaining or recording a person's personal identifying information is guilty of a Class H felony, including up to six years in jail and a \$10,000 fine.

Statute: §943.82:

<http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=stats&jd=943.82>

Victim Assistance:

Mandatory Police Reports: Law enforcement agencies are required to take a police report from people in their jurisdiction who believe that their personal identifying information or a personal identification document is in the possession of another person, or has been used or attempted to be used. If a law enforcement agency concludes that it does not have jurisdiction to investigate the violation, it must inform the individual which law enforcement agency may have jurisdiction. The officer must give a copy of the report to the individual who has made the request.

Statute: §943.201:

<http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=stats&jd=943.201>

Security Freeze: All Wisconsin consumers are allowed to place security freezes on their consumer credit reports to prevent others from opening new accounts in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information. To request a freeze, an identity theft victim must request one in writing by certified mail to the credit reporting agencies. Credit reporting agencies may charge \$10 for each security freeze, removal of a security freeze, or temporary lifting of a freeze for a period of time. However, victims of identity theft with a valid police report may not be charged.

The reporting agency must place the freeze within five business days after receiving the request, and within ten days must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time.

Requests for a temporary unlocking of the freeze must be completed within three business days.

Statute: §100.54:

<http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=stats&jd=100.54>

“Wisconsin Consumers Have the Right to Obtain a Security Freeze”:

<http://www.privacy.wi.gov/securityfreeze/pdf/IDTheftSecurityFreeze631.pdf>

How to Place a Security Freeze in Wisconsin:

<http://www.consumersunion.org/pdf/security/securityWI.pdf>

Security Breach: State law requires businesses operating in the state and state and local government agencies that maintain or license computerized data that include consumers’ personal information to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. The law requires the business or governmental entity to notify an individual whenever personal information held by the business or governmental entity is acquired by an unauthorized person. However, no notice is required if the unauthorized acquisition does not create a material risk of identity theft or fraud, or if the information was acquired in good faith by an employee or agent and is used for a lawful purpose of the entity.

Consumers must be notified within a reasonable time, not to exceed 45 days after the entity learns of the unauthorized acquisition, but notification can be delayed at the request of law enforcement. The notice must be provided by a mail or by a method that the entity has

previously used to communicate with the subject of the information. Upon written request of the person whose information was acquired, the entity must also identify the nature of the personal information acquired. If an entity cannot determine the mailing address of the person whose information was acquired, and if the entity has not previously communicated with that person, it must give notice in a manner that is reasonably calculated to provide notice. Such methods might include notice in the newspaper or on television or radio. In addition, if the breach affects more than 1000 people, the consumer reporting agencies must also be notified.

Personal information means an individual's first name or first initial and his/her last name, in combination with and linked to any one or more of the following data elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: Social Security number; driver's license or Wisconsin identification card number; a financial account number, credit or debit card number, or any security code, access code, or password that would permit access to the individual's financial account; DNA profile; or unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Statute: §134.98:

<http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=stats&jd=134.98>

“Wisconsin's Data Breach Notification Law”

(http://www.privacy.wi.gov/factsheets/notification_law.jsp)

State Resources:

Office of Privacy Protection: <http://www.privacy.wi.gov/>

The Office of Privacy Protection has a number of useful fact sheets available on its website, including the ones listed below: (<http://www.privacy.wi.gov/factsheets/factsheets.jsp>)

“Identity Theft: The Basics of Safeguarding Your Information”

(http://www.privacy.wi.gov/factsheets/safeguarding_info.jsp)

What To Do If It Happens To You” (http://www.privacy.wi.gov/factsheets/what_to_do.jsp)

This fact sheet directs victims to: *“Report the theft to the police. Under Wisconsin law, your local police department is obligated to prepare a report of identity theft even if the theft might have occurred at some other place. The police are also required to give you a copy of the report if you request it. You should request a copy since you will need it when dealing with your financial institution, credit card issuers, and others. Also, if you request a “freeze” on your credit report and send a copy of the report to the credit reporting agency, you do not have to pay the \$10 fee.”*

It also directs victims to file an identity theft complaint with the Office of Privacy Protection:

“The Wisconsin Office of Privacy Protection wants to hear from you if your identity has been stolen. Your complaint will assist us in knowing specifically where and how identity thieves are operating in Wisconsin and share that information with other law enforcement agencies. In addition, the Office of Privacy Protection will use the information you provide to try and track

down identity thieves and prosecute them. You can file an identity theft complaint by calling and requesting a complaint form at 800-422-7128 or obtain one online at www.privacy.wi.gov.”

