



Senate Fiscal Agency
P. O. Box 30036
Lansing, Michigan 48909-7536



BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986
TDD: (517) 373-0543

Senate Bill 220 (Substitute S-2 as passed by the Senate)
Senate Bill 657 (as passed by the Senate)
Senate Bill 792 (Substitute S-4 as passed by the Senate)
Senate Bill 793 (Substitute S-1 as passed by the Senate)
Senate Bill 794 (Substitute S-2 as passed by the Senate)
Senate Bill 795 (Substitute S-4 as passed by the Senate)
Senate Bill 797 (as passed by the Senate)
Senate Bill 798 (Substitute S-1 as passed by the Senate)
Senate Bill 803 (as passed by the Senate)
Senate Bill 1384 (as reported without amendment)

Sponsor: Senator Valde Garcia (S.B. 220)
Senator Cameron S. Brown (S.B. 657)
Senator Michael D. Bishop (S.B. 792)
Senator Gerald Van Woerkom (S.B. 793)
Senator Laura M. Toy (S.B. 794 & 1384)
Senator Nancy Cassis (S.B. 795)
Senator Tom George (S.B. 797)
Senator Alan Sanborn (S.B. 798)
Senator Alan L. Cropsey (S.B. 803)

Committee: Economic Development, Small Business and Regulatory Reform (S.B. 220)
Judiciary (S.B. 657, 792-795, 797, 798, 803 & 1384)

Date Completed: 9-23-04

RATIONALE

Identity theft occurs when someone uses another's personal information, such as name, address, Social Security number, or bank or credit card account number, without that person's knowledge or consent, to commit fraud or other crimes. For instance, by obtaining a person's Social Security number, an identity thief could obtain credit cards and loans in that person's name, open utility accounts, rent an apartment or house, secure cellular telephone service, or purchase a car or home, without the knowledge of the person whose name and identity information were used. Identity theft has been widely characterized as the fastest growing crime in the United States. According to a report of the Federal Trade Commission (FTC), it received 214,905 identity theft complaints in 2003, an increase from 161,836 complaints received in 2002 and 86,212 in 2001 ("National and State Trends in Fraud & Identity Theft, January-December 2003", FTC, January 22,

2004.) Of those identity theft complaints, 6,566 were from Michigan victims in 2003.

The Michigan Penal Code currently prohibits a person from obtaining or attempting to obtain another person's personal identifying information with the intent to use that information unlawfully, without the other person's authorization, for the purpose of obtaining financial credit, buying or otherwise obtaining real or personal property, obtaining employment, obtaining access to medical records, or committing any illegal act. Some people believe, however, that Michigan law should include more comprehensive protections against identity theft. They contend that the law also should include measures to protect a consumer's financial account numbers, Social Security number, and medical benefits number; clarify court jurisdiction over identity theft cases; and allow a victim to secure a certificate of victimization to

protect him or her against the consequences of an identity thief's actions.

CONTENT

Senate Bills 220 (S-2), 657, and 798 (S-1) would amend the Michigan Consumer Protection Act to prohibit all of the following:

- Issuing or delivering to a consumer a receipt that showed any part of a credit or debit card's expiration date or more than the last four digits of the account number.
- Requiring a consumer to disclose his or her Social Security number as a condition of sale, unless the transaction involved an extension of credit or related to an employer-provided health-related benefit, or disclosure was required or authorized by law.
- Denying credit or public utility service to, or reducing the credit limit of, a consumer who was an identity theft victim.

Senate Bill 792 (S-4) would create the "Identity Theft Protection Act" to do all of the following:

- Prohibit a person from committing identity theft; obtaining or possessing another person's personal identifying information with the intent to use it to commit identity theft or another unlawful act; selling or transferring another person's personal identifying information; or falsifying a victim certificate or knowingly creating, possessing, or using a false victim certificate issued under Senate Bill 794.
- Specify exceptions to the identity theft violations.
- Prohibit certain actions in the conduct of trade or commerce.
- Allow a law enforcement agency, financial institution, or identity theft victim to obtain copies of vital records, if necessary to enforce the proposed Act or investigate or prevent identity theft.
- Create an "Identity Theft Advisory Board" to recommend to the Legislature statutory changes related to identity theft issues.
- Repeal a section of the Michigan Penal Code that prohibits obtaining

or attempting to obtain another person's personal identity information with the intent to use it unlawfully for certain purposes.

