Prepared by the North Dakota Legislative Council
staff for the Judicial Process Committee
September 2005

IDENTITY THEFT - BACKGROUND MEMORANDUM

House Concurrent Resolution No. 3042 (attached as Appendix A) directs a study of the laws of this state and other states as they relate to the unauthorized acquisition, theft, and misuse of personal identifying information belonging to another individual. Testimony in support of the resolution indicated that a need exists to review the laws of the state to determine if those laws provide the citizens of the state with adequate protection from identity theft.

WHAT IS IDENTITY THEFT?

Identity theft occurs when an individual possesses or uses another individual's name, address, Social Security number, bank or credit card account number, or other personal identifying information without that other individual's knowledge with the intent to commit fraud or other crimes. The Federal Trade Commission reports that identity theft is the fastest growing white-collar crime.

Identity thieves use a variety of low- and high-tech methods to gain access to an individual's personal identifying information. For example, an identity thief may get information from businesses or institutions by stealing records, bribing an employee who has access to the records, conning information out of employees, or hacking into the organization's computers. Other methods an identity thief may use to get information include rummaging through an individual's trash, the trash of businesses, or in dumpsters in a practice known as "dumpster diving"; obtaining credit reports by abusing the identity thief's employer's authorized access to credit reports; posing as a landlord, employer, or someone else who may have a legitimate need for and a legal right to the information; stealing credit and debit card account numbers as the card is processed by using a special information storage device in a practice known as "skimming"; stealing wallets and purses containing identification and credit and bank cards; stealing mail, including bank and credit card statements, preapproved credit offers, new checks, or tax information; completing a "change of address form" to divert mail to another location; stealing personal information from a person's home; or scamming information from a person by posing as a legitimate business person or government official.

Once an identity thief obtains personal identifying information, the thief may:

- Go on spending sprees using the victim's credit and debit card account numbers to buy "big-ticket" items, like computers, which can be sold easily;
- Open a new credit card account, using the stolen name, date of birth, and Social Security number. When the bills for those purchases are unpaid, the delinquent account is reported on the victim's credit report;
- Change the mailing address on the victim's credit card account. The thief then runs up charges on the account. Because the bills are being sent to the new address, it may take some time before the victim realizes there is a problem;
- Take out auto loans in the victim's name;
- Establish telephone or wireless service in the victim's name;
- Use counterfeit checks or debit cards to drain the victim's bank account;
- Open a bank account in the victim's name and write bad checks on that account;
- File for bankruptcy under the victim's name to avoid paying debts the thief has incurred, or to avoid eviction; or
- Give the victim's name to the police during an arrest. If the thief is released and does not show up for the court date, an arrest warrant could be issued in the victim's name.

PREVALENCE OF IDENTITY THEFT

According to the National Conference of State Legislatures (NCSL), a 2003 survey of over 4,000 people indicated that 4.6 percent of respondents reported being a victim of identity theft in the last year. According to NCSL, this percentage suggests that almost 10 million Americans discovered they were victims of identity theft in the last year. The survey indicated that almost 13 percent discovered that they were victimized in the last five years. The survey categorized identity theft into three types. The most serious--new accounts and other frauds--involved misusing personal information to open new credit accounts or new loans and misusing identifying information when charged with a crime, renting an apartment, or obtaining medical care. The second category addressed the misuse of an existing credit card account or credit card number. The final category involved the misuse of an existing non-credit card account, such as a checking or savings account.

More than half of those individuals who fell into the first category--new accounts and other frauds--also experienced the misuse of existing credit card or non-credit card accounts. Twenty-two percent of victims contacted one or more credit bureaus once they discovered their information had been misused. Of those, 62 percent reported that one or more of the credit bureaus placed a fraud alert on their credit report. Twenty-six percent reported the misuse to their local law enforcement agency.

According to a Federal Trade Commission report, between January and December 2004--Consumer Sentinel--the complaint data base developed and maintained by the Federal Trade Commission, received over 635,000 consumer fraud and identity theft complaints. According to the report, consumers reported losses from fraud and identity theft of more than $547 million. In the area of identity fraud, the report indicated that credit card fraud (28 percent) was the most common form of reported identity theft followed by telephone or utilities fraud (19 percent), bank fraud (18 percent), and employment fraud (13 percent). Other significant categories of identity theft reported by victims were government documents and benefits fraud and loan fraud. According to the report, the percentage of complaints about "electronic fund transfer" related identity theft more than doubled between 2002 and 2004. The major metropolitan areas with the highest per capita rates of reported identity theft were Phoenix-Mesa-Scottsdale, Arizona; Riverside-San Bernardino-Ontario, California; and Las Vegas-Paradise, Nevada.

