INFORMATION BRIEF
Research Department
Minnesota House of Representatives
600 State Office Building
St. Paul, MN 55155

Rebecca Pirius, Legislative Analyst
651-296-5044
Updated: October 2007

Identity Theft and Related Crimes
An Overview of Minnesota Criminal Law

In 1999, Minnesota first enacted legislation specifically targeted at the burgeoning crime of identity theft. As identity theft has become more prevalent and sophisticated, the legislature has augmented various provisions intended to advance the prosecution of these offenses, aid identity theft victims, and prevent identity theft.

This information brief summarizes Minnesota's criminal identity theft law. Because identity theft is not generally an isolated crime, the brief reviews a selection of related criminal statutes. It also provides a historical summary of identity theft legislation, highlights sentencing guideline provisions, and references federal criminal statutes. Unless otherwise noted, all of the statutory citations are to Minnesota Statutes, as amended through the 2007 Regular Session.

Contents

Overview of Identity Theft

A 2003 Federal Trade Commission survey estimated that, over the course of a year, nearly ten million Americans were victims of identity theft with losses totaling almost $53 billion ($48 billion to businesses and $5 billion to individuals).[1] As one of the fastest growing crimes in the country, identity theft takes on many forms: financial theft, nonfinancial theft, account takeover theft, true party theft, reverse record identity theft, and criminal record identity theft. All have significant consequences, requiring victims to spend time and resources restoring their credit, shutting down and opening accounts, filling out forms, and attending court proceedings. Victims may lose the ability to use credit, cash checks, obtain credit, or purchase a home or car. In insidious cases, one could be arrested for crimes committed by an identity thief.

Minnesota's identity theft law applies to various forms of identity theft. In reviewing the law, it is useful to discern their differences.[2]

Financial and Nonfinancial Identity Theft

Identity theft can be broken down into two main categories: financial and nonfinancial. In a case of financial identity theft, the identity thief uses personal information to access bank accounts, obtain credit cards, or charge purchases. Nonfinancial identity theft typically involves using personal information to obtain telephone services, rent apartments, avoid prosecution, or secure a job. It also includes altering passports or other identification documents to obtain entry into a country.

True Party Fraud vs. Account Takeover

Financial and nonfinancial identity theft can be further broken down according to whether a thief accesses old accounts or creates new ones. In "true party" frauds, the thief pretends to be the victim by using pieces of personal information to obtain new credit cards, open bank accounts, apply for loans, or rent apartments. In the case of "account takeover" frauds, the thief gains access to a victim's existing accounts to steal money or assets. The thief may redirect a victim's mail and have additional cards on the victim's account sent to the thief.

Reverse Record Identity Theft

A less commonly known type of identity theft is reverse record identity theft. This type of theft occurs when the thief uses the victim's identity to prevent someone else from detecting the thief's criminal history. The classic case involves a thief using another's identity to apply for a job because the thief wants his or her criminal history record concealed from a prospective employer (e.g., background checks).

---

[1] Department of Justice, FBI, Financial Crimes Report to the Public, May 2005.

[2] This information brief is limited to an overview of criminal provisions. Minnesota law also contains civil provisions relating to the prevention of identity theft, including data privacy, consumer rights, credit reporting, and unauthorized transaction liability. *See* Minn. Stat. chs. 13, 13C, 325E, 325F, 325G, and 325M.

Criminal Record Identity Theft

Another relatively unknown type of nonfinancial identity theft is criminal record identity theft. In such cases, the identity thief commits a separate crime (e.g., DWI, traffic violation) but provides the victim's name and address to avoid prosecution and a criminal record. A victim may only become aware of her predicament upon receipt of a citation notice or a notice of an outstanding arrest warrant. In egregious cases, the victim may be arrested for crimes committed by the identity thief.

