

MINNESOTA

IDENTITY THEFT RANKING BY STATE: Rank 35, 55.0 Complaints Per 100,000
Population, 2857 Complaints (2007)
Updated June 8, 2008

Current Laws: It is a crime for a person to transfer, possess, or use an identity that is not the person’s own, with the intent to commit, aid, or abet any unlawful activity. Unlawful activities include any felony violations and lesser offenses involving theft, forgery, fraud, or misrepresentation to a public official. An unlawful activity is not limited to illegal acts for financial gain.

“Identity” is defined as any name, number, or data transmission that may be used, alone or in conjunction with any other information, to identify a specific individual, including:

- Name, Social Security number, date of birth, driver’s license, passport, employer or taxpayer identification number;
- Unique electronic identification number, address, account number, or routing code; or
- Telecommunication identification information or access device.

Identity theft penalties vary and are tied to the resulting loss or harm involved. The offense level correlates with the amount of loss incurred, the number of direct victims involved, or the related offense. The value of the money or property, as well as the number of direct or indirect victims, may be aggregated within any six-month period. Loss is defined as the value obtained and the expenses incurred as a result of the crime.

Identity Theft Penalties			
Number of Direct Victims	Combined Loss to Direct & Indirect Victims/or Crime Involved	Penalty – Maximum Term of Imprisonment/Fine	Offense Level
1	\$250 or less	90 days/\$1,000	Misdemeanor
1	\$251 to \$500	1 year/\$3,000	Gross misdemeanor
1	\$501 to \$2,500	5 years/\$10,000	Felony
1	\$2,501 to \$35,000	10 years/\$20,000	Felony
1	More than \$35,000	20 years/\$100,000	Felony
1+	Possession or distribution of pornographic work involving minors	20 years/\$100,000	Felony
2 or 3	Any amount	5 years/\$10,000	Felony
4 to 7	Any amount	10 years/\$20,000	Felony
8+	Any amount	20 years/\$100,000	Felony

Statute: §609.527:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=609.527

Phishing: State law criminalizes the electronic use of a false pretense to obtain another's identity, often referred to as "phishing." "False pretense" is defined as "any false, fictitious, misleading, or fraudulent information or pretense or pretext depicting or including or deceptively similar to the name, logo, Web site address, e-mail address, postal address, telephone number, or any other identifying information of a business or organization or of a governmental agency, to which the user has no legitimate claim of right." A crime is committed even if a person does not obtain or use another's identity. It is not a defense that the violator did not obtain personal information from another person, or that the crime did not result in loss to another. Phishing is a felony, punishable by up to five years in prison and/or a \$10,000 fine.

Statute: §609.527:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=609.527

Jurisdiction: Identity theft crimes may be prosecuted in either the county where the offense occurred, or the county of residence or place of business of the victim. If the same person commits two or more offenses in two or more counties, he may be prosecuted for all the offenses in any of the counties where an offense occurred.

Statute: § 628.26:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP&year=2006§ion=628#stat.628.26.0

For phishing offenses, the venue is also located in the county of residence of the person whose identity was obtained or sought. In a phishing scheme, a person's identity might not be taken; it is the scheme to deceive a person into revealing personal information that is prosecuted.

Statute: §609.527:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=609.527

Statute of Limitations: The limitations period for prosecuting identity theft and phishing is three years from the commission of the offense, excluding any period of time during which the defendant does not reside in Minnesota.

Statute: § 628.26:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP&year=2006§ion=628#stat.628.26.0

Driver's Licenses and Identification Cards: It is a crime to control, possess, or use equipment or software designed to generate fraudulent drivers' licenses and identification cards with the intent to manufacture, sell, issue, publish, or pass more than one fraudulent license or card. It is also a crime to manufacture or possess more than one fraudulent driver's license or identification card with intent to sell. A first time offense under this section is a gross misdemeanor. A subsequent offense is a five-year felony offense subject to a \$10,000 fine.