Senate Bills 793 (S-1), 794 (S-2), 797, and 803 would amend the Code of Criminal Procedure to do all of the following:

- Specify that a violation of the proposed Identity Theft Protection Act could be prosecuted in the jurisdiction in which the offense occurred, in which the information used to commit the violation was illegally used, or in which the victim lived.
- Allow an identity theft victim to secure from the county prosecuting attorney a certificate stating that he or she was an identity theft victim.
- Include in the sentencing guidelines a violation of the proposed Identity Theft Protection Act.
- Extend the period of limitations for identity theft, when a previously unidentified person who provided evidence was identified.

Senate Bill 795 (S-4) would create the "Social Security Number Privacy Act" to prohibit certain actions regarding the disclosure, display, or use of a person's Social Security number.

Senate Bill 1384 would amend the Crime Victim's Rights Act to allow a victim of identify theft to obtain a police report.

Senate Bill 792 (S-4) is tie-barred to Senate Bills 657, 793, and 794; Senate Bills 793 (S-1), 794 (S-2), 797, and 798 (S-1) all are tie-barred to Senate Bill 792. Senate Bill 1384 is tie-barred to Senate Bill 794.

Under Senate Bill 792 (S-4), "identity theft" would mean any unauthorized use of another person's personal identifying information either to obtain credit, goods, services, money, property, medical records or information, or employment, except as otherwise authorized under the bill, or to commit any other unlawful act. "Personal identifying information" would mean a name, number, or other information that could be used to identify a specific person or provide access to a person's financial accounts, including a person's name,

address, telephone number, driver license or State personal identification card number, Social Security number, place of employment, employee ID number, employer or taxpayer ID number, government passport number, health insurance ID number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or password, stock or other security certificate or account number, credit card number, or medical records or information.

Senate Bill 220 (S-2)

The Michigan Consumer Protection Act provides that unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce are unlawful, and includes a list of such practices. The bill would include in that list issuing or delivering to a consumer a receipt that displayed any part of a credit or debit card's expiration date or more than the last four digits of the consumer's account number, if a credit card or debit card were used for payment in a consumer transaction. This prohibition would not apply if the only receipt issued were one on which the account number or expiration date was handwritten, mechanically imprinted, or photocopied.

The prohibition would apply to any consumer transaction that occurred on or after the bill's effective date. If a credit or debit card receipt were printed by an electronic device, however, the prohibition would apply to a transaction that occurred using that device only after one or the following dates, as applicable:

- If the electronic device were placed in service after the bill's effective date, 60 days after that date or the date the device was placed in service, whichever was later.
- July 1, 2006, if the electronic device were in service on or before the bill's effective date.

Also, it would be an unfair trade practice for a person to require a consumer to disclose his or her Social Security number as a condition to selling goods or providing a service to the consumer, unless the transaction included an extension of credit to the consumer or disclosure was required by State or Federal law.

Senate Bill 657

The bill would make it an unfair trade practice for a person to require a consumer to disclose his or her Social Security number as a condition to selling goods or providing a service to the consumer, unless the transaction included an extension of credit to the consumer or related to the administration of an employer-provided health-related benefit, or disclosure was required or authorized by applicable State or Federal statute, rule, or regulation.

Senate Bill 792 (S-4)

Identity Theft Penalty

The bill would prohibit a person from doing any of the following:

- Committing or attempting to commit identify theft.
- Except as otherwise provided by the bill, obtaining or possessing or attempting to obtain or possess another person's personal identifying information with the intent to use it to commit identity theft or another unlawful act.
- Except as otherwise provided by the bill, selling or transferring or attempting to sell or transfer another person's personal identifying information, if the person knew or had reason to know that the specific intended recipient would use, attempt to use, or further transfer the information to another person for the purpose of committing identity theft or another unlawful act.
- Falsifying a victim certificate or knowingly creating, possessing, or using a false victim certificate.

A violation would be a felony punishable by up to five years' imprisonment, a maximum fine of \$10,000, or both.

The bill specifies that this prohibition would not prohibit a person from lawfully obtaining or attempting to obtain another person's personal identifying information under either of the following circumstances:

- Pursuant to the discovery process in a civil or criminal action, an administrative proceeding, or an arbitration proceeding.
- For the purpose of detecting, preventing, or deterring a financial or other crime, identity theft, or the funding of a criminal activity.