Outline of Minnesota's Identity Theft Law

Crimes: Identity Theft and "Phishing"

To address identity theft, section 609.527 (Minnesota's identity theft law) criminalizes two types of behavior. First, it is a crime 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. Minn. Stat. § 609.527, subd. 2. Second, the law criminalizes the electronic use of a false pretense to obtain another's identity, often referred to as "phishing." Minn. Stat. § 609.527, subd. 5a.

For purposes of both crimes, the following definitions apply:

Direct victim: A person or entity who incurs a loss or harm and whose identity has been transferred, used, or possessed in violation of section 609.527

Indirect victim: A person or entity, other than a direct victim, who incurs a loss or harm (This is typically a bank or financial institution.)

Identity: 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.

Loss: Value obtained and expenses incurred

Definition of Identity Theft

Section 609.527, subdivision 2, prohibits transferring, possessing, or using another's identity with the intent to perpetrate 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.

The threshold question under subdivision 2 is whether the perpetrator intended to use another's identity to commit a crime. Identity theft is often associated with financial crimes, such as theft, financial transaction card fraud, or check fraud. These financial crimes fall under the purview of subdivision 2. In the case of nonfinancial identity theft, a crime may also be involved. For example, the typical case of criminal record identity theft involves a person giving another's identity to law enforcement or the court to avoid prosecution. Under Minnesota law, it is a gross misdemeanor to provide false information to a public official or court official. In the case of reverse record identity theft, the thief uses another's identity when applying for a job or an apartment to conceal a criminal record. It is a crime to forge a document for purposes of identification.[3] These cases of nonfinancial identity theft would fall under the criminal definition of identity theft.

Definition of "Phishing"

Another provision in the law specifically criminalizes the use of "phishing" schemes to obtain another's identifying information. Minn. Stat. § 609.527, subd. 5a. In a typical phishing scheme, a perpetrator uses fraudulent e-mail messages that appear to come from legitimate businesses. Authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers, passwords, credit card numbers, and Social Security numbers.

Under subdivision 5a, it is a crime to use a false pretense in an e-mail or web page to trick a victim into divulging his or her personal information. A "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 for-profit or not-for-profit business or organization or of a government agency, to which the user has no legitimate claim of right." Minn. Stat. § 609.527, subd. 1(c).

An important piece of the phishing legislation provides that a crime is committed even if a person does not obtain or use another's identity. The statute specifically forecloses the following defenses:

- the person committing the offense did not obtain another's identity
- the person committing the offense did not use another's identity
- the offense did not result in a financial loss or other loss to any person

[3] Certain misrepresentations on background checks are also made crimes by statute. For example, a person who makes a false representation to obtain a permit to possess, purchase, or carry certain firearms is guilty of a gross misdemeanor. Minn. Stat. §§ 624.7131, 624.7132, 624.714.

Penalties

There are separate penalty provisions for identity theft and phishing. Identity theft penalties vary and are tied to the resulting loss or harm involved. Because the crime of "phishing" is related to the conduct involved, whether or not it results in harm or loss, the penalty is fixed.

Identity Theft Penalties

The penalties for identity theft range from a misdemeanor to a 20-year felony. The offense level correlates with the amount of loss incurred, the number of direct victims involved, or the related offense. Loss is defined as the value obtained and the expenses incurred as a result of the crime.

Penalties for financial crimes are readily distinguishable by the monetary loss thresholds. For example, if the amount of loss is $250 or less, the maximum penalty is a misdemeanor. If the amount of loss is more than $35,000, the maximum penalty is a 20-year felony. Nonfinancial crimes that result in zero loss and involve only one victim default to the misdemeanor penalty. If a crime involves more than one victim, the penalty is raised to a felony.

Identity Theft Penalties **Minn. Stat. § 609.527, subd. 3.**			
Number of Direct Victims	**Combined Loss to Direct and 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 (§§ 617.246-617.247)	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

Phishing Penalties

For phishing crimes, the maximum penalty is a five-year felony and/or a $10,000 fine. Minn. Stat. § 609.527, subd. 5a.

