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 Bills 220 and 657 (as enrolled) **PUBLIC ACTS 461 & 462 of 2004**
Senate Bills 792, 793, 795, 798, and 1384 (as enrolled) **PUBLIC ACTS 452-456 of 2004**
House Bills 6169, 6172, 6174, and 6177 (as enrolled) **PUBLIC ACTS 457-460 of 2004**

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 Nancy Cassis (S.B. 795)
Senator Alan Sanborn (S.B. 798)
Senator Laura M. Toy (S.B. 1384)
Representative William Van Regenmorter (H.B. 6169)
Representative Matt Milosch (H.B. 6172)
Representative Mike Nofs (H.B. 6174)
Representative Sal Rocca (H.B. 6177)

Senate Committee: Judiciary
Economic Development, Small Business and Regulatory Reform (S.B. 220)

House Committee: Criminal Justice

Date Completed: 4-18-05

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, 1-22-04.) Of those identity theft complaints, 6,566 were from Michigan victims in 2003.

The Michigan Penal Code previously prohibited 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. It was suggested, however, that Michigan law should include more comprehensive protections against identity theft; include measures to protect a consumer's financial account numbers, Social Security number, and medical benefits number; and clarify court jurisdiction over identity theft cases.

CONTENT

Senate Bills 220, 657, and 798 and House Bill 6174 amended the Michigan Consumer Protection Act to prohibit a person from requiring a consumer to disclose his or her Social Security number as a condition to selling or

leasing goods or providing a service to the consumer. The bills also prohibit the issuance or delivery of a receipt for a credit card or debit card transaction that displays any part of the card's expiration date or more than the last four digits of the consumer's account number.

Senate Bill 792 created the "Identity Theft Protection Act" to do all of the following:

- **-- Prohibit the use of another person's personal identifying information for certain purposes, including committing identity theft, regardless of whether the victim is alive or dead.**
- **-- Prohibit specific activities in the conduct of trade or commerce.**
- **-- Establish criminal and civil liability for violations of the Act.**
- **-- Authorize a person to assert certain defenses in a civil action or criminal prosecution.**
- **-- Allow a law enforcement agency or identity theft victim to verify information from a vital record or, under certain circumstances, obtain a copy of a vital record.**

The bill also repealed a section of the Michigan Penal Code that prohibited obtaining another person's personal identity information with the intent to use it unlawfully for certain purposes.

Senate Bill 793 amended the Code of Criminal Procedure to specify that a violation of the Identity Theft Protection Act or the former offense of obtaining personal information without authorization may 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 lives.

Senate Bill 795 created the "Social Security Number Privacy Act" to prohibit certain actions regarding the disclosure, display, or use of a person's Social Security number. Beginning January 1, 2006, the bill also will require a person who obtains one or more Social Security numbers in the ordinary course of business to create a privacy policy concerning those numbers.

Senate Bill 1384 amended the Crime Victim's Rights Act to allow a victim of identity theft to file and obtain a police report.

House Bill 6169 amended the Code of Criminal Procedure to include identity theft violations in the sentencing guidelines.

House Bill 6172 amended the Code of Criminal Procedure to extend the period of limitations for filing identity theft charges when evidence is obtained but the identity of the offender is not known.

House Bill 6177 amended the Michigan Penal Code to prohibit a person who is not a party to a transaction involving the use of a financial transaction device from secretly capturing or recording, or distributing or transmitting, an individual's personal identifying information from the transaction, without the individual's consent.

The bills took effect March 1, 2005. Senate Bill 793 was tie-barred to Senate Bill 792.

Senate Bills 220, 657, & 798 and House Bill 6174

The bills amended Section 3 of the Michigan Consumer Protection Act (MCL 445.903). That section lists certain activities that are designated as unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce and, as such, are unlawful.

Senate Bill 220 added to the list issuing or delivering to the consumer, in a credit or debit card transaction, a receipt that displays any part of the card's expiration date or more than the last four digits of the consumer's account number. The bill specifies that this provision does not apply if the only receipt issued is one on which the account number or expiration date is handwritten, mechanically imprinted, or photocopied.