The identity theft prohibition also would not apply to a violation of a statute or rule administered by a regulatory board or officer acting under State or Federal authority that conferred exclusive jurisdiction on that board or officer to authorize, prohibit, or regulate certain transactions and conduct. This would include, but would not be limited to, a State or Federal statute or rule governing a financial institution and the Insurance Code, if the act were committed by a person subject to and regulated by the statute or rule, or by another person who contracted with the regulated person to use personal identifying information and who had similar privacy protection policies making the information confidential.

The identity theft prohibition would apply regardless of whether the victim or intended victim was alive or dead at the time of the violation.

The bill states that it would not prohibit a person from being charged with, convicted of, or sentenced for any other violation committed by using information obtained in violation of the bill.

Prohibited Practices

The bill would prohibit a person from doing any of the following in the conduct of trade or commerce:

- Denying credit or public utility service to or reducing the credit limit of a consumer solely because he or she was a victim of identity theft, if the person had prior knowledge that the consumer was an identity theft victim. (A consumer would be presumed to be a victim if he or she possessed a valid victim certificate issued under the Code of Criminal Procedure, as proposed by Senate Bill 794.)
- Soliciting to extend credit to a consumer who did not have an existing line of credit, or had not had or applied for a line of credit within the past year, through the use of an unsolicited check that included personal identifying information other than the recipient's name, address, and a partial, encoded, or truncated personal identifying number.
- Soliciting to extend credit to a consumer who did not have a current credit card, or had not had or applied for a credit card within the past year, through the use of an unsolicited credit card sent to the consumer.

- Extending credit to a consumer without exercising procedures to verify his or her identity. (Compliance with U.S. Treasury regulations under the USA Patriot Act would be considered compliance with this requirement.)

A knowing or intentional violation of this prohibition would be a misdemeanor punishable by up to 30 days' imprisonment, a maximum fine of \$100, or both. The bill states that this penalty would not affect the availability of any civil remedy for a violation of the proposed Identity Theft Protection Act, the Michigan Consumer Protection Act, or any other State or Federal law.

In addition to any other penalty or remedy under the proposed Act or the Michigan Consumer Protection Act, for a violation involving a solicitation to extend credit, a credit card issuer, financial institution, or lender would be liable for the amount of the financial instrument and any fees assessed to the consumer, and for any credit card charges and interest or finance charges, if the instrument or credit card were used by an unauthorized user. The consumer would not be liable for those amounts, fees, or charges.

Vital Records

The bill would allow a law enforcement agency, financial institution, or identity theft victim to obtain copies of a vital record from a local registrar, if necessary to enforce the proposed Act or investigate or prevent identity theft. The registrar could charge a financial institution or identity theft victim for the actual costs of copying vital records.

Advisory Board

The bill would create an Identity Theft Advisory Board. The board's five members would be the Governor, the Attorney General, the Secretary of State, the Senate Majority Leader, and the Speaker of the House; or the designee of one of those individuals. The Attorney General would serve as the board's chairperson. The board annually would have to report to the Senate and House standing committees with jurisdiction over issues relating to identity theft, with any recommendations for statutory changes. The board would have to study data from identity theft cases in Michigan.

Repealer

The bill would repeal Section 285 of the Michigan Penal Code (MCL 750.285). That section prohibits a person from obtaining or attempting to obtain personal identity information of another person with the intent to use it unlawfully, without the person's authorization, for any of the following purposes:

- Obtaining financial credit.
- Purchasing or otherwise obtaining or leasing any real or personal property.
- Obtaining employment.
- Obtaining access to medical records or information contained in them.
- Committing any illegal act.

A violation is a felony, punishable by up to five years' imprisonment, a maximum fine of \$10,000, or both.

The prohibition does not apply to a person who obtains or attempts to obtain another person's personal identity information pursuant to the discovery process of a civil action, an administrative proceeding, or an arbitration proceeding.

Under Section 285, "personal identity information" means any of the following information of another person:

- A Social Security number.
- A driver license number or State personal ID card number.
- Employment information.
- Information regarding any financial account held by another person, including a saving or checking account number, a financial transaction device account number, a stock or other security certificate or account number, and a personal information number for any of those accounts.