Incident Reporting and Prosecution

The law's reporting and venue requirements reflect the ubiquitous nature of identity theft. While incident reporting and venue are typically tied to the location of the crime, the identity theft law

allows venue and reporting in the jurisdiction where the victim resides. This aids the victim whose perpetrator committed the crime in another state or over the Internet. 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. Minn. Stat. § 628.26.

Identity Theft Reporting and Prosecution

A person who has learned or reasonably suspects that he or she is a direct victim of identity theft may report the crime in the jurisdiction where the person resides, regardless of where the crime occurred. Law enforcement must prepare a police report and provide the complainant with a copy of the report. The agency may then begin an investigation or refer the report to another jurisdiction. Minn. Stat. § 609.527, subd. 5.

An offense may be prosecuted in either: (1) the county where the offense occurred, or (2) the county of residence or place of business of the direct or indirect victim. If the same person commits two or more offenses in two or more counties, the accused may be prosecuted for all the offenses in any of the counties where an offense occurred. 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. Minn. Stat. § 609.527, subds. 6 and 7.

Phishing Prosecution

In the case of phishing schemes, the venue is also located in the county of residence of the person whose identity was obtained *or sought.* This provision was included because 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. Minn. Stat. § 609.527, subd. 6.

Identity Theft Victims

A primary concern of identity theft legislation involves protecting and assisting victims. Identity theft often leaves victims in a quandary. A victim may need to spend time and resources restoring credit, closing and re-opening accounts, filling out forms, or attending court proceedings. Victims may also lose their ability to obtain credit, cash checks, or make purchases. In insidious cases, one could be arrested for crimes committed by an identity thief. The following provisions assist victims in recovering from identity theft and help curb further misuse of their identities.

Crime Victims' Rights

The law provides that a victim of identity theft is considered a victim for all purposes, including any rights that accrue under chapter 611A (Crime Victims: Rights, Programs, and Agencies).[4] Examples of victims' rights under this chapter include restitution, privacy rights (a victim may request that his or her identity and address remain confidential), notification rights (notice of a

[4] For more information on crime victims' rights, see the House Research information brief, *Crime Victim Laws in Minnesota: An Overview*, September 2007.

plea agreement, final disposition of the case, or defendant's appeal), and the right to present an impact statement in court. Minn. Stat. § 609.527, subd. 4(a).

Mandatory Restitution and Free Court Documents

Under the identity theft law, all direct victims are entitled to free certified court documents and mandatory restitution in an amount not less than $1,000. Mandatory restitution allows victims to seek compensation from a defendant without providing detailed documentation of losses incurred (which is otherwise required under chapter 611A). This provision was added to address the problem that victims may have in accounting for intangible losses and expenses involved in clearing their records (e.g., filling out paperwork, making telephone calls). Free copies of court documents aid victims in clearing up their personal credit and criminal histories without accumulating more costs. A direct victim or a prosecutor must make a written request to the court to receive free certified copies of the complaint, judgment, and order. Minn. Stat. § 609.527, subd. 4 (b), (c).

Mandatory restitution is not available to phishing victims, and free court documents are only provided to victims whose identity was transferred, used, or possessed in violation of the statute.

Minnesota Financial Crimes Oversight Council and Task Force

The Minnesota Financial Crimes Oversight Council and Task Force also aids victims of identity theft. The council is a coordinated state and local effort that aids in the investigation and prosecution of identity theft and financial crimes. Its primary duty is developing an overall strategy to ameliorate the harm caused to the public by identity theft and financial crimes in Minnesota. To achieve this goal, the governing statute confers statewide jurisdiction to law enforcement officers to conduct criminal investigations and authorizes the making of grants to state and local units of government to combat identity theft crimes. The council may offer financial rewards for tips that lead to the investigation and successful prosecution of identity thieves. In addition, the statute authorizes the establishment of a victims' assistance program to provide advice and guidance to victims on reporting identity theft and protecting their personal information. Minn. Stat. § 299A.681.