This bill applies to consumer transactions that occur after March 1, 2005. If a receipt is printed by an electronic device, however,

the provision applies to transactions using the device after one of the following dates, as applicable:

-- July 1, 2005, or the date the device is placed in service, whichever is later, if the device is placed in service after March 1, 2005.
-- July 1, 2006, if the device is placed in service on or before March 1, 2005.

Senate Bill 657 added to the list requiring a consumer to disclose his or her Social Security number as a condition to selling or leasing goods, or providing a service to the consumer, unless any of the following apply:

-- The sale, leasing, provision, terms of payment, or transaction includes an application for or an extension of credit to the consumer.
-- The disclosure is required or authorized by applicable State or Federal statute, rule, or regulation.
-- The disclosure is requested by a person to obtain a consumer report for a purpose allowed under Section 604 of the Fair Credit Reporting Act (15 USC 1681b). (That section lists permissible purposes of consumer reports.)
-- The disclosure is requested by a landlord, lessor, or property manager to obtain a background check of the individual in conjunction with the rental or leasing of real property.

Also, the prohibition against requiring a consumer to disclose his or her Social Security number does not apply if the disclosure is requested to effect, administer, or enforce a specific telephonic or other electronic consumer transaction that is not made in person but is requested or authorized to be used solely to confirm the individual's identity through a fraud prevention service database. The consumer goods or service still must be provided to the consumer upon verification of his or her identity, if he or she refuses to provide his or her Social Security number but provides other verification. The person may inform the consumer that verification through means other than his or her Social Security number may delay the provision of the service or goods.

In addition, the bill's prohibition does not apply to either of the following:

-- Providing a service related to the administration of health- or dental-related benefits or services to patients.
-- An employer providing benefits or services to an employee.

The bill specifies that the exception for the provision of health- or dental-related benefits "is intended to limit the application of" the bill's prohibition "and is not intended to imply that" the Michigan Consumer Protection Act otherwise applies to health- or dental-related benefits.

Senate Bill 798 added to the list of unlawful methods, acts, or practices, denying credit or a public utility service to, or reducing the credit limit of, a consumer who is a victim of identity theft under the Identity Theft Protection Act, with prior knowledge that the consumer was an identity theft victim.

House Bill 6174 added to the list violating Section 11 of the Identity Theft Protection Act, and omitted the provision added by Senate Bill 798. (Section 11 prohibits certain practices in the conduct of trade or commerce, including activity similar to that proscribed by Senate Bill 798.)

Senate Bill 792

Prohibitions

The bill prohibits a person from using or attempting to use another person's personal identifying information, with the intent to defraud or violate the law, in order to obtain credit, goods, services, money, property, a vital record, medical records or information, or employment, or to commit another unlawful act.

The bill also prohibits a person from using or attempting to use another person's personal identifying information, by concealing, withholding, or misrepresenting the user's identity, in order to obtain credit, goods, services, money, property, a vital record, medical records or information, or employment, or to commit another unlawful act. A person who violates this prohibition may assert one or more of the following as a defense in a civil action or as an affirmative defense in a criminal prosecution, and has the burden of providing that defense by a preponderance of the evidence:

-- That the person gave a bona fide gift for or for the benefit or control of, or use or consumption by, the person whose personal identifying information was used.
-- That the person acted in otherwise lawful pursuit or enforcement of a person's legal rights, including an investigation of a crime or an audit, collection, investigation, or transfer of a debt, child or spousal support obligation, tax liability, claim, receivable, account, or interest in a receivable or account.
-- That the action taken was authorized or required by State or Federal law, rule, regulation, or court order or rule.
-- That the person acted with the consent of the person whose personal identifying information was used, unless the person giving consent knows that the information will be used to commit an unlawful act.

The bill also prohibits a person from doing any of the following:

-- 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 crime.
-- Selling or transferring, or attempting to sell or transfer, another's personal identifying information, if the person knows or has reason to know that the specific intended recipient will use, attempt to use, or further transfer the information to another person for the purpose of committing identity theft or another crime.
-- Falsifying a police report of identity theft, or knowingly creating, possessing, or using a false police report of identity theft.