Statute: §609.652:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=609.652

Payment Cards: A person commits financial transaction fraud if he:

- Without the consent of the cardholder, and knowing that the cardholder has not given consent, uses or attempts to use a card to obtain the property of another, or a public assistance benefit issued for the use of another;
- Uses or attempts to use a card knowing it to be forged, false, fictitious, or obtained in fraudulently;
- Without the consent of the cardholder and knowing that the cardholder has not given consent, falsely alters, makes, or signs any written document pertaining to a card transaction to obtain or attempt to obtain the property of another; or
- Upon applying for a financial transaction card to an issuer, or for a public assistance benefit which is distributed by means of a financial transaction card, knowingly gives a false name or occupation; knowingly and substantially overvalues assets or substantially undervalues indebtedness for the purpose of inducing the issuer to issue a financial transaction card; or knowingly makes a false statement or representation for the purpose of inducing an issuer to issue a financial transaction card used to obtain a public assistance benefit.

Violations for these offenses are punished based on the value of the property the person obtained or attempted to obtain. The value of the transactions made or attempted within any six-month period may be aggregated and the defendant charged accordingly. When two or more offenses are committed by the same person in two or more counties, the accused may be prosecuted in any county in which one of the card transactions occurred for all of the transactions aggregated.

Value of Property Obtained or Attempted to Be Obtained	Penalty – Maximum Term of Imprisonment/Fine
\$250 or less	1 year/\$3,000
\$250 or less with a previous felony or gross misdemeanor conviction in the last five years for robbery, theft, forgery offenses	5 years/\$10,000
\$250 to \$2,500	5 years/\$10,000
\$2,501 to \$35,000	10 years/\$20,000
More than \$35,000	20 years/\$100,000

- Sells or transfers a card knowing that the cardholder and issuer have not authorized the person to whom the card is sold or transferred to use the card, or that the card is forged, false, fictitious, or was obtained fraudulently.
- Without a legitimate business purpose, and without the consent of the cardholders, receives or possesses, with intent to use, or with intent to sell or transfer two or more cards issued in the name of another, or two or more cards knowing the cards to be forged, false, fictitious, or obtained fraudulently.

These violations are punishable by up to three years in prison and/or a fine up to \$5000.

Statute: §609.821:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=609.821

State law prohibits merchants from retaining specific information drawn from the magnetic stripe of a credit or debit card, including the personal identification number or access code, after completion of a transaction. For debit card transactions, merchants would be prohibited from storing such information for longer than 48 hours after completion of a transaction. If the merchant violates these anti-storage prohibitions, a bank would have standing to sue the merchant to recover “the cost of reasonable actions undertaken” to respond to any security breach, including the costs of cancelling and reissuing credit cards, closing and/or reopening accounts, stop-payment actions, unauthorized transaction reimbursements, and the providing of breach notification to account holders.

Statute: §325E.64:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=current§ion=325e.64

Social Security Numbers: State law places limits on the use and dissemination of Social Security numbers (SSNs). The law prohibits a person or an entity (excluding government entities but including Minnesota state colleges and universities) from:

- Publicly posting or publicly displaying, defined as intentionally communicating or otherwise making available to the general public, in any manner an individual’s SSN;
- Printing an individual’s SSN on any card required to access products or services provided by the person or business;
- Requiring an individual to transmit his SSN over the Internet, unless the connection is secure or the Social Security number is encrypted;
- Requiring an individual to use his SSN to access an Internet website, unless a password or unique personal identification number or other authentication device is also required.
- Printing an individual’s SSN on any materials that are mailed to the individual, unless state or federal law requires the number to be on the document to be mailed.
- Assigning or using a number as the primary account identifier that is identical to or incorporates an individual’s complete SSN;
- Selling SSNs obtained from individuals in the courts of business.
- Restricting access to individual SSNs it holds so that only employees who require the numbers in order to perform their job duties have access to the numbers.

