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

Fifty-ninth Legislative Assembly of North Dakota
In Regular Session Commencing Tuesday, January 4, 2005

HOUSE CONCURRENT RESOLUTION NO. 3042
(Representatives Kasper, Ruby, Thoreson, Weiler)
(Senators Holmberg, Klein)

A concurrent resolution directing the Legislative Council to study 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.

WHEREAS, identity theft is an issue of rising national importance, with the federal government as well as state governments investing significant energy into researching possible approaches to more effectively deal with this problem; and

WHEREAS, as technology continues to evolve, the opportunities for identity theft become more and more sophisticated and far-reaching; and

WHEREAS, the personal and commercial damages resulting from unauthorized use of personal identifying information are significant; and

WHEREAS, North Dakotans are being harmed by identity theft; and

WHEREAS, residents of this state have voiced a concern that North Dakota's laws do not adequately and comprehensively address the prohibition of and the penalties for identity theft;

NOW, THEREFORE, BE IT RESOLVED BY THE HOUSE OF REPRESENTATIVES OF NORTH DAKOTA, THE SENATE CONCURRING THEREIN:

That the Legislative Council study 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; and

BE IT FURTHER RESOLVED, that the Legislative Council report its findings and recommendations, together with any legislation required to implement the recommendations, to the Sixtieth Legislative Assembly.

IDENTITY THEFT STATUES AS OF FEBRUARY 9, 2005

State	Statutory Citation	Title	Penalty
Alabama	13A-8-190 to 13A-8-201	The Consumer Identity Protection Act	Identity theft in which there is a financial loss of greater than $500 or the defendant has previously been convicted of identity theft constitutes identity theft in the first degree. Identity theft in the first degree is a Class C felony. Identity theft in which the defendant has not previously been convicted of identity theft and there is no financial loss or the financial loss is $500 or less constitutes identity theft in the second degree. Identity theft in the second degree is a Class A misdemeanor. Trafficking in stolen identities is a Class B felony. Obstructing justice using a false identity is a Class C felony.
Alaska	11.46.180	Theft by deception	First degree is a Class B felony Second degree is a Class C felony Third degree is a Class A misdemeanor Fourth degree is a Class B misdemeanor
Arizona	13-2008	Taking identity of another person; classification	Class 4 felony
Arkansas	5-37-227	Financial identity fraud	Class D felony
California	Penal Code 530.5 to 530.8		Upon conviction a person shall be punished either by imprisonment in a county jail not to exceed one year, a fine not to exceed $1,000, or both that imprisonment and fine, or by imprisonment in the state prison, a fine not to exceed $10,000, or both that imprisonment and fine.
Colorado		Does not have a specific identity theft law	
Connecticut	53a-129a Public Act 03-156	Identity theft Identity theft in the first degree Identity theft in the second degree. Identity theft in the third degree. Trafficking in personal identifying information	Class D felony Class B felony Class C felony Class D felony Class D felony
Delaware	11 §854	Identity theft	Class D felony
District of Columbia	22-3227.01 to 3227.08	Identity theft	Identity theft in the first degree. -- Any person convicted of identity theft shall be fined not more than (1) $10,000, (2) three times the value of the property obtained, or (3) three times the amount of the financial injury, whichever is greatest, or imprisoned for not more than 10 years, or both, if the property obtained or the amount of the financial injury is $250 or more. Identity theft in the second degree. -- Any person convicted of identity theft shall be fined not more than $1,000 or imprisoned for not more than 180 days, or both, if the value of the property obtained or the amount of the financial injury, whichever is greater, is less than $250. Any person who commits the offense of identity theft against an individual who is 65 years of age or older, at the time of the offense, may be punished by a fine of up to 1 1/2 times the maximum fine otherwise authorized for the offense and may be imprisoned for a term of up to 1 1/2 times the maximum term of imprisonment otherwise authorized for the offense, or both.
Florida	817.568	Criminal use of personal identification information	817.568(2)(a) Third degree felony 817.568(2)(b) Second degree felony 817.568(2)(c) First degree felony 817.568(3) First degree misdemeanor 817.568(4) First degree misdemeanor 817.568(5) reclassification