The Federal Trade Commission report also indicated that there were 188 identity theft complaints from North Dakota victims, including 53 for credit card fraud (28 percent), 42 for telephone or utilities fraud (22 percent); 27 for bank fraud (14 percent); 12 for employment-related fraud (6 percent); 11 for government documents or benefits fraud (6 percent); 9 for loan fraud (5 percent); 52 for other (28 percent); and 11 for attempted identity theft (6 percent). The report also listed the number of identity thefts by city--Fargo (42), Grand Forks (22), Bismarck (17), Minot (17), Cavalier (6), Dickinson (6), Mandan (6), and Minot Air Force Base (6).

NORTH DAKOTA LAW

North Dakota Century Code Section 12.1-23-11, enacted in 1999, prohibits the unauthorized use of personal identifying information. This section provides, in part:

> A person is guilty of an offense if the person uses or attempts to use any personal identifying information of an individual, living or deceased, to obtain credit, money, goods, services, or anything else of value without the authorization or consent of the individual and by representing that person is the individual or is acting with the authorization or consent of the individual. The offense is a class B felony if the credit, money, goods, services, or anything else of value exceeds one thousand dollars in value, otherwise the offense is a class C felony. A second or subsequent offense is a class A felony.

In addition to the specific statute for the unauthorized use of personal identifying information, there are a number of theft statutes that are likely to be applicable. North Dakota Century Code Section 12.1-23-02 provides:

> A person is guilty of theft if he:
>
> 1. Knowingly takes or exercises unauthorized control over, or makes an unauthorized transfer of an interest in, the property of another with intent to deprive the owner thereof;
> 2. Knowingly obtains the property of another by deception or by threat with intent to deprive the owner thereof, or intentionally deprives another of his property by deception or by threat; or
> 3. Knowingly receives, retains, or disposes of property of another which has been stolen, with intent to deprive the owner thereof.

North Dakota Century Code Section 12.1-23-03 applies to theft of services. This section provides:

> A person is guilty of theft if:
>
> 1. He intentionally obtains services, known by him to be available only for compensation, by deception, threat, false token, or other means to avoid payment for the services; or
> 2. Having control over the disposition of services of another to which he is not entitled, he knowingly diverts those services to his own benefit or to the benefit of another not entitled thereto.
>
> Where compensation for services is ordinarily paid immediately upon their rendition, as in the case of hotels, restaurants, and comparable establishments, absconding without payment or making provision to pay is prima facie evidence that the services were obtained by deception.

North Dakota Century Code Section 12.1-23-05 provides for the grading of theft offenses. This section provides that theft is a Class B felony if the property or services stolen exceed $10,000 in value or are acquired or retained by a threat to commit a Class A or Class B felony or to inflict serious bodily injury on the person threatened or on any other person. This section provides that theft is a Class C felony if certain criteria are met, including that the property or services stolen exceed $500 in value; the property or services stolen are acquired or retained by threat and either exceed $50 in value or are acquired or retained by a public servant by a threat to take or withhold official action; or the property or services stolen exceed $50 in value and are acquired or retained by a public servant in the course of official duties. With some exceptions, all other theft under Chapter 12.1-23 is a Class A misdemeanor.

North Dakota also has a body of law that addresses issues relating to consumer fraud. North Dakota Century Code Chapter 51-15 is often referred

to as the state's "consumer fraud law." Section 51-15-02 provides that:

> The act, use, or employment by any person of any deceptive act or practice, fraud, false pretense, false promise, or misrepresentation, with the intent that others rely thereon in connection with the sale or advertisement of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is declared to be an unlawful practice.

The law authorizes the Attorney General to conduct and investigate unlawful practices under North Dakota Century Code Chapter 51-15. The chapter also authorizes the Attorney General, upon court approval, to obtain injunctions, cease and desist orders, restitution, the appointment of a receiver, and the imposition of penalties, attorney's fees, and expenses. Section 51-15-09 creates a private cause of action for violations of the consumer fraud laws.