Senate Bill 793 (S-1)

Under the bill, a violation of the proposed Identity Theft Protection Act or a violation of law committed in furtherance of or arising from the same transaction as a violation of that Act, could be prosecuted in the jurisdiction in which the offense occurred, the jurisdiction in which the information used to commit the violation was illegally used, or the jurisdiction in which the victim lived. If a person were charged with more than one identity theft violation and those

violations could be prosecuted in more than one jurisdiction, any of those jurisdictions would be a proper jurisdiction for all of the violations.

Senate Bill 794 (S-2)

Under the bill, an individual who was the victim of identity theft could apply to the county prosecuting attorney having jurisdiction over the violation for a certificate stating that he or she was an identity theft victim. Before submitting an application, the individual would have to file a complaint regarding the violation with a law enforcement agency having jurisdiction over the violation. If an individual applied properly, the prosecuting attorney would have to issue a certificate without charge. Before issuing the certificate, the prosecuting attorney could request the law enforcement agency receiving the complaint to investigate the violation. A person who knowingly made a material false statement on an application would be guilty of perjury.

A certificate would have to be on a form prescribed by the Department of State Police and provided free of charge to county prosecuting attorneys. A prosecuting attorney would have to maintain an application on file for two years.

A county prosecutor could revoke a certificate by mailing a written notice of revocation to the applicant, who would have to return the certificate within 14 days. Knowingly failing to do so would be a misdemeanor punishable by up to 93 days' imprisonment and/or a maximum fine of \$500.

A certificate issued under the bill would be an official State record.

Senate Bill 795 (S-4)

Except as otherwise provided under the proposed Social Security Number Privacy Act, the bill would prohibit a person from knowingly doing any of the following with all or more than four sequential digits an employee's, student's, or other individual's Social Security number:

- Disclosing them to a third party.
- Publicly displaying or including them in any documents or information mailed or otherwise sent to an individual if the

digits were visible on or from outside of the envelope packaging.

- Using them as the primary identification number for the individual or his or her account, including printing or using them on any membership card. (If a person implemented a plan or schedule for eliminating the use of all or more than four sequential digits by a certain date, this provision would not apply to that person until January 1, 2006, or the plan's or schedule's completion date, whichever was earlier.)
- Requiring an individual to use or transmit the digits over the Internet or a compute system or network unless the connection was secure or the transmission was encrypted, and a password or other unique personal ID number or other authentication device was first required to gain access to the website.
- Including the digits in any document or information mailed to an individual, unless State or Federal law, rule, or regulation authorized, permitted, or required that a Social Security number appear in the document; the document was sent as part of an application or enrollment process; or the document was sent to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the Social Security number of an individual with an account, contract, or policy.

The bill's prohibition would not apply under any of the following circumstances:

- An individual or his or her parent or legal guardian consented to a disclosure of the individual's number to a third party or to the use of the number in a mailed document or information after being fully informed of the reasons for the disclosure or use.
- A disclosure, display, or other use of the individual's Social Security number was authorized or required by State or Federal statute, rule, or regulation or by court order or rule.
- A law enforcement agency disclosed an individual's Social Security number as part of a criminal investigation or prosecution.
- A county register of deeds office disclosed or distributed a copy of a public record filed or recorded with the office that included an individual's Social Security number, to a person entitled to that documentation.

The prohibition against disclosure of a Social Security number to a third party would not apply to disclosures by any of the following to a third party who had a written privacy policy making use of the number confidential:

- A person providing health benefits or an employment benefit plan or payroll plan.
- A person when determining an individual applicant's suitability for an employment opportunity.
- A person in lawful pursuit or enforcement of a person's legal rights, including the audit, collection, investigation, or transfer of a debt, claim, receivable, or account, or an interest in a receivable or account.
- A person who was subject to and regulated by a statute administered by a regulatory board or officer acting under State or Federal authority that conferred exclusive jurisdiction on that board or officer to authorize, prohibit, or regulate certain transactions and conduct. (These statutes would include, but not be limited to, any State or Federal statute governing a financial institution and the Insurance Code.)
- A vendor or contractor of a person described above.

In regard to disclosure by a person subject to regulatory statute, the disclosure would have to be either for verification of identity or other administrative purposes related to a transaction, product, or service, including investigating and checking the individual's credit, claim, or driving history; or for detecting, preventing, or deterring a financial crime, identity theft, or the funding of criminal activity.