State	Statutory Citation	Title	Penalty
Georgia	16-9-121 to 16-9-128	Financial identity fraud	Punishable by imprisonment for not less than one nor more than 10 years or a fine not to exceed $100,000, or both for first offense. Punishable by imprisonment for not less than three nor more than 15 years, a fine not to exceed $250,000, or both for subsequent offenses
Hawaii	708.839.6 708.839.7 708.839.8	Identity theft in the first degree. Identity theft in the second degree. Identity theft in the third degree	Class A felony Class B felony Class C felony
Idaho	18-3126 18-3128	Misappropriation of personal identifying information	Misdemeanor Felony if retail value exceeds $300
Illinois	720 ILCS 5/16G-1 to 720 ILCS 5/16G-25	Identity theft	Class A misdemeanor if under $300 in value for first offense Class 4 felony for subsequent offense Class 4 felony if between $300 and $2,000 Class 3 felony if between $2,000 and $10,000 Class 2 felony if between $10,000 and $100,000 Class 1 felony if exceeds $100,000
Indiana	35-43-5-1 34-43-5-3.5	Definitions Penalties	Class D felony
Iowa	715A-8	Identity theft	Aggravated misdemeanor if under $1,000 Class D felony if exceeds $1,000
Kansas	21-4018	Identity theft	Severity level 7 person felony
Kentucky	514.160 514.170	Theft of identity Trafficking in stolen identities	Class D felony Class C felony
Louisiana	RS 14:67.16	Identity theft	Punishable by imprisonment for not more than six months or fined not more than $500, or both if less than $300 for first offense. Punishable by imprisonment for not more than three years, with or without hard labor, or fined not more than $300 for subsequent offenses. Punishable by imprisonment, with or without hard labor, for not more than three years, or fined not more than $3,000, or both if between $300 and $500. Punishable by imprisonment, with or without hard labor, for not more than five years, or fined not more than $5,000, or both if between $500 and $1,000. Punishable by imprisonment, with or without hard labor, for not more than 10 years, or fined not more than $10,000, or both if $1,000 or more.
Maine	17-A§905-A	Misuse of identification	Class D crime
Maryland	§8-301 to §8-303	Identity fraud	Misdemeanor where the benefit, credit, good, service, or other thing of value has a value of less than $500. Felony where the benefit, credit, good, service, or other thing of value has a value of $500 or greater.
Massachusetts	266§37E	Use of personal identification of another; identity fraud; penalty; restitution	Felony
Michigan	750.285	Obtaining personal identity information of another with intent to unlawfully use information; violation as felony; nonapplicability to	Guilty of a felony punishable by imprisonment for not more than five years or a fine of not more than $10,000, or both.

State	Statutory Citation	Title	Penalty
		discovery process; definitions	
Minnesota	609.527	Identity theft	If the offense involves a single direct victim and the total, combined loss to the direct victim and any indirect victims is $250 or less, the person may be sentenced to imprisonment not more than 90 days or fined not more than $700, or both. If the offense involves a single direct victim and the total, combined loss to the direct victim and any indirect victims is more than $250 but not more than $500, the person may be sentenced to imprisonment for not more than one year or to payment of a fine of not more than $3,000, or both. If the offense involves two or three direct victims or the total, combined loss to the direct and indirect victims is more than $500 but not more than $2,500, the person may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $10,000, or both. If the offense involves four or more direct victims, or if the total, combined loss to the direct and indirect victims is more than $2,500, the person may be sentenced to imprisonment for not more than ten years or to payment of a fine of not more than $20,000, or both.
Mississippi	97-19-85	Fraudulent use of identity, Social Security number, credit card or debit card number or other identifying information to obtain thing of value	Guilty of a felony and upon conviction thereof for a first offense shall be fined not more than $5,000 or imprisoned for a term not to exceed five years, or both. For a second or subsequent offense such person, upon conviction, shall be fined not more than $10,000 or imprisoned for a term not to exceed 10 years, or both.
Missouri	570.223	Identity theft--penalty--restitution	Identity theft or attempted identity theft which does not result in the theft or appropriation of credit, money, goods, services, or other property is a class B misdemeanor; (2) Identity theft which results in the theft or appropriation of credit, money, goods, services, or other property not exceeding $500 in value is a class A misdemeanor; (3) Identity theft which results in the theft or appropriation of credit, money, goods, services, or other property exceeding $500 and not exceeding $10,000 in value is a class C felony; (4) Identity theft which results in the theft or appropriation of credit, money, goods, services, or other property exceeding $10,000 and not exceeding $100,000 in value is a class B felony; (5) Identity theft which results in the theft or appropriation of credit, money, goods, services, or other property exceeding $100,000 in value is a class A felony. In addition, the court may order that the defendant make restitution to any victim of the offense. Restitution may include payment for any costs, including attorney fees, incurred by the victim.
Montana	45-6-332	Theft of identity	If no economic benefit was gained or was attempted to be gained or if an economic benefit of less than $1,000 was gained or attempted to be gained, punishable by fine in an amount not to exceed $1,000, imprisonment in the county jail for a term not to exceed six months, or both. If an economic benefit of $1,000 or more was gained or attempted to be gained, punishable by fine an amount not to exceed $10,000, imprisonment in a state prison for a term not to exceed 10 years, or both.
Nebraska	28-608	Criminal impersonation; penalty; restitution	Class II misdemeanor if no credit, money, goods, services, or other thing of value was gained or was attempted to be gained, or if the credit, money, goods, services, or other thing of value that was gained or was attempted to be gained was less than $200. Any second conviction under this subdivision is a Class I misdemeanor, and any third or subsequent conviction under this subdivision is a Class IV felony. Class I misdemeanor if the credit, money, goods, services, or other thing of value that was gained or was attempted to be gained was