Criminal History Data Accuracy

In the event one'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. Certain criminal history data is public, and employers and landlords often use this information for background checks. Public data includes: (1) the identity of an individual who was convicted of a crime, (2) the convicted offense, (3) associated court disposition and sentence information, (4) the controlling agency, and (5) confinement information. This information is public for 15 years following the discharge of the imposed sentence. Minn. Stat. § 13.87.

If an individual's name or other identifying information is erroneously associated with a criminal history record, the individual may establish his or her innocence through fingerprint verification. Upon verification, the Bureau of Criminal Apprehension must redact the individual's name or other identifying information from the *public* criminal history record. The information continues to remain on the record as private data that is available only to criminal justice agencies. The

record is not completely redacted for public safety reasons. For example, if an identity thief is later arrested and uses the innocent person's identity again, the private data in the criminal history database would alert law enforcement to the fact that the arrested person may be using an alias. Minn. Stat. § 13.87.

To determine what data is associated with an individual's identity, the individual may request an "integrated search service" query be performed by a state or local law enforcement agency. The query would provide (1) a list of government entities that have public or private data about that individual, and (2) data that describes what information is maintained about that individual. Minn. Stat. § 13.873. If the individual subject of the data believes that private or public data is inaccurate or incomplete, the individual may notify the responsible authority in writing and seek a correction. Upon receiving notice, the responsible authority 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 government entity that holds the data. Minn. Stat. § 13.04.

If the responsible authority fails to take appropriate corrective action, it may be subject to civil and criminal liability. The responsible authority is liable for any damages suffered by the individual. In addition, for a willful violation, a responsible authority is guilty of a misdemeanor and is also liable for exemplary damages up to $10,000 for each violation. Finally, in addition to the above remedies, an aggrieved individual may seek an injunction or bring an action to compel compliance. Minn. Stat. §§ 13.08, 13.09.

Related Criminal Statutes

As the definition of the crime suggests, identity theft is perpetrated to facilitate other unlawful activities, such as credit card fraud, check fraud, or mortgage fraud. An identity thief may steal someone's identity to evade law enforcement or avoid arrest or prosecution. A crime may also involve the act of obtaining someone's identity through mail theft or computer theft.

The following crimes are frequently associated with identity theft. Prosecutors may bring several charges for the same act or series of acts, but a conviction on more than one offense must be based on different acts. (This section provides summary information on selected statutes. Readers should consult the most recent version of the criminal code for complete and updated information.)

Giving a peace officer a false name. It is a gross misdemeanor to obstruct justice by giving a peace officer the name and date of birth of another person in response to an inquiry incident to a lawful investigatory stop or arrest. The same penalty applies to persons who give the name and date of birth of another person to a court official in a criminal proceeding. Minn. Stat. § 609.506.

False information to financial institution. A person who informs a financial institution that a person's blank checks or debit cards have been lost or stolen, knowing or having reason to know that the information is false, is guilty of a misdemeanor. Minn. Stat. § 609.508.

Theft. It is a crime to intentionally and without claim of right take, use, transfer, conceal, or retain possession of property of another without the other's consent. Penalties for theft range from a misdemeanor to a 20-year felony. Minn. Stat. § 609.52.

Stolen or counterfeit checks. A person who sells, possesses, receives, or transfers a check that the person knows or has reason to know is stolen or counterfeit is guilty of a crime. Penalties for this crime range from a misdemeanor to a ten-year felony depending the amount of loss or number of direct victims involved. (A direct victim is any person or entity from whom a check is stolen or whose name or other identifying information is contained in a counterfeit check.) Minn. Stat. § 609.528.