A knowing violation of the proposed Act would be a misdemeanor punishable by up to 93 days' imprisonment, a maximum fine of \$1,000, or both. Also, an individual could bring a civil action against a person who violated the Act and could recover actual damages or \$1,000, whichever was greater, plus reasonable attorney fees.

Senate Bill 797

The bill would include in the sentencing guidelines a violation of the proposed Identity Theft Protection Act. Identity theft would be a Class E felony against the public order, with a statutory maximum penalty of five years' imprisonment.

The bill also would delete from the sentencing guidelines the offense of obtaining personal information without authorization (which Senate Bill 792 would repeal). That offense is a Class E property felony, with a statutory maximum penalty of five years' imprisonment.

Senate Bill 798 (S-1)

The bill would prohibit as an unfair trade practice denying credit or public utility service to, or reducing the credit limit of, a consumer who was a victim of identity theft under the proposed Identity Theft Protection Act, if the person doing so had prior knowledge that the consumer was a victim of identity theft. A person would be presumed to be a victim of identity theft if he or she possessed a valid victim certificate under the Code of Criminal Procedure (as proposed by Senate Bill 794).

Senate Bill 803

The bill would extend the period of limitations for identity theft, when a previously unidentified person who provided evidence was identified. ("Identity theft" would mean that term as defined in the proposed Identity Theft Protection Act.)

Under the Code of Criminal Procedure, an indictment must be found and filed within six years after an offense is committed (except as provided for particular offenses). The bill specifies that an indictment for identity theft or attempted identity theft could be found and filed within six years after the offense was committed. If evidence of an identity theft violation were determined to be from an unidentified individual, however, an indictment could be found and filed at any time after the offense was committed, but not more than six years after the individual was identified. ("Identified" would mean that the individual's legal name was known.)

Senate Bill 1384

The bill specifies that, to facilitate compliance with Federal law (15 USC 1681g), a bona fide victim of identity theft would be entitled to a police report from a law enforcement agency in a jurisdiction where the alleged violation of identity theft could be prosecuted as provided under MCL 762.10c (the section of the Code of Criminal Procedure proposed by Senate Bill 793).

The bill would insert the same language in each of the Act's three articles. Article I deals with felonies, Article II involves juvenile offenses, and Article III applies to serious misdemeanors.

(Under 15 USC 1681g, every consumer reporting agency, upon request, must clearly and accurately disclose certain information to consumers. This includes information in the consumer's file at the time of the request, the sources of the information, identification of each consumer who procured a consumer report, and a record of all inquiries received by the agency during the one-year period preceding the request that identified the consumer in connection with a credit or insurance transaction but was not initiated by the consumer.)

MCL 445.903 (S.B. 220, 657, & 798)
Proposed MCL 762.10c (S.B. 793)
Proposed MCL 776.23 (S.B. 794)
MCL 777.14h & 777.16o (S.B. 797)
MCL 767.24 (S.B. 803)
Proposed MCL 780.754a et al. (S.B. 1384)

ARGUMENTS

(Please note: The arguments contained in this analysis originate from sources outside the Senate Fiscal Agency. The Senate Fiscal Agency neither supports nor opposes legislation.)

Supporting Argument

A victim of identity theft can be devastated by the crime and might not even be aware that he or she has been targeted until well after the violation has occurred. According to the Director of the FTC's Bureau of Consumer Protection, unlike most crimes, in which the victim may be immediately aware of the violation, "[I]dentity theft is often silent and invisible. Identity thieves do not need direct contact with their victims. All they need is access to some key components of a victim's personal information, which, for most Americans, may be maintained and used by numerous different public and private entities" (testimony before the U.S. Senate Judiciary Committee's Subcommittee on Technology, Terrorism, and Government Information, March 20, 2002). The Bureau Director also testified that access to personal information, whether through legal or illegal means, is the key to identity theft.

According to "Consumer Sentinel", the FTC's fraud and identity theft complaint database, the most common identity theft complaints received in 2003 related to credit card fraud, phone or utility fraud, bank fraud, employment-related fraud, government document or benefit fraud, and loan fraud, in that order. Typically, an identity thief obtains personal information, such as a person's Social Security number, and then opens accounts in that person's name and runs up charges on the accounts. A victim of identity theft can spend years trying to recover from the consequences of the crime. Loans and other credit accounts opened in the victim's name, or legitimate accounts tapped into by the perpetrator, go delinquent and the victim's credit rating is sullied. Also, new accounts may be opened long after the crime is realized and the victim believes he or she has corrected fraudulent records. Reportedly, the names of some victims have even been discovered in criminal records for acts committed by identity thieves.