State	Statutory Citation	Title	Penalty
			$200 or more but less than $500. Any second or subsequent conviction under this subdivision is a Class IV felony. Class IV felony if the credit, money, goods, services, or other thing of value that was gained or was attempted to be gained was $500 or more but less than $1,500. Class III felony if the credit, money, goods, services, or other thing of value that was gained or was attempted to be gained was $1,500 or more.
Nevada	205.463 205.465	Obtaining and using personal identifying information of another person to harm person or for unlawful purpose. Possession or sale of document or personal identifying information to establish false status or identity	Category B felony or Category E felony Category C felony
New Hampshire	638:25 to 638:27	Identity fraud	Class A felony
New Jersey	2C:21-17	Impersonation; theft of identity; disorderly persons offense, crime	Guilty of a crime of the second degree if the pecuniary benefit, the value of the services received, the payment sought to be avoided or the injury or fraud perpetrated on another is $75,000 or more. Guilty of a crime of the third degree if the pecuniary benefit, the value of the services received, the payment sought to be avoided or the injury or fraud perpetrated on another is at least $500 but is less than $75,000. Guilty of a crime of the fourth degree if the pecuniary benefit, the value of the services received, the payment sought to be avoided or the injury or fraud perpetrated on another is at least $200 but is less than $500
New Mexico	30-16-24.1	Theft of identity	Misdemeanor
New York	Penal Code 190.77 to 190.84	Offenses involving theft of identity	190.78 Class A misdemeanor 190.79 Class E felony 190.80 Class D felony 190.81 Class A misdemeanor 190.82 Class E felony 190.83 Class De felony
North Carolina	14-113.20 to 14-113.23	Financial identity fraud. Trafficking in stolen identities	Felony
North Dakota	12.1-23-11	Unauthorized use of personal identifying information - Penalty	Class C felony
Ohio	2913.49	Identity fraud	First degree misdemeanor unless: If the value of the credit, property, services, debt, or other legal obligation involved in the violation or course of conduct is $500 or more and is less than $5,000, identity fraud is a felony of the fourth degree. If the value of the credit, property, services, debt, or other legal obligation involved in the violation or course of conduct is $5,000 or more and is less than $100,000, identity fraud is a felony of the third degree.

State	Statutory Citation	Title	Penalty
			If the value of the credit, property, services, debt, or other legal obligation involved in the violation or course of conduct is $100,00 or more, identity fraud is a felony of the second degree.
Oklahoma	21§1533.1	Identity theft	Felony
Oregon	165.800	Identity theft	Class C felony
Pennsylvania	18 Pa.C.S.A. §4120	Identity theft	If the total value involved is less than $2,000, the offense is a misdemeanor of the first degree.
			If the total value involved is $2,000 or more, the offense is a felony of the third degree.
			Regardless of the total value involved, if the offense is committed in furtherance of a criminal conspiracy, as defined in section 903, the offense is a felony of the third degree.
			Regardless of the total value involved, if the offense is a third or subsequent offense, the offense is a felony of the second degree
Rhode Island	11-49.1-1 to 11-49.1-5	Impersonation and Identity Fraud Act	First offense punishable by imprisonment for not more than three years and may be fined not more than $5,000, or both.
			Second offense punishable by imprisonment for not less than three years nor more than five years and shall be fined not more than $10,000, or both.
			Subsequent offense punishable by imprisonment for not less than five years nor more than 10 years and shall be fined not less than $15,000, or both.
South Carolina	16-13-500 to 16-13-530	Personal Financial Security Act	Felony
South Dakota	22-30A-3.1 to 22-30A-3.3	Identity theft	Misdemeanor
Tennessee	39-14-150	Identity theft	Class D felony
	39-16-303	Using a false identification	Class C misdemeanor
Texas	Penal Code 32.51	Fraudulent Use or Possession of Identifying Information	State jail felony
Utah	76-6-1101 to 76-6-1104	Identity fraud	Class A misdemeanor if the value of the credit, goods, services, or any other thing of value is less than $1,000.
			Third degree felony if the value of the credit, goods, services, or any other thing of value is or exceeds $1,000 but is less than $5,000.
			Second degree felony if the value of the credit, goods, services, or any other thing of value is or exceeds $5,000
Vermont	13 § 2030	Identity theft	A person who violates this section shall be imprisoned for not more than three years or fined not more $5,000.00, or both. A person who is convicted of a second or subsequent violation of this section involving a separate scheme shall be imprisoned for not more than ten years or fined not more than $10,000.00, or both.
Virginia	18.2-186.3	Identity theft; penalty; restitution; victim assistance	Class 1 misdemeanor
			Any violation resulting in financial loss of greater than $200 shall be punishable as a Class 6 felony. Any second or subsequent conviction shall be punishable as a Class 6 felony. Any violation resulting in the arrest and detention of the person whose identification documents or identifying information were used to avoid summons, arrest, prosecution, or to impede a criminal investigation shall be punishable as a Class 6 felony.