However, if a business or government agency has previously used an individual’s SSN in a manner inconsistent with these provisions prior to July 1, 2007, it may continue using the SSN if the following conditions are met:

- The use of the SSN must be continuous. If its use is stopped for any reason, the provisions will apply.
- The individual is provided an annual disclosure that informs him/her that he/she has the right to stop the use of his or her Social Security number in a manner prohibited by the law.

- A written request by an individual to stop the use of his or her Social Security number is implemented within 30 days of the receipt of the request. There may not be a fee or charge for implementing the request.
- The business does not deny services to an individual because the individual makes a written request pursuant to this subsection.

Statute: §325E.59:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP&year=2006§ion=325E#stat.325E.59.0

Victim Assistance:

Restitution: Identity theft victims are entitled to a mandatory restitution payment of at least \$1000. Mandatory restitution allows victims to seek compensation from a defendant without providing detailed documentation of losses incurred. This addresses the problem that victims may have in accounting for intangible losses and expenses involved in clearing their records, such as filling out paperwork and making phone calls.

Statute: §609.527:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=609.527

Mandatory Police Reports: A person who has learned or reasonably suspects that he/she is a victim of identity theft may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction where the person resides, regardless of where the crime may have occurred. The agency must prepare a police report of the matter, provide the complainant with a copy of that report, and may begin an investigation of the facts, or, if the suspected crime was committed in a different jurisdiction, refer the matter to the law enforcement agency where the suspected crime was committed for an investigation of the facts. If a law enforcement agency refers a report to the law enforcement agency where the crime was committed, it need not include the report as a crime committed in its jurisdiction for purposes of information that the agency is required to provide to the commissioner of public safety.

Statute: §609.527:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=609.527

Court Documents: Victims are also entitled to free certified court documents, including copies of the complaint, the judgment of conviction, and the order setting forth the facts of the case, upon written request.

Statute: §609.527:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=609.527

Criminal History Records: If a person's identity is stolen and used by a thief to avoid prosecution, the victim's criminal history record may incorrectly reflect crimes committed by the identity thief. If an individual believes that his or her criminal history record is inaccurate or incomplete, the individual may notify the Bureau of Criminal Apprehension in writing and seek a correction. Upon receiving notice, the Bureau has 30 days to correct the data or notify the

individual that the authority believes the information to be correct. Data that is successfully challenged must be completed, corrected, or destroyed by the agency that holds the data.

Statute: §13.04:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=13.04

Security Breach: State law requires any person or business that conducts business in the state and that owns or licenses data that includes personal information to disclose any breach of the security of the system to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

A security breach occurs upon “unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity” of personal information maintained by the person or business. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

Personal information means an individual’s first name or first initial and last name, in combination with any one or more of the following data elements, when the data elements is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired: Social Security number; driver’s license or Minnesota identification card number; or an account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual’s financial account. Publicly available information is not included.

Notification can be provided to the affected persons by mail or e-mail. If the cost of providing regular notice would exceed \$250,000, the amount of people to be notified exceeds 500,000, or the entity or business not have sufficient contact information, 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. In addition, if more than 500 people are to be notified, the national consumer reporting agencies must also be notified within 48 hours.

Statute: §325E.61:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=325E.61

Starting August 1, 2008, certain retailers and other merchants will be liable to banks for costs associated with data breaches, including consumer notification and card replacement. This liability applies to entities that do not meet strict security standards regarding the amount of time they are allowed to retain information from credit or debit cards after transactions.

Statute: §325E.64:

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=current§ion=325e.64

Credit Freeze: All Minnesota consumers are allowed to place security freezes on their consumer credit reports to prevent new accounts from being opened 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, a consumer must request one in writing by certified mail; by telephone; or directly to the consumer reporting agency through a secure electronic mail connection if the connection is made available by the consumer reporting agency. Consumer reporting agencies may charge a fee of \$5 to place or temporarily lift a security freeze. However, victims of identity theft with a valid police report may not be charged.