It also provides instructions on what to do if you are accused of a crime committed in your name: *“If someone commits a crime in your name or gives your name to the police when arrested and then disappears, the police might come to you thinking you’re the wrongdoer. Explain to the police that your identity has been stolen and provide the police with a copy of the police report you filed as well as the identity theft complaint you filed with the Wisconsin Office of Privacy Protection. Ask those questioning you to contact the Office of Privacy Protection and the police where you filed a police report for additional information and verification.”*

“How Law Enforcement Can Help a Victim of Identity Theft”

(http://www.privacy.wi.gov/law_enforcement/law_enforcement.jsp)

This document provides a list of steps that law enforcement can do to assist victims of identity theft. This includes taking a written report, collecting and preserving any evidence supplied by the victim, providing a copy of the official police report to the victim, and informing them on how to close accounts and obtain a fraud alert. It also suggests providing victims with a copy of “Identity Theft – What to Do If It Happen to You”

(http://www.privacy.wi.gov/factsheets/what_to_do.jsp).

In addition, it requests that law enforcement officers share identity theft complaints with the Office of Privacy Protection, to assist other law enforcement officials track down identity thefts. The Office also provides law enforcement with investigative assistance and helps victims resolve financial issues resulting from identity theft.

“Requesting Information of Fraudulent Accounts – A Guide for Identity Theft Victims”

(<http://www.privacy.wi.gov/factsheets/pdf/IDTheftFraudulentAcctInfo616.pdf>)

“Federal law gives an identity theft victim an important right. This is the right to get copies of documents relating to fraudulent transactions made or accounts opened using the victim’s personal information. The information can help law enforcement investigate the crime and can prevent repeated violations. You may use the form provided with this Information Sheet to ask creditors or other businesses to give you copies of applications and other business records relating to transactions or accounts that resulted from the theft of your identity. When you file your police report of identity theft, the officer may give you a form to use to request information from creditors or other businesses. If the officer does not do this, you may use the form provided here. After you receive the documents from the business, give copies to the officer investigating your case.”

Office of the Attorney General, “Minimizing Identity Theft”

(http://www.doj.state.wi.us/dls/ConsProt/cp_identitytheft.asp)

This site directs victims to *“Contact the Police. File a police report with your local police or wherever the identity theft took place. Get a copy of the report to show to creditors and financial institutions.”*

“Identity Theft Brochure” (http://www.doj.state.wi.us/docs/ID_theft_broc.pdf)

Legislation:

2006:

AB 912 allows consumers to place security freezes on their consumer credit reports to prevent identity thieves from opening new accounts in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information.

SB 164 requires businesses operating in the state and state and local government agencies that collect and maintain computerized records containing consumer's personal information to notify affected consumers in the event that personal data is compromised. Consumers must be notified within a reasonable time, not to exceed 45 days after the entity learns of the unauthorized acquisition, but notification can be delayed at the request of law enforcement.

2003:

AB 288 seeks to crack down on identity theft by redefining "personal identification documents" to cover any document containing personal identifying information, including a credit card. It also now includes DNA profiles, fingerprints, voice prints and retina images. Previous law defined a personal identification document as a birth certificate or a financial transaction card as well as information such as name, address, phone number, driver's license number, Social Security number and checking or savings account number. The bill also expands the crime of identity theft to stealing a dead person's identity and using an identity to hurt a person's reputation or to avoid a criminal or civil process.

In addition, the bill:

- Requires a law enforcement agency to prepare a report if a person who resides in the agency's jurisdiction reports an identity theft violation.
- Prohibits the unauthorized use of identifying information relating to businesses or government.
- Makes the use of a false statement or false identification in connection with a transaction with a financial institution a felony.
- Allows a person to get service from a public utility if the only reason the person cannot get it is because of identity theft.