State	Statutory Citation	Title	Penalty
Washington	9.35.001 to 9.35-902	Identity crimes	First degree Class B felony Second degree Class C felony
West Virginia	61-3-54	Taking identity of another person; penalty	Felony
Wisconsin	943.201	Misappropriation of personal identifying information or personal identification documents	Class H felony
Wyoming	6-3-901	Unauthorized use of personal identifying information; penalties; restitution	A misdemeanor punishable by imprisonment for not more than six months, a fine of not more than $750.00, or both, if no economic benefit was gained or was attempted to be gained, or if an economic benefit of less than $500.00 was gained or was attempted to be gained. A felony punishable by imprisonment for not more than 10 years, a fine of not more than $10,000.00, or both, if an economic benefit of $500.00 or more was gained or was attempted to be gained

2005 ENACTED IDENTITY THEFT LEGISLATION AS OF AUGUST 24, 2005

State	Bill Summary
Arizona	H.B. 2414 *Signed by governor 4/18/05, Chapter 136* Defines advertisement, computer software, damage, execute, intentionally deceptive, Internet, owner or operator, person, personally identifiable information, and transmit as they relate to this chapter. Prohibits any person from transmitting, through intentionally deceptive means, computer software and using the software to: 1) Change Internet control settings. 2) Collect personally identifiable information, including bank account numbers. 3) Prevent the operator's efforts to block the installation or execution of computer software. 4) Falsely claim that software will be disabled by the operator's actions. 5) Remove or disable security computer software installed on the computer. 5) Take control of the computer. Designates this to be a matter of statewide concern. Thus, the chapter will supersede regulations set forth by local governmental bodies. Allows the attorney general and a computer software provider or a Web site or trademark owner who is adversely affected to bring action against a violator to enjoin further violations or recover the greater of actual damages or one hundred thousand dollars for each separate violation. States that the number of violators must be based on the number of paragraphs violated. The court may increase the damages up to three times if the defendant has a pattern of violating the provisions of the bill. The court may also award costs and reasonable attorney fees to the prevailing party. S.B. 1017 *Signed by governor 4/18/05, Chapter 82* Adds premiums for long-term and critical care insurance, prepaid legal services, personal computer systems, and identity theft protection services to those payroll deductions that a state officer or employee may authorize as additional deductions. S.B. 1058 *Signed by governor 4/25/05, Chapter 190* Creates the crime of aggravated identity theft if a person knowingly takes, purchases, manufactures, records, possesses or uses personal identifying information of either: five or more persons or entities or a person or entity and causes a loss to a person/entity of $3,000 or more. Provides that proof of possession of the personal/entity identifying information of five or more persons/entities out of the course of regular business may give rise to an inference that the information was possessed for an unlawful purpose. Makes aggravated identity theft a Class 3 felony. Creates the crime of trafficking in the identity of another person or entity if a person knowingly sells, transfers or transmits personal/entity identifying information (real or fictitious) for an unlawful purpose or to cause loss, whether the person or entity actually suffers any economic loss. Makes trafficking in the identity of a person or entity a Class 2 felony. Exempts a violation of A.R.S. 4-241 by a person under 21 years of age from the penalties associated with identity theft (Class 4 felony), aggravated identity theft (Class 3 felony) and trafficking in the identity of another person (Class 2 felony). A.R.S. § 4-241 makes it a Class 1 misdemeanor if a person under 21 years old uses a fraudulent piece of identification to gain access to an establishment licensed to sell liquor. S.B. 1447 *Signed by governor 4/18/05, Chapter 114* Prohibits a person from soliciting identifying information by representing that they are from an on-line business when they are not approved to do so by the on-line business. Defines pertinent terms. Prohibits any person from using a web page or electronic mail message to request identifying information by representing itself as an on-line business without the authority or approval of the on-line business. Allows the attorney general, a person engaged in the business of providing Internet access service to the public, or a person who owns a Web page or trademark that is adversely affected by a violation to bring action as follows: A) To enjoin further violations. B) To recover the greater of actual damages or $500,000 for each violation. C) Permits the attorney general to also recover reasonable attorney fees and costs. Stipulates that if the court determines there is a pattern of violations, the court may increase the damage award to not more than three times the amount otherwise outlined. Prescribes that multiple violations resulting from one act shall constitute a single violation. Classifies a violation as a Class 5 felony (1.5 years / $150,000).
Arkansas	H.B. 1354 *Signed by governor 2/25/05, Act 280* Clarifies that the offense of financial identity fraud pertains to the use of identifying information to open or create an account or financial resource. H.B. 1740 *Signed by governor 3/10/05, Act 744* Provides for the issuance of an identity theft passport by the attorney general to victims of financial identity fraud.