The reporting agency must place the freeze within three 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: §13C.016:

<http://www.revisor.leg.state.mn.us/bin/getpub.php?type=s&num=13C.016&year=2006>

How to Place a Security Freeze: www.consumersunion.org/pdf/security/securityMN.pdf

Minnesota Identity Theft Freeze Law:

<http://www.ag.state.mn.us/Brochures/pubSecurityFreezeLaw.pdf>

State Resources:

Office of the Attorney General: “Guarding Your Privacy”

(<http://www.ag.state.mn.us/Consumer/Privacy/GuardingYPrivacy/Default.asp>)

This comprehensive document includes tips on preventing identity theft, and a checklist of actions that victims of identity theft should take.

- “What is Personal Information and Identity Theft”
(http://www.ag.state.mn.us/Consumer/Privacy/GuardingYPrivacy/GYP_1.asp)
- “A Look at Identity Thieves and How to Lessen Your Risk of Being a Victim”
(http://www.ag.state.mn.us/Consumer/Privacy/GuardingYPrivacy/GYP_2.asp)
- “What to Do If You’re a Victim”
(http://www.ag.state.mn.us/Consumer/Privacy/GuardingYPrivacy/GYP_3.asp)

This document directs victims to: *“Report the crime to your local police or sheriff as soon as you are aware of the theft. Be sure to file a report with your local police or sheriff’s department. For your records, keep a copy of the incident reports you filed. A law enforcement record of the incident is important because it will allow you to present your creditors and banks with proof of the crime.”*

The Office of the Attorney General has produced several publications related to identity theft, including:

- “Minnesota Identity Theft Freeze Law”
(<https://www.ag.state.mn.us/Brochures/pubSecurityFreezeLaw.pdf>)
- “Tips to Businesses on Identity Theft”
(<https://www.ag.state.mn.us/Brochures/pubIDTheftAndBusiness.pdf>)

- “Beware of Phishing” (<https://www.ag.state.mn.us/Brochures/pubBewareOfPhishing.pdf>)
- “Beware of Phishing: Protect Your Computer” (<http://www.ag.state.mn.us/Brochures/pubBewarePhishingProtectYourComputer.pdf>)
- “Identity Theft on Campus” (<http://www.ag.state.mn.us/Brochures/pubIdentityTheftOnCampus.pdf>)
- “Credit Reports” (<https://www.ag.state.mn.us/Brochures/pubCreditReports.pdf>)
- “Know the FACT Act on Consumer Reporting” (<https://www.ag.state.mn.us/Brochures/pubKnowTheFACTAct.pdf>)

Department of Public Safety, “Identity Theft” (<http://www.dps.state.mn.us/dvs/DriverLicense/DL%20Info/idTheft.htm>)

“Confirmation of Identity: Driving Red Flag” (<http://www.dps.state.mn.us/dvs/PDFForms/DL%20Forms/VictimofIdentityTheft.pdf>)
“Upon receipt of this completed form, we will make an entry on a your driving record. This “flag” will alert law enforcement officers that someone else may be using your identity. It should prevent someone else from successfully using your name when dealing with law enforcement personnel.”

Legislation:

2007:

With the passage of **HF 1758**, Minnesota became the first state to pass legislation that will make retailers and other merchants liable to banks for costs associated with data breaches, including consumer notification and card replacement. The bill also prohibits merchants from retaining specific information drawn from the magnetic stripe of a credit or debit card, including the personal identification number or access code, after completion of a transaction. For debit card transactions, merchants would be prohibited from storing such information for longer than 48 hours after completion of a transaction. If the merchant violates this anti-storage prohibition, a bank would have standing to sue the merchant to recover “the cost of reasonable actions undertaken” to respond to the breach, including the costs of cancelling and reissuing credit cards, closing and/or reopening accounts, stop-payment actions, unauthorized transaction reimbursements, and the providing of breach notification to account holders. The prohibition on storing information took effect on August 1, 2007, while the liability provisions take effect on August 1, 2008.