2005 Legislation

In 2005 the North Dakota Legislative Assembly passed a number of bills related to the issue of identity theft.

- House Bill No. 1211, which amended North Dakota Century Code Section 12.1-23-11, provided that a person is guilty of an offense if the person uses or attempts to use any personal identifying information of an individual, living or deceased, to obtain credit, money, goods, services, or anything else of value without the authorization or consent of the individual. The bill provided that the offense is a Class B felony if the value of the credit, money, goods, or services obtained exceeds $1,000 in value, otherwise the offense is a Class C felony; and a subsequent offense is a Class A felony. The bill also provided that prosecution for a violation must be commenced within six years after the discovery by the victim of the facts constituting the violation.
- House Bill No. 1500, codified as North Dakota Century Code Chapter 51-31, created a new body of law regarding identity theft. The bill provided that, upon the request of a consumer, a consumer reporting agency is required to include an initial or extended fraud alert on the file of that consumer. The bill also provided that an individual who learns or reasonably suspects that the individual's personal identifying information has been unlawfully used by another may initiate a law enforcement action by contacting the local law enforcement agency and that an individual who reasonably believes the individual is the victim of identity theft may petition the district court for an expedited judicial determination of the individual's factual innocence. The bill also provided that identity theft laws may be enforced by the Attorney General and a violation of the identity theft laws is a violation of the consumer fraud and unlawful credit practices laws.
- Senate Bill No. 2251 provided that in the case of a breach of security, a person that conducts business in North Dakota and that owns or licenses computerized data that includes personal information is required to notify the residents of this state who may have been affected by the breach and provides that a person that maintains such computerized data for such an owner or licensee must notify the owner if there is a breach of security. The bill also provided that the breach of security laws may be enforced by the Attorney General and violation of the breach of security laws is a violation of the consumer fraud and unlawful credit practices laws.

IDENTITY THEFT LAWS OF OTHER STATES

Nearly all 50 states have enacted laws that specifically address the issue of identity theft. Several states, such as Alaska and Colorado, have not enacted specific identity theft laws but rather rely on their general theft statutes to address the issue. A number of states, including Missouri, Montana, Nebraska, and Pennsylvania, make the act of stealing identifying information a crime even if no credit, money, goods, services, or other thing of value was gained or was attempted to be gained. Although the classification of the offenses varies greatly from state to state, most states base the severity of the penalty on the dollar amount of the theft. Attached as Appendix B is a summary, compiled by NCSL, of the identity theft statutes of each of the 50 states as well as the District of Columbia.

IDENTITY THEFT LEGISLATION OF OTHER STATES - 2005

In 2005 at least 25 states enacted legislation to address issues relating to identity theft. For example, Illinois passed a law that removed the statute of limitations for the commencement of an identity theft prosecution and a law that increased the penalties for identity theft and aggravated identity theft by one class higher than the current law. Illinois also passed a law that prohibits the denial of credit, public utility services, or the reduction in the credit limit of a consumer solely because the consumer has been a victim of identity theft. Kansas changed the definition of identity theft from someone who uses personal identification to knowingly and intentionally defraud a person for economic benefit to a person receiving any benefit from using someone else's personal identification. A number of states, including North Dakota,

Maine, and Montana, enacted legislation that limits the information a consumer reporting agency may report without the consumer's authorization. Several states, including North Dakota, Montana, Maryland, and Hawaii, passed legislation to study issues relating to identity theft. Attached as Appendix C is a summary, compiled by NCSL, of identity theft legislation enacted in 2005.

FEDERAL IDENTITY THEFT LAWS

Identity Theft and Assumption Deterrence Act of 1998

In October 1998 Congress passed the Identity Theft and Assumption Deterrence Act of 1998 [Pub. L. 105-318; 112 Stat. 3007; 18 U.S.C. 1028] to address the problem of identity theft. Specifically, the Act made it a federal crime when anyone:

> [K]nowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

Violations of the Act are investigated by federal investigative agencies, such as the United States Secret Service, the Federal Bureau of Investigation, and the United States Postal Inspection Service and are prosecuted by the Department of Justice. Section 5 of this Act makes the Federal Trade Commission a central clearinghouse for identity theft complaints. The Act requires the Federal Trade Commission to log and acknowledge such complaints, provide victims with relevant information, and refer their complaints to appropriate entities, such as the major national consumer reporting agencies and other law enforcement agencies.