	H.B. 2094 *Signed by governor 3/21/05, Act 968* Prohibits persons convicted of financial identity fraud from being eligible to work with the developmentally disabled. H.B. 2904 *Signed by governor 4/15/05, Act 2255* Protects consumers from improper use of computer spyware.
California	A.B. 988 *Signed by governor 7/18/05, Chapter 53* Existing law specifies various offenses for purposes of defining criminal profiteering activity, and patterns of criminal profiteering activity. Existing law also provides for the forfeiture of specified assets for persons who engage in a pattern of criminal profiteering activity, upon conviction of an underlying offense, as specified. This bill adds to those specified offenses, the offense of theft of personal identifying information, as specified.
Colorado	H.B. 1347 *Signed by governor 6/1/05, Chapter 218* Concerns criminal penalties for the use of electronic devices for the purpose of identity theft.
Connecticut	H.B. 6831 *Signed by governor 6/2/05, Public Act 05-62* Specifically provides that the state statutes concerning financial privacy do not prevent 1) the disclosure of information to information networks accessed by financial institutions, other commercial enterprises and law enforcement authorities for the purpose of detecting or preventing against fraud, and 2) disclosures made to a victim of identity theft pursuant to the federal Fair Credit Reporting Act.
Delaware	S.B. 50 *Signed by governor 7/12/05, Chapter 162* Provides that a person is guilty of the crime of possession of burglar's tools or instruments facilitating theft when the person possesses any tool, instrument, or other thing adapted, designed, or commonly used for committing or facilitating the offense of identity theft, such as a credit card, driver license or other document issued in a name other than the name of the person who possesses the document.
Florida	H.B. 481 *Signed by governor 6/14/05, Chapter 229* S.B. 284 *Laid on table 5/3/05* Relates to the unlawful use of personal identification information; includes other information within the definition of the term "personal identification information"; defines the term "counterfeit or fictitious personal identification information"; revises criminal penalties regarding the offense of fraudulently using, or possessing with intent to fraudulently use, said information; requires business persons maintaining computerized data that includes personal information to provide notice of breaches of system security.
Georgia	S.B. 127 *Signed by governor 5/10/05, Act 389* Relates to forgery and fraudulent practices, so as to enact the "Georgia Computer Security Act of 2005." Prohibits certain deceptive acts and practices with regard to computers; requires certain notices be given prior to certain software or programs being loaded onto certain computers; requires certain functions be available in certain software; provides for certain exceptions; provides for civil and criminal penalties; provides for recovery of certain damages.
Hawaii	S.B. 1170 *Signed by governor 5/19/05, Act 65* Establishes a Hawaii Anti-Phishing Task Force to review other jurisdictions' activities on curtailing electronic commerce criminal activities. Requires the task force to submit a report and make recommendations prior to the 2006 regular session.
Idaho	S.B. 1156 *Signed by governor 3/31/05, Chapter 219* Amends existing law to provide that it is unlawful for any person to falsely assume or pretend to be a member of the armed forces of the United States or an officer or employee acting under authority of the United States or any department, agency or office thereof or of the state of Idaho or any department, agency or office thereof, and in such pretended character, seek, demand, obtain or attempt personal identifying information of another person; and provides felony penalties for such action.
Illinois	H.B. 265 *Signed by governor 7/19/05, Public Act 94-0245* Amends the Use of Credit Information in Personal Insurance Act. Defines extraordinary life events to include identity theft. H.B. 457 *Signed by governor 7/19/05, Public Act 94-0253* Provides that a prosecution for identity theft or aggravated identity theft may be commenced at any time (rather than within one year and six months after the commission of the offense if it is misdemeanor identity theft and within three years after commission of the offense if it is felony identity theft or aggravated identity theft). H.B. 2696 *Signed by governor 6/16/05, Public Act 94-0037* Provides that it is an unlawful practice for a person to deny credit or public utility service to or reduce the credit limit of a consumer solely because the consumer has been a victim of identity theft, if the consumer i) has provided a copy of an identity theft report as defined under the

	federal Fair Credit Reporting Act and implementing regulations (instead of a police report) evidencing the consumer's claim of identity theft; ii) has provide d a properly completed copy of a standardized affidavit of identity theft or an affidavit of fact that is acceptable to the person for that purpose; iii) has obtained placement of an extended fraud alert in his or her file maintained by a nationwide consumer reporting agency, in accordance with the requirements of the federal Fair Credit Reporting Act; and iv) is able to establish his or her identity and address to the satisfaction of the person providing credit or utility services. H.B. 2697 *Signed by governor 6/16/05, Public Act 94-0038* Amends the Criminal Code of 1961. Provides that a person who is not a party to a transaction that involves the use of a financial transaction device may not secretly or surreptitiously photograph, or otherwise capture or record, electronically or by any other means, or distribute, disseminate, or transmit, electronically or by any other means, personal identifying information from the transaction without the consent of the person whose information is photographed, or otherwise captured, recorded, distributed, disseminated, or transmitted. Provides that a violation is a Class A misdemeanor. H.B. 2699 *Signed by governor 6/16/05, Public Act 94-0039* Amends the Criminal Code of 1961. Increases the penalties for identity theft and aggravated identity theft by one class higher than the current law. H.B. 2700 *Signed by governor 6/17/05, Public Act 94-0051* Amends the Criminal Code of 1961. Provides that a person who commits the offense of identity theft or aggravated identity theft may be tried in any one of the following counties in which: 1) the offense occurred; 2) the information used to commit the offense was illegally used; or 3) the victim resides. Provides that if a person is charged with more than one violation of identity theft or aggravated identity theft and those violations may be tried in more than one county, any of those counties is a proper venue for all of the violations.
Iowa	H.F. 614 *Signed by governor 5/3/05* Protects owners and operators of computers from the use of spyware and malware that is deceptively or surreptitiously installed on the owner's or the operator's computer. S.F. 270 *Signed by governor 4/6/05* Relates to identity theft including criminal violations and damages recoverable in a civil action, provides for forfeiture of property and for certain rights of financial institutions, and provides for civil remedies.
Kansas	H.B. 2087 *Signed by governor 4/13/05* Changes 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. Establishes identity theft for economic benefit as a severity level 7 person felony, and identity theft for non-economic benefit as a class A non-person misdemeanor under Kansas criminal code.
Maine	L.D. 581 *Signed by governor 5/26/05, Chapter 243* Prohibits a consumer reporting agency from furnishing a consumer report or disclosing information about a consumer unless the consumer has authorized the disclosure if the consumer has given a copy of a police report to the consumer reporting agency that was prepared by a law enforcement agency in an investigation of identity theft involving the consumer.
Maryland	H.B. 800 *Signed by governor 5/26/05, Chapter 579* Requires a local law enforcement agency, after being contacted by a person who knows or reasonably suspects that the person is a victim of identity fraud, to promptly prepare and file a report of the alleged identity fraud and provide a copy of the report to the victim. H.B. 818 *Signed by governor 4/26/05, Chapter 241* Establishes a Task Force to Study Identity Theft; specifies the membership and duties of the Task Force; provides for the appointment of a Senate cochairman and House cochairman of the Task Force; provides for the staffing of the Task Force; prohibits a member of the Task Force from receiving compensation for serving on the Task Force; authorizes a member of the Task Force to receive reimbursement; requires a report to the General Assembly by December 31, 2006. S.B. 43 *Signed by governor 4/23/05, Chapter 242* Establishes a Task Force to Study Identity Theft; specifies the membership and duties of the Task Force; provides for the appointment of a Senate cochairman and House cochairman of the Task Force; provides for the staffing of the Task Force; prohibits a member of the Task Force from receiving compensation for serving on the Task Force; authorizes a member of the Task Force to receive reimbursement for specified expenses; requires a report to the General Assembly on or before December 31, 2006.