2006:

SF 2002 is designed to help consumers prevent identity theft. The bill allows consumers to freeze their credit reports to prevent any unauthorized release of personal information. People who request a freeze could allow the report to be released to a specific person or business so that credit reports could be checked for legitimate purchases. It also allows victims to request a quick judicial ruling to clear their name if someone has been someone has been arrested or convicted for the theft, and used their identity.

The bill also removes two key exemptions from the security breach notification law passed in 2005 (HF 2121). As passed by the legislature, the 2005 law exempted health care companies and financial services firms from the requirement that they disclose security breaches to customers whose personal information might be compromised.

SF 3132 expands the existing restrictions on the use of Social Security numbers (SSNs) by prohibiting individuals and entities (excluding governmental entities) from assigning or using a number as the primary account identifier that is identical to or incorporates an individual's complete SSN and from selling SSNs obtained from individuals in the course of business. It also requires that entities restrict access to individual Social Security numbers it holds so that only employees who require the numbers in order to perform their job duties have access to the numbers.

2005:

HF 2121 requires businesses to notify individuals when a security breach causes their personal information to be released to unauthorized parties. It affects companies that electronically store unencrypted personal information, such as customer names, along with their credit card, bank account or Social Security numbers. Companies can provide written or electronic notice, including e-mail, "conspicuous" Web page posting, or major statewide media to provide notice in certain circumstances. Those methods of notice can be utilized if notice would cost more than \$250,000 or if more than 500,000 people are affected. The bill contains the caveat that notification can be delayed if law enforcement determines that the disclosure would impede a criminal investigation.

Exempted from the law are financial institutions, including banks, savings and loans, and other financial institutions covered under federal banking regulations, and health clinics, including hospitals and medical providers. Opponents argued that federal banking regulations are defined so broadly that few businesses would actually fall under the state law, and that federal regulations do not require hospitals to disclose security breaches.

SF 336 creates a new crime that prohibits a person, with intent to obtain another's identity from using pretense in an e-mail, Web page, or other Internet communication. Commonly known as "phishing," the crime will be punishable by up to five years in prison and/or a \$10,000 fine. It is not a defense that the violator did not obtain personal information from another person, or that the crime did not result in loss to another. The venue for prosecution of phishing is expanded to the county of residence of the person whose identity was obtained or sought.

In addition, the bill states that victims of identity theft will be entitled to a minimum of \$1,000 in restitution from the offender and to free copies of court documents needed to repair their credit record.

The bill also increased penalties for identity theft, expanding the 20-year felony to include offenses related to possession or distribution of pornographic work involving minors.

HF 225 restricts the use of Social Security numbers. It prevents businesses from printing a customer's Social Security number on a card. In addition, companies cannot require a customer to transmit a Social Security number over the Internet unless the site is secure or the number is encrypted. Customers can only be required to use their Social Security number to access a site if a personal identification number or authentication device is also required.

2003:

SF 980 seeks to make it easier to prosecute for identity theft. The bill:

- Adds another level of offense for those who commit identity theft, victimizing eight or more parties or causing a combined loss of more than \$35,000. The penalty is a 20-year felony sentence and fine up to \$100,000.
- Directs the Sentencing Guidelines Commission to amend the sentencing guidelines by adding the use of another's identity in the commission of a crime to the list of aggravating factors a court may consider in sentencing.
- Permits victims of identity theft to report the crime to law enforcement where they live, regardless of where the crime occurred. Some agencies refused to accept reports of theft when it occurred elsewhere. Prosecutors can file charges for identity theft either in the county where the offense occurs or where the victim resides or does business.
- Allows identity theft offenses occurring within any six-month period to be aggregated, and may be prosecuted in any county in which one of the offenses occurred.
- Creates a new mail theft felony for stealing or opening mail addressed to someone else, with a penalty up to three years in prison and fine up to \$5,000. While already a federal crime, federal courts and prosecutors do not have resources to deal with most mail crimes. Now state prosecutors can file mail theft charges in the county where the theft occurred or where the victim lives or works.