In recent years, both Federal and Michigan law have recognized the significance of the problem by prohibiting, and prescribing criminal penalties for, actions that constitute identity theft. Under the Identity Theft and Assumption Deterrence Act of 1998, it is a Federal crime to use another person's means of identification with intent to commit, aid, or abet any violation of Federal law or any felony under any applicable state or local law (18 USC 1028). In Michigan, Public Act 386 of 2000 added Section 285 to the Michigan Penal Code to prohibit a person from obtaining or attempting to obtain the personal identity information of another person for unlawful purposes (described in **CONTENT**, above).

While those statutes prohibit activity that constitutes identity theft, penalize criminals after the fact, and perhaps deter some would-be identity thieves, the bills would help to prevent identity theft from occurring in the first place. In addition to recodifying and expanding upon the penalties enacted by Public Act 386, the bills would prohibit certain activities regarding soliciting the extension of credit to someone who did not have an existing account or had not recently applied for a line of credit; denying credit or utility service to an identity theft victim; extending credit to a consumer without exercising procedures to verify the consumer's identity in compliance with

Federal law; and issuing a receipt that showed an entire account number.

Response: According to the director of the Michigan State University (MSU) Identity Theft Lab, the legislation could do more to protect individuals' personal identifying information and aid enforcement of identity theft laws. In a *Lansing State Journal* opinion column, she suggested that "an identity theft 'alert code' be placed on the driver's license of identity theft victims similar to the fraud alerts that are placed on credit bureau reports" ("ID Theft Measure Needs Revamp", 11-9-03). In addition, she proposed that "post office businesses, financial institutions and other places where ATMs are located should be required to store the video they routinely capture for a minimum of two years—the time it often takes to uncover identity theft networks". These additional measures could help stop identity thieves before they invade the lives of unsuspecting victims.

Supporting Argument

The law should require private and public entities to reduce or eliminate the use of Social Security numbers as universal identifiers. Many services, from health insurance providers to utility companies, to video rental stores, routinely use a person's Social Security number to index his or her account. When the Social Security system was created, its numbers were not meant to be used in this manner and these practices should at least be limited. By restricting the use, display, and disclosure to a third party of more than four sequential numbers of an employee's, student's, or other individual's Social Security number, Senate Bill 795 (S-4) would go a long way toward protecting that sensitive information.

Supporting Argument

The question of jurisdiction has been a problem in combating identity theft. While Federal laws include some prohibitions, enforcement measures, and information-gathering activities, and Federal courts have jurisdiction over violations of those laws, there apparently has been confusion over whether law enforcement agencies and courts where the victim lives, where personal identity information is gathered, or where that information is used illegally, have the proper jurisdiction to investigate and prosecute violations of State law. Senate Bill 793 (S-1) would eliminate this confusion by specifying that a violation of the proposed Identity Theft Protection Act or of

another law committed in furtherance of or arising out of a violation of that Act, could be prosecuted in the jurisdiction in which the offense occurred, in which the information used to commit the violation was illegally used, or in which the victim lived. In addition, under the bill, if a person were charged with more than one identity theft violation that could be prosecuted in more than one jurisdiction, he or she could be prosecuted in any of those jurisdictions for all of the violations.

Supporting Argument

Victims of identity theft often feel further victimized by their difficulty or inability to secure credit or to contract for other products and services legitimately, after their name and credit history have been besmirched. A publicly certified document identifying a person as an identity theft victim could aid him or her in convincing creditors and others that he or she was not responsible for the bad credit rating on his or her record. Senate Bill 794 (S-2) would provide for such a certificate to be issued, free of charge, by a county prosecuting attorney. To apply for a certificate, the victim would have to file a complaint regarding the identity theft with a law enforcement agency having jurisdiction over the violation. The prosecuting attorney could request that the law enforcement agency investigate the complaint. By including these provisions, the bill not only would offer protection and redemption to identity theft victims, but also would encourage greater investigation of identity theft claims.

Response: The creation of a certificate of identity theft victimization and the data base that would be necessary to track the certificates would be ripe for abuse. According to the director of the MSU Identity Theft Lab, criminals would be likely to falsify the certificates, giving identity thieves another avenue to perpetrate their crimes.