Montana	H.B. 110 *Signed by governor 3/24/05, Chapter 55* Creates an identity theft passport program. H.B. 732 *Signed by governor 4/28/05, Chapter 518* Adopts and revises laws to implement individual privacy and to prevent identity theft; requires a consumer reporting agency to block or expunge information on a report that results from a theft of identity; provides privacy protection provisions for credit card solicitations and renewals and telephone accounts; provides privacy protection for business records by requiring destruction of records; requires businesses to report a breach of computer security; requires a business that has an established business relationship with a customer and that has disclosed certain personal information to third parties to report that information to the customer; providing remedies and penalties for violation. S.J.R. 38 *Passed both houses 4/19/05* Requests the Legislative Council to designate an appropriate interim committee or direct sufficient staff resources to study issues related to identity theft, including jurisdictional issues regarding federal and state authority, the prosecution of Internet crimes, the role of credit reports and credit reporting agencies, the role of education for businesses and consumers, victim restitution, sales of personal information by third parties and direct marketing firms, and other identity theft issues raised during the study.
Nevada	A.B. 1, Special Session *Signed by governor 6/17/05, Chapter 6* Changes the effective date for A.B. 334 and amends the definition of personal information in S.B. 347. S.B. 304 *Signed by governor 6/8/05, Chapter 321* Authorizes the attorney general to issue identity theft passports to victims of identity theft; prescribes the manner in which victims of identity theft may use such passports; requires the attorney general to adopt regulations relating to the issuance of identity theft passports; authorizes the attorney general to accept gifts, grants and donations to carry out the provisions relating to the issuance of identity theft passports; makes an appropriation. S.B. 347 *Signed by governor 6/17/05, Chapter 485* Relates to personal identifying information; prohibits the establishment or possession of a financial forgery laboratory; enhances the penalties for crimes involving personal identifying information that are committed against older persons and vulnerable persons; requires the issuer of a credit card to provide a notice including certain information concerning its policies regarding identity theft and the rights of cardholders when issuing a credit card to a cardholder; requires data collectors to provide notification concerning any breach of security involving system data; making various other changes concerning personal identifying information; provides penalties; and provides other matters properly relating thereto.
New Mexico	S.B. 720 *Signed by governor 4/7/05, Chapter 296* Creates a new criminal offense known as obtaining identity by electronic fraud; increases a penalty.
North Dakota	H.B. 1211 *Signed by governor 3/30/05* Relates to unauthorized use of personal identifying information of a deceased individual; and provides a penalty. H.B. 1500 *Signed by governor 4/22/05* Provides for protection of victims of identity fraud; and provides a penalty. H.C.R. 3042 *Passed both houses 4/4/05* Directs the Legislative Council to study 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. S.B. 2251 *Signed by governor 4/22/05* Relates to requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form; relates to the unauthorized use of personal identifying information, penalties, and prosecution of offenses in multiple counties; jurisdiction in offenses involving conduct outside this state; and provides a penalty.
Ohio	H.B. 48 *Signed by governor 6/14/05, Session Law 22* Increases the penalty for identity fraud in certain circumstances, including when it is committed against an elderly person or disabled adult, modifies the affirmative defenses available for that offense, and creates the Identity Fraud Passport.
Rhode Island	H.B. 6191 *Effective without governor's signature 7/10/05, Public Law 225* Creates the "Rhode Island Identity Theft Protection Act of 2005", and establishes standards for such protection, and provides for penalties for violations of the act.