Mail theft. The crime of mail theft is punishable by a three-year felony subject to a $5,000 fine. Mail theft includes, but is not limited to, doing any of the following acts intentionally and without claim of right: removing mail from a mail depository, making a false representation to wrongly obtain custody of mail, or removing the contents of mail addressed to another. Minn. Stat. § 609.529.

Issuance of dishonored checks. It is a crime to issue a check intending that it should not be paid. Proof of intent includes evidence that the issuer did not have an account with the financial institution. Penalties for issuing a dishonored check vary depending on the value of the dishonored check. Checks may be aggregated within any six-month period. Minn. Stat. § 609.535.

Forgery. Whoever, with intent to injure or defraud, uses a false writing for identification or falsifies any record, account, or other document relating to a person or business is guilty of forgery. A person who violates this section may be sentenced to three years' imprisonment and/or to payment of a $5,000 fine. Minn. Stat. § 609.63.

Check forgery/Offering a forged check. Whoever, with the intent to defraud, falsely makes or alters a check so that it purports to be made by another or falsely endorses a check is guilty of check forgery. Whoever, with the intent to defraud, offers or possesses with intent to offer a forged check is guilty of offering a forged check, regardless of whether the forged check is accepted.

The penalties for check forgery and offering a forged check range from a gross misdemeanor to a 20-year felony depending on the aggregate amount involved within a six-month period. Minn. Stat. § 609.631.

Fraudulent 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 for consideration and 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. Minn. Stat. § 609.652.

Fraud in obtaining credit. It is a crime to obtain credit from a bank, trust company, savings association, or credit union, by means of a present or past false representation as to the person or another's financial ability. If no money or property is obtained, the maximum penalty is 90 days' imprisonment and/or a $300 fine. If money or property is obtained, a person may be sentenced as provided in section 609.52, subdivision 3 (theft). Minn. Stat. § 609.82.

Financial transaction card fraud. The crime of financial transaction card fraud includes using a card without the consent of the cardholder to obtain property of another; knowingly using a forged card; providing false information to obtain a card; and falsely reporting that a card is lost or stolen with the intent to defraud the issuer. Other actions are also prohibited under this section.

The term "financial transaction card" includes, but is not limited to, credit cards, banking cards, debit cards, and electronic benefit system cards used to obtain credit, money, services, public assistance benefits, or anything else of value. A "cardholder" refers to the person in whose name a card is issued, and an "issuer" means a person, firm, or government agency that issues a financial transaction card.

The range of penalties for the offense is determined primarily by the type of fraud and amount of loss involved (certain losses may be aggregated over a six-month period). The minimum penalty is a gross misdemeanor and the maximum penalty is a 20-year felony. Enhanced sentences may apply if the person was convicted within the preceding five years of a gross misdemeanor or felony for robbery, theft, burglary, or forgery. Certain actions are criminalized even if no property is obtained. Minn. Stat. § 609.821.

Computer theft. Whoever, intentionally and without authorization or claim of right, accesses a computer, computer system, or computer network for the purpose of obtaining services or property is guilty of computer theft. Additionally, whoever intentionally and without authorization or claim of right, and with intent to deprive the owner of use or possession, takes, transfers, conceals, or retains possession of any computer, computer system, or any computer software or data is guilty of computer theft.

Misdemeanor and felony penalties apply to the crime of computer theft. The maximum penalty is a ten-year felony and applies if the loss involved is more than $2,500. Minn. Stat. § 609.89.

Unauthorized computer access. A person is guilty of unauthorized computer access if the person intentionally and without authorization attempts to or does penetrate a computer security system. A "computer security system" is a program or device that intends to protect the confidentiality of computer data.

The penalties for unauthorized computer access range from a misdemeanor to a ten-year felony. Gross misdemeanor and felony penalties apply to repeat offenses and offenses that compromise personal data, data security, public health and safety, or personal safety. Minn. Stat. § 609.891.