Supporting Argument

Under the Code of Criminal Procedure, an indictment generally must be filed within six years after an offense is committed. An identity theft violation may not be discovered until long after the offense actually was committed, however, and even then the true identity of a person who has evidence of the crime might not be readily known. With unavailable evidence, or unknown suspects and witnesses, it may be difficult or even impossible to prosecute an

identity theft violation within six years after the crime is committed. Senate Bill 803 would alleviate this problem by allowing identity theft to be prosecuted at any time after the offense was committed, but not more than six years after the individual was identified, if evidence of the violation were determined to be from an unidentified individual.

Opposing Argument

Maintaining the integrity of personal identifiers, such as Social Security numbers, is crucial to protecting consumers against identity theft. Severely limiting the use of those numbers, however, would not be entirely beneficial. For instance, financial institutions rely on personal identifiers in order to prevent identity theft and to maintain accurate account records. Identity theft can result when a legitimate creditor or other supplier of a service or product does not have enough information about the customer, not when it has too much. If a bank or utility provider, for example, has John Doe's Social Security number, it will have a better chance of verifying the identity of a person claiming to be John Doe than if it did not have that information. The prohibitions in Senate Bill 795 (S-4), then, actually could make it more difficult for a service provider to ensure that the proper customer was being granted and charged for that service, and make it easier for an identity thief to convince a creditor or utility that he or she was someone else.

In addition, prohibiting the disclosure of a person's Social Security number to a third party could hinder many banking practices because financial institutions must disclose Social Security numbers in the ordinary course of business for legitimate reasons. For example, if a lender wanted to sell its portfolio of loans to another creditor, as is often done with mortgage loans, that portfolio would include each debtor's Social Security number. A creditor also must use a loan applicant's Social Security number to obtain a copy of that person's credit report, which is crucial to the decision of whether to extend credit to the individual. Also, in the course of a fraud investigation, a financial institution may have to provide the Social Security number of a possible victim—including an identity theft victim—to law enforcement agencies, courts, and insurance investigators.

Further, many public records contain Social Security numbers. These public records must be made available and often are compiled on computer discs and sold to businesses such as title companies. Prohibiting or limiting the disclosure of those documents or information in them could result in other violations and would require enormous effort to examine each record and remove the information that could not be disclosed.

Response: While Senate Bill 795 (S-4) would limit the use, display, and disclosure of Social Security numbers, it contains broad enough exceptions to allow use of those numbers in the legitimate practice of business. For instance, the bill's prohibitions would not apply under the following circumstances: if an individual or his or her parent or legal guardian consented to the disclosure of his or her Social Security number to a third party, or if a disclosure, display, or other use were authorized or required by law, regulation, rule, or court order.

In addition, the bill includes an exception for disclosure to a third party who had a written privacy policy making use of the numbers confidential. This would include a person providing health benefits or an employment benefit or payroll plan, determining an applicant's suitability for employment, or lawfully pursuing or enforcing someone's legal rights regarding such things as audits, collections, and transfers of debt.

Also, for certain administrative and enforcement purposes, the bill would excuse from the third-party disclosure prohibition a person (such as a banker or insurance agent) subject to and regulated by a statute administered by a regulatory board on the State or Federal level. Therefore, a financial institution could include all necessary identifying information when transferring a debt or investment portfolio, verifying an individual's identity, or investigating a possible identity theft or other financial crime.

Opposing Argument

The prohibitions in Senate Bill 792 (S-4) against soliciting to extend credit are too broad and would be inconvenient to consumers. Pre-approved checks and credit cards are an effective marketing tool for creditors wishing to expand their business and helpful for consumers looking for new sources of credit.

Response: Consumers could still seek credit, and creditors could still offer it, under the bill. The bill would allow solicitations to extend credit if the customer had an existing line-of-credit or credit card or had applied for credit in the past year. In addition, the prohibition against soliciting to extend credit through the use of an unsolicited check would apply only to one that included identifying information beyond a person's name, address, and partial, encoded, or truncated personal identifying number. These restrictions should not hinder the legitimate operation of a creditor's business.

Opposing Argument

Senate Bill 220 (S-2) would prohibit merchants from issuing a receipt that showed any part of a credit or debit card's expiration date or more than the last four digits of the account number. The bill should limit this prohibition to receipts that are printed electronically.