Texas	H.B. 982 *Signed by governor 5/27/05* Relates to posting a sign warning restaurant or bar employees against fraudulent use or possession of identifying information; provides a criminal penalty. H.B. 1098 *Signed by governor 6/17/05, Chapter 544* S.B. 326 Relates to using the Internet to obtain identifying information of another person for a fraudulent purpose; provides penalties. H.B. 1321 *Tabled 5/12/05* S.B. 122 *Signed by governor 6/17/05* Amends the Code of Criminal Procedure by requiring that a peace officer to whom an alleged violation of identity theft is reported make a written report that includes the name of the victim, suspect, if known, type of identifying information obtained, possessed, transferred, or used, and the results of the investigation. Sets forth provisions for prevention and punishment of identity theft and assistance to certain victims of identity theft. Imposes a civil penalty of at least $2,000 but not more than $50,000 for each identity theft violation and authorizes the attorney general to bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or a permanent or temporary injunction. Gives the attorney general the option to file in a district court in Travis County or in any county in which the offense occurred or where the victim lives. Authorizes the attorney general to recover reasonable expenses incurred in obtaining injunctive relief and civil penalties. Penalties collected by the attorney general under this section would be required to be deposited into the General Revenue Fund and could be appropriated only for the investigation and prosecution of other cases under Chapter 48 of the Code of Criminal Procedure. Sets out that no bond is required and gives the court authority to grant other equitable relief to protect victims. Gives a victim the option to file an application with the district court for the issuance of a court order to declare them a victim of identity theft. Information contained in the court order would be considered confidential. H.B. 1379 *Signed by governor 6/18/05, Chapter 1059* Makes communications by a seller of goods or services to a member of a law enforcement agency regarding an investigation of an identity theft violation inadmissible in a civil action. H.B. 1430 S.B. 327 *Signed by governor 6/17/05, Chapter 298* Prohibits the unauthorized collection or transmission of personally identifiable information, including Social Security number and credit card numbers, unauthorized transmission or modifications of computer settings, unauthorized interference with installation or disabling of computer software, damage, or any other deceptive act to obtain information from a consumer's computer. Provides the attorney general authority to bring suit to seek injunctive relief and recover civil penalties of an amount not to exceed $100,000 for each violation of this statute as well as reasonable attorneys fees and costs. In addition, the bill adds a definition for "cause computer software to be copied;" provides clean up language to incorporate this definition; and adds additional provisions to protect consumers. The bill also adds additional provisions for private causes of action. H.B. 2013 *Tabled 5/5/05* H.B. 3212 S.B. 99 *Signed by governor 5/20/05* Prohibits a lender or any other person involved in a transaction from denying credit or loans or restricting or limiting the credit extended to a person based on the person being a victim of identity theft. Provides victims of identity theft with another tool to mend their credit histories and bring state law in line with the Federal Equal Credit Opportunity Act, which prohibits creditors from discriminating against credit applicants who exercise their rights, in good faith, under the Fair Credit Billing Act.
Utah	S.B. 118 *Signed by governor 3/11/05, Chapter 101* Includes the personal identifying information of persons who are deceased in the statute that prohibits the use of identifying information to commit identity fraud crimes.
Virginia	H.B. 2471 *Signed by governor 3/26/05, Chapter 827* S.B. 1163 *Signed by governor 3/26/05, Chapter 761* Updates the Virginia Computer Crimes Act to include recommendations made by the 2004 joint study on Computer Crimes by the Joint Commission on Technology and Science and Virginia State Crime Commission. Modernizes definitions of "computer", "using a computer" and "without authority" to comport with changing technology. Revises provisions regarding computer trespass, a Class 1 misdemeanor, unless the damage to the property of another is $1,000 ($2,500 under current law) or more, in which case it is a Class 6 felony. Provisions