Criminal use of encryption. It is a crime to intentionally use or attempt to use encryption to: (1) commit, further, or facilitate conduct constituting a crime; (2) conceal the commission of a crime; (3) conceal or protect the identity of another who has committed a crime; or (4) prevent,

impede, delay, or disrupt the normal operation of a computer. The maximum penalty for criminal use of encryption is a five-year felony. Minn. Stat. § 609.8912.

Facilitating access to a computer security system. A person is guilty of a gross misdemeanor if the person knows or has reason to know that by facilitating access to a computer security system, the person is aiding another who intends to commit a crime and, in fact, commits a crime. "Facilitating access" includes intentionally disclosing a password, identity code, or other confidential information about the computer security system. Minn. Stat. § 609.8913.

Telecommunications and information services fraud. It is a crime to obtain telecommunication services for one's own use by any fraudulent means with the intent to evade a lawful charge. "Telecommunications service" means a service (in exchange for a pecuniary consideration) that provides or offers to provide transmission of messages, signals, faxes, or other communication via telephone, telegraph, cable, wire, fiber-optic cable, or the projection of energy. The amounts involved relating to one scheme or course of conduct may be aggregated. Minn. Stat. § 609.893.

Other Related Crimes

Crime	Minnesota Statute	Maximum penalty	Offense level
Bringing stolen property into state	§ 609.525	20 years/$100,000	Felony
Receiving stolen property	§ 609.53	20 years/$100,000	Felony
Misusing a credit card to secure services	§ 609.545	90 days/$1,000	Misdemeanor
Burglary	§ 609.582	20 years/$35,000	Felony
Insurance fraud	§ 609.611	20 years/$100,000	Felony
Aggravated forgery	§ 609.625	10 years/$20,000	Felony
Filing a forged instrument	§ 609.64	3 years/$5,000	Felony
False certification by (purported) notary public	§ 609.65	3 years/$5,000	Felony
Fraudulent or otherwise improper financing statements	§ 609.7475	5 years/$10,000	Felony
Computer damage	§ 609.88	10 years/$50,000	Felony
Cellular telephone counterfeiting	§ 609.894	5 years/$10,000	Felony
Interception and disclosure of wire or oral communications	§ 626A.02	5 years/$20,000	Felony

Additional Penalties and Sanctions

A perpetrator of identity theft or a related crime may be subject to additional sanctions under the law, including forfeiture and racketeering penalties.

Forfeiture. Minnesota's forfeiture law lists a felony violation of, or a felony-level attempt to violate, section 609.527 (identity theft) as a "designated offense." Other "designated offenses" include felony violations or felony-level attempt violations of sections 609.52 (theft); 609.525 (bringing stolen goods into the state); 609.528 (possession or sale of a stolen or counterfeit check); 609.631 (check forgery); and 609.89 (computer theft).

All personal property is subject to forfeiture if it was used or intended for use to commit or facilitate the commission of a designated offense. All money and other property, real or personal, which represent proceeds of a designated offense, are subject to forfeiture. The property may be seized immediately without process if certain provisions are met. All right, title, and interest in the property vests in the appropriate agency upon commission of the act giving rise to forfeiture. Minn. Stat. § 609.531.

Racketeering. The crime of racketeering targets individuals participating in a pattern of *criminal activity* (three or more acts). Criminal activity includes a felony violation of identity theft, as well as other related identity theft crimes. Racketeering is punishable by a sentence of imprisonment of 20 years and/or payment of a $1,000,000 fine. Minn. Stat. §§ 609.902 *et seq.*

Historical Summary of Criminal Identity Theft Legislation

Original Legislation

1999 In 1999, the legislature created the crime of identity theft in section 609.527 of the Minnesota criminal code. The original act provided criminal penalties and forfeiture sanctions for persons who transferred, possessed, or used the identity of another to commit or aid in the commission of an unlawful activity. Penalties ranged from a misdemeanor to a ten-year felony and were based on the combined loss to the direct and indirect victims or the number of direct victims involved. The original legislation provided that identity theft victims were entitled to court-ordered restitution and any rights that accrued under chapter 611A. Laws 1999, ch. 244, §§ 2-3.