Response: The bill includes an exception for a handwritten, mechanically imprinted, or photocopied receipt. It also would allow a phase-in period to program equipment, so that electronically generated receipts would not include the restricted information.

Opposing Argument

By allowing a law enforcement agency or financial institution to obtain copies of a vital record, such as a birth certificate, from a local registrar, Senate Bill 792 (S-4) could open up the State's vital records system to abuse, even if the record were considered necessary to investigate or prevent identity theft. Easing restrictions on access to such records could give identity thieves a way to obtain those documents, making it easier for them to commit the crimes the bills aim to prevent.

Opposing Argument

The identity theft legislation was rendered unnecessary, and perhaps even unenforceable, by the overhaul of the Federal Fair Credit Reporting Act (FCRA) in the fall of 2003. According to the National Conference of State Legislatures, the FCRA contains measures to fight identity theft and preempts state laws in nine areas in which the FCRA establishes national standards. These include the truncation of credit and debit card numbers, Social Security number truncation, and coordination of consumer complaint investigations.

Response: According to a *Wall Street Journal* article on the Federal legislation, states will continue to "have some discretion, including setting criminal penalties for identity thieves and defining limits on any sharing of Social Security numbers" ("Identity Theft Deal Would Give States Some Jurisdiction", 11-24-03).

Legislative Analyst: Patrick Affholter

FISCAL IMPACT

Senate Bill 220 (S-2)

The bill would have an indeterminate impact on the State and local units of government. Enforcement costs and penalty revenue would depend on the number of violators under the bill.

Senate Bill 657

The enforcement costs and fine revenue would depend on the number of violations.

Senate Bills 792 (S-4) & 797

The bills would have an indeterminate fiscal impact on State and local government. The proposed felony of identity theft would replace the existing felony of obtaining personal identification information without authorization and with intent to use the information unlawfully. According to the Department of Corrections Statistical Report, in 2001 seven people were convicted of that offense. Of those, one offender received incarceration in a State prison, one received incarceration in a local jail, and five received probation. Local units pay for incarceration in local facilities, the cost of which varies by county. The State incurs the cost of felony probation at an average annual cost of \$1,800, as well as the cost of incarceration in a State facility at an average annual cost of \$28,000. If one assumes that the number of offenders and types of sentences received for the proposed offense would be similar to those for the existing offense, the change would have no fiscal impact.

There are no data to indicate how many offenders would be convicted of a misdemeanor for committing the trade practices described in the bill. Offenders would receive probation, imprisonment for up to 30 days in a local facility, and/or a fine of up to \$100. Local units would incur the

costs of both misdemeanor probation and incarceration, which vary by county.

Senate Bill 793 (S-1)

The bill would have no fiscal impact on the State and an indeterminate fiscal impact on local units of government. To the extent that the bill would increase the number of cases prosecuted, it would increase local court costs.

Senate Bill 794 (S-2)

The bill would have an indeterminate fiscal impact on the Department of State Police, which would have to provide certificate forms to county prosecuting attorneys. The number of certificates to be provided under the bill cannot be determined at this time. The bill also would result in an indeterminate financial cost for local prosecutors, depending on the number of applications they received for certificates of identity theft.

Senate Bill 795 (S-4)

The bill would have no fiscal impact on the State and an indeterminate fiscal impact on local units of government.

There are no data to indicate how many offenders would be convicted of the proposed misdemeanor. Offenders could receive probation, incarceration in a local facility, and/or a fine of up to \$1,000. Local units of government incur the costs of both misdemeanor probation and incarceration in local facilities, which vary by county. Public libraries would benefit from any additional penal fine revenue raised due to the proposed penalty.

Senate Bill 798 (S-1)

Enforcement costs and fine revenue would depend on the number of violations.

Senate Bill 803

The bill would have an indeterminate fiscal impact on State and local government.

By extending the period to file an indictment to six years after the identification of an individual from whom evidence was obtained, the bill could increase local court costs and both local and State corrections costs to the extent that it would allow

additional identity theft cases to be prosecuted and offenders to be convicted.

Senate Bill 1384

The bill would have no fiscal impact on State or local government.

Fiscal Analyst: Bruce Baker
Bill Bowerman
Bethany Wicksall

A0304\s220a

This analysis was prepared by nonpartisan Senate staff for use by the Senate in its deliberations and does not constitute an official statement of legislative intent.