	regarding computer invasion of privacy are rewritten to include unauthorized gathering of identifying information and Class 6 penalties added for persons with previous convictions, selling or distributing the information to another or using the information in the commission of another crime. Adds as a new Class 6 felony using a computer to fraudulently gather identifying information of another (phishing), unless the information is sold or distributed to another or the information is used in the commission of another crime, in which case it is a Class 5 felony. Statute of limitation and venue provisions are relocated in the Code. H.B. 2631 *Signed by governor 3/26/05, Chapter 837* Revises provisions in the Virginia Computer Crimes Act relating to computer fraud and redefines computer invasion of privacy by including the unauthorized gathering of identifying information and punishes subsequent offenses and transferring the information to another or use of the information in the commission of another crime as a Class 6 felony. Currently, the offense is punishable as a Class 1 misdemeanor. Additionally, the fraudulent gathering of such information is punished as a Class 6 felony, a new crime, and transferring the information to another or use of the information in the commission of another crime is a Class 5 felony. S.B. 1147 *Signed by governor 3/26/05, Chapter 760* Makes it a Class 6 felony to fraudulently obtain, record, or access from a computer the following identifying information of another: (i) social security number; (ii) driver's license number; (iii) bank account numbers; (iv) credit or debit card numbers; (v) personal identification numbers (PIN); (vi) electronic identification codes; (vii) automated or electronic signatures; (viii) biometric data; (ix) fingerprints; (x) passwords; or (xi) any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services. Any person who sells or distributes such information or uses it to commit another crime is guilty of a Class 5 felony.
Washington	H.B. 1012 *Signed by governor 5/17/05, Chapter 500* Declares that it is unlawful for a person who is not an owner or operator to transmit computer software to the owner or operator's computer with actual knowledge or with conscious avoidance of actual knowledge and to use such software to do any of the following: (1) Modify, through intentionally deceptive means, settings that control any of the following: (a) The page that appears when an owner or operator launches an Internet browser or similar computer software used to access and navigate the Internet; (b) the default provider or web proxy the owner or operator uses to access or search the Internet; and (c) the owner or operator's list of bookmarks used to access web pages; (2) Collect, through intentionally deceptive means, personally identifiable information: (a) Through the use of a keystroke-logging function that records all keystrokes made by an owner or operator and transfers that information from the computer to another person; (b) in a manner that correlates such information with data respecting all or substantially all of the Web sites visited by an owner or operator, other than Web sites operated by the person collecting such information; and (c) described in section 1(10) (d), (e), or (f)(i) or (ii) of this act by extracting the information from the owner or operator's hard drive; (3) Prevent, through intentionally deceptive means, an owner or operator's reasonable efforts to block the installation or execution of, or to disable, computer software by causing the software that the owner or operator has properly removed or disabled automatically to reinstall or reactivate on the computer; (4) Intentionally misrepresent that computer software will be uninstalled or disabled by an owner or operator's action; and (5) Through intentionally deceptive means, remove, disable, or render inoperative security, antispyware, or antivirus computer software installed on the computer. Declares that it is unlawful for a person who is not an owner or operator to transmit computer software to the owner or operator's computer with actual knowledge or with conscious avoidance of actual knowledge and to use the software to do any of the following: (1) Take control of the computer by: (a) Accessing or using the modem or Internet service for such computer to cause damage to the computer or cause an owner or operator to incur financial charges for a service that is not authorized by the owner or operator; (b) opening multiple, sequential, stand-alone advertisements in the owner or operator's Internet browser without the authorization of an owner or operator and that a reasonable computer user cannot close without turning off the computer or closing the Internet browser; (2) Modify any of the following settings related to the computer's access to, or use of, the Internet: (a) Settings that protect information about the owner or operator in order to steal the owner or operator's personally identifiable information; and (b) security settings in order to cause damage to a computer; and (3) Prevent an owner or operator's reasonable efforts to block the installation of, or to disable, computer software by doing any of the following: (a) Presenting the owner or operator with an option to decline installation of computer software with knowledge that, when the option is selected, the installation nevertheless proceeds; and (b) falsely representing that computer software has been disabled. Declares that it is unlawful for a person who is not an owner or operator to do any of the following with regard to the owner or operator's computer: (1) Induce an owner or operator to install a computer software component onto the computer by intentionally misrepresenting the extent to which installing the

software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content; and (2) Deceptively cause the execution on the computer of a computer software component with the intent of causing an owner or operator to use the component in a manner that violates any other provision of this act. Authorizes a person who is injured under this act to bring a civil action in the superior court to enjoin further violations, or to seek up to $1,000 per violation, or actual damages, whichever is greater. The injured individuals may not bring their cause of action as a class action. Nothing in this section prohibits the attorney general from bringing a class action suit under chapter 19.86 RCW. Provides that, in an action under this act, a court may increase the damages up to three times the damages allowed if the defendant has engaged in a pattern and practice of violating this act. The court may also award costs and reasonable attorneys' fees to the prevailing party. Declares an intent that this act is a matter of statewide concern. This act supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding spyware and notices to consumers from computer software providers regarding information collection.

H.B. 1888 *Signed by governor 3/10/05, Chapter 378*
Prohibits a person from soliciting, requesting, or taking any action to induce another person to provide personally identifying information by means of a Web page, electronic mail message, or otherwise using the Internet by representing oneself, either directly or by implication, to be a business or individual, without the authority or approval of such business or individual. Defines "personally identifiable information" as any of the following types of information: 1) Social Security number; 2) driver's license number; 3) bank account number; 4) credit or debit card number; 5) personal identification number; 6) automated or electronic signature; 7) unique biometric data; 8) account passwords; or 9) any other piece of information that can be used to access an individual's financial accounts or to obtain goods or services. Allows an injured person to bring a civil action against a person or entity that directly violates these provisions and seek damages of up to $500 per violation, or actual damages, whichever is greater. Allows an Internet Service Provider, an owner of a Web page, or a trademark owner to bring a civil action against a person or entity that directly violates these provisions and seek to enjoin further violations, and may also recover $5,000 per violation, or actual damages, whichever is greater. In addition, the court may increase the damage award up to three times (up to $15,000) if the defendant has engaged in a pattern and practice of engaging in the prohibited activities. The court may also award costs and reasonable attorneys' fees to the prevailing party. A violation of these provisions is defined as an unfair or deceptive act for purposes of applying the Consumer Protection Act.

S.B. 5939 *Signed by governor 5/10/05, Chapter 366*
Requires police and sheriff's departments to provide a police report or original incident report at the request of any consumer claiming to be a victim of identity theft.