Legislative Changes

2000 In 2000, the legislature adjusted the loss amounts for identity theft penalties. It also enacted new crimes to address the issue of stolen and counterfeit checks, as well as false reporting of lost or stolen checks and debit cards. Corresponding provisions were added to the forfeiture and racketeering statutes to reflect these new crimes. Laws 2000, ch. 354, §§ 2-7.

2001 During special session, the 2001 Legislature established the Financial Crimes Investigation Task Force to investigate consumer identity theft cases and financial crimes. Laws 2001, 1st spec. sess., ch. 8, art. 5, § 5.

2003 The 2003 Legislature added reporting, venue, and aggregation provisions to the identity theft law and criminalized mail theft. It also made changes to the Financial Crimes Task Force, including a repealer of the sunset provision. Laws 2003, ch. 106, § 1 (reporting), § 2 (venue), § 3 (aggregation), § 4 (mail theft).

During the 2003 special session, the identity theft penalties were changed to reflect a new 20-year felony for offenses that involved eight or more direct victims or combined losses of more than $35,000. The legislature also directed the Sentencing Guidelines Commission to add to its list of aggravating factors an offender's use of another identity without authorization, to commit a crime. Laws 2003, 1st spec. sess., ch. 2, art. 8, §§ 9, 18.

2005 In 2005, the crime of "phishing" (electronic use of false pretense to obtain identity) was created. The legislature also expanded the identity theft restitution provisions, providing direct victims with mandatory restitution and access to free court documents. The legislature augmented the identity theft penalty provisions, expanding the 20-year felony to include offenses related to possession or distribution of pornographic work involving minors. Finally, the legislature restructured the Financial Crimes Task Force and made it permanent. The new Minnesota Financial Crimes Oversight Council provides guidance in investigating and prosecuting identity theft crimes and is authorized to establish a victims' assistance program. Laws 2005, ch. 136, art. 11, § 5; art.17, §§ 32-36.

2006 The 2006 Legislature addressed identity theft by amending statutes to account for increasing technological advances. It created the crimes of criminal use of encryption and facilitating access to a computer security system; it increased penalties for unauthorized computer access to personal data; and it deleted the requirement that a hacker receive "notice" of breaking into a security system to be guilty of a crime. Laws 2006, ch. 260, art. 1, §§ 30-37.

2007 In 2007, the legislature enacted laws to aid victims of criminal record identity theft. The law provides that if an innocent person's identifying information is erroneously associated with a criminal history record, any identifying information must be redacted from the public criminal history record. Previously, the erroneous information remained on the public record with a note stating that the information was erroneously attributed to the data subject. This was problematic in instances where an employer or landlord conducted a background check on an innocent person, did not fully understand the cautionary note, and made adverse decisions based on incorrect information (e.g., denying a job or apartment based on someone else's criminal record). Laws 2007, ch. 129, §§ 44, 46.

For more information about criminal laws, visit the criminal justice area of our web site, www.house.mn/hrd/issinfo/crime.htm.

Appendix A

Minnesota Sentencing Guidelines

Under the Minnesota Sentencing Guidelines, felony offenses are divided into eleven levels of severity, ranging from low (Level I) to high (Level XI). The offense level, combined with the offender's criminal history, determines the offender's presumptive sentence. The following table references crimes associated with identity theft and their corresponding presumptive sentence.