Identity Theft Penalty Enhancement Act of 2003

The Identity Theft Penalty Enhancement Act of 2003 [18 U.S.C. 47] establishes penalties for aggravated identity theft. The Act prescribes sentences of two years' imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during and in relation to specified felony violations, including felonies relating to theft from employee benefit plans and various fraud and immigration offenses; and five years' imprisonment for knowingly taking such action during and in relation to specified felony violations pertaining to terrorist acts, in addition to the punishments provided for such felonies. The Act prohibits a court from placing any person convicted of the violation on probation; reducing any sentence for the related felony to take into account the sentence imposed for the violation; or providing for concurrent terms of imprisonment for a violation of the Act and any other violation, except, in the court's discretion, an additional violation of the Act. The Act also expands the existing identity theft prohibition to cover possession of a means of identification of another with intent to commit specified unlawful activity, increase penalties for violations, and include acts of domestic terrorism within the scope of a prohibition against facilitating an act of international terrorism.

Fair Credit Reporting Act

The Fair Credit Reporting Act [15 U.S.C. 1681 et seq.] establishes procedures for correcting mistakes on an individual's credit record and requires that a credit record only be provided for legitimate business needs. The Act, enforced by the Federal Trade Commission, is designed to promote accuracy and ensure the privacy of the information used in consumer reports. Recent amendments to the Act were intended to expand consumer rights and place additional requirements on credit reporting agencies.

Other Federal Laws

- Fair Credit Billing Act [15 U.S.C. 1601] establishes procedures for resolving billing errors on credit card accounts. The Act also limits a consumer's liability for fraudulent credit card charges.
- Fair Debt Collection Practices Act [15 U.S.C. 1692] prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection.
- Electronic Fund Transfer Act [15 U.S.C. 1693] provides consumer protection for all transactions using a debit card or electronic means to debit or credit an account. The Act also limits a consumer's liability for unauthorized electronic fund transfers.
- Driver's Privacy Protection Act of 1994 [Pub. L.103-322; 18 U.S.C. 2721 et seq.] places limits on disclosures of personal information in records maintained by departments of motor vehicles.
- Family Educational Rights and Privacy Act of 1974 [20 U.S.C. 1232g] puts limits on disclosure of educational records maintained by agencies and institutions that receive federal funding.
- Gramm-Leach-Bliley Act [Pub. L. 106-102; 113 Stat. 1338, 1436-4515; U.S.C. 6801-6809] requires the Federal Trade Commission, along with the federal banking agencies, the National Credit Union Administration, the Treasury Department, and the Securities and Exchange Commission, to issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information. Those institutions are required to develop and give notice of their privacy policies to their own

customers at least annually, and before disclosing any consumer's personal financial information to a nonaffiliated third party, must give notice and an opportunity for that consumer to "opt out" from such disclosure.

- Health Information Portability and Accountability Act of 1996 [Pub. L. 104-191; 110 Stat. 1936; 42 U.S.C. 201] regulates the security and confidentiality of patient information.

PREVIOUS STUDIES

The 2001-02 interim Family Law Committee, pursuant to Senate Concurrent Resolution No. 4019, studied the medical and financial privacy laws in this state, the effectiveness of medical and financial privacy laws in other states, the interaction of federal and state medical and financial privacy laws, and whether current medical and financial privacy protections meet the reasonable expectations of the citizens of North Dakota. The committee recommended two bills. House Bill No. 1038, which failed to pass the House, would have provided for financial privacy definitions of customer and financial institution and provided for certain financial privacy exceptions. Senate Bill No. 2037, which limits the information on electronically printed credit card receipts, was enacted in 2003.

SUGGESTED STUDY APPROACH

The committee, in its study of the laws of this state and other states as they related to the unauthorized acquisition, theft, and misuse of personal identifying information belonging to another individual, may wish to approach this study as follows:

- Receive information and testimony from the Attorney General's office regarding identity theft issues in North Dakota and the need for legislative changes to address those issues;
- Receive information from law enforcement agencies on the issues and problems that may arise in investigating identity fraud cases;
- Receive information on whether North Dakota's laws adequately and comprehensively address the prohibition of and the penalties for identity theft; and
- Develop recommendations and prepare legislation necessary to implement the recommendations.

ATTACH:3