Minnesota Sentencing Guidelines (Criminal History Score = 0–6)				
Crime	**Amount Involved**	**Statutory Ref.**	**Offense Severity Level**	**Presumptive Sentence Range (in months)**
Identity theft	Over $35,000	609.527, subd. 3(5)	VIII	48–108
Check forgery	Over $35,000	609.631, subd. 4(1)	V	18–48
Financial transaction card fraud	Over $35,000	609.821, subd. 3(1)(I)	V	18–48
Check forgery	Over $2,500	609.631, subd. 4(2)	III	12–23
Identity theft	Over $2,500	609.527, subd. 3(4)	III	12–23
Stolen or counterfeit check		609.528, subd. 3(4)	III	12–23
Phishing		609.527, subd. 5a	II	12–21
Check forgery	$251–$2,500	609.631, subd. 4 (3)(a)	II	12–21
Identity theft	$501–$2,500	609.527, subd. 3(3)	II	12–21
Check forgery	$250 or less	609.631, subd. 4(3)(b)	I	12–19
Financial transaction card fraud		609.821, subd. 2 (3) & (4)	I	12–19
Fraudulent drivers' licenses and ID		609.652	I	12–19

A judge must use the presumptive sentence found in the guidelines when imposing a sentence. However, if substantial and compelling circumstances are involved and determined by the factfinder, the court may depart upward from the presumptive sentence. One such recognized circumstance is an offender's use of another's identity without authorization to commit a crime. This is considered an **aggravating factor**, but it may only be used when the use of another's identity is not an element of the offense.

Appendix B

Selection of Federal Criminal Laws Relating to Identity Theft

Citation	Act or Short Name	Description of Crime	Maximum Penalty
18 U.S.C. § 1028 (a)(7)	Identity Theft and Assumption Deterrence Act of 1998	Makes it a crime to knowingly transfer, possess, or use personally identifying information without authorization and with the intent to commit any unlawful activity under federal law or an activity that is a felony under state law. Identifying information includes name, date of birth, Social Security number, driver's license, fingerprints, retina or iris image, and electronic identification numbers. The maximum penalty applies if the offense facilitated an act of domestic or international terrorism.	30 years' imprisonment/ $250,000 fine
15 U.S.C. § 1644	Consumer Credit Protection Act	Sets out six different acts relating to the fraudulent use of a credit card	10 years' imprisonment/ $10,000 fine
18 U.S.C. § 1029	Credit Card Fraud Act of 1984	Makes it a crime to knowingly produce, use, possess, or traffic in "counterfeit access devices" or "unauthorized access devices," which includes debit cards, credit cards, account numbers, and forged credit card receipts	20 years' imprisonment/ $250,000 fine
18 U.S.C. § 1341	Mail fraud	Makes it a crime for anyone with an intent or scheme to defraud to use the U.S. Postal Service or private or commercial carriers to send or receive anything in the course of the scheme	30 years' imprisonment/ $1,000,000 fine
18 U.S.C. § 1343	Wire fraud	Makes it a crime for anyone who "transmits or causes to be transmitted by means of wire, radio or television communications in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing … a scheme or artifice" with intent to defraud	30 years' imprisonment/ $1,000,000 fine
18 U.S.C. § 1344	Financial institution fraud	Makes it a crime to knowingly execute, or attempt to execute, a scheme to defraud a financial institution or obtain any moneys or funds controlled by the institution	30 years' imprisonment/ $1,000,000 fine
18 U.S.C. § 1030(a)(4)	Computer fraud	Makes it a crime to knowingly and with intent to defraud, access a protected computer without authorization and obtain anything of value	10 years' imprisonment/ $250,000 fine
42 U.S.C. § 408(a)(7)(B)	Unauthorized use of Social Security number	Prohibits the unauthorized use of a Social Security number to obtain payment or a benefit to which the person is not entitled by falsely representing the assignment of a Social Security number	5 years' imprisonment
15 U.S.C. § 1693n	Electronic Fund Transfer Act	Provides consumer protection for ATM and debit card transactions. Contains disclosure requirements and violations for transaction fraud Disclosure violation: one-year imprisonment/$5,000 fine Transaction violation: ten years' imprisonment /$10,000 fine	See description of crime