These prohibitions apply whether an individual who is a victim or intended victim is alive or deceased at the time of the violation.

The bill defines "personal identifying information" as a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including a person's name, address, telephone number, driver license or State personal ID card number, Social Security number, place of employment, employee identification 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, vital record, or medical records or information.

Trade or Commerce

The bill prohibits a person, in the conduct of trade or commerce, from 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. The bill specifies that a consumer is presumed to be an identity theft victim if he or she provides a copy of a police report showing the victim's claim of identity theft and either a properly completed copy of a standardized affidavit of identity theft developed and made available by the FTC or an affidavit of fact acceptable for that purpose.

The bill also prohibits a person from doing either of the following in the conduct of trade or commerce:

-- Soliciting to extend credit to a consumer who does not have an existing line of credit, or has not had or applied for a line of credit within the preceding year, through the use of an unsolicited check that includes 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 does not have a current credit card, or has not had or applied for a credit card within the preceding year, through the use of an unsolicited credit card sent to the consumer.

In addition, the bill prohibits a person, in the conduct of trade or commerce, from extending credit to a consumer without exercising reasonable procedures to verify the identity of the consumer. The bill provides that compliance with regulations issued for depository institutions, and to be issued for other financial institutions, by the U.S. Treasury under the USA Patriot Act is considered compliance with this provision. Also, this prohibition does not apply to a

purchase of a credit obligation in an acquisition, merger, purchase of assets, or assumption of liabilities or any change to or review of an existing credit account.

Penalties, Exceptions, & Defense

The bill makes it a felony, punishable by up to five years' imprisonment and/or a maximum fine of $25,000, to violate any of the prohibitions involving the use of another person's personal identity information; obtaining, possessing, selling, or transferring that information; or falsifying a police report.

The bill specifies that this provision does not prohibit a person from being charged with, convicted of, or sentenced for any other violation of law committed by that person using information obtained in violation of the Identity Theft Protection Act or any violation of law committed by him or her while violating or attempting to violate the Act. The sentencing court may order that a term of imprisonment be served consecutively to any term of imprisonment imposed for a conviction of any other violation of law committed by that person using the information obtained in violation of the Act or any other violation committed while violating or attempting to violate the Act.

The criminal penalties do not apply to a violation of a statute or rule administered by a regulatory board, commission, or officer, acting under authority of the State or the United States that confers primary jurisdiction on that board, commission, or officer to authorize, prohibit, or regulate the transactions and conduct of that person. This includes, but is not limited to, a State or Federal statute or rule governing a financial institution and the Insurance Code, if the act is committed by a person subject to and regulated by that statute or rule, or by another person who has contracted with that person to use personal identifying information.

A person may assert as a defense in a civil action or as an affirmative defense in a criminal prosecution, and has the burden of proving that defense by a preponderance of the evidence, that he or she lawfully transferred, obtained, or attempted to obtain another's personal identifying information for the purpose of detecting, preventing, or deterring identity theft or another crime or the funding of a criminal activity.

A knowing or intentional violation of the bill's trade or commerce prohibitions is a misdemeanor punishable by up to 30 days' imprisonment, a maximum fine of $1,000, or both. The bill states that this provision does not affect the availability of any civil remedy for a violation of the 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 Identity Theft Protection Act, or the Michigan Consumer Protection Act, for a violation involving a solicitation to extend credit, a credit card issuer, financial institution, or lender is 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 is used by an unauthorized user and for any fees assessed to the consumer if the instrument is dishonored. The consumer is not liable for those amounts, fees, or charges.

Vital Records

A law enforcement agency or victim of identity theft may verify information from a vital record from a local registrar, or the State registrar, in the manner described in Section 2881(2) of the Public Health Code (MCL 333.2881(2)). (That section requires the State registrar or a local registrar to verify certain facts upon written request and payment of a prescribed fee.)

A State or local registrar that verifies information from a vital record under Section 2881(2) for a law enforcement agency investigating identity theft may provide that agency with all of the following information about any previous requests concerning that public record that is available to the registrar:

-- Whether or not a certified copy or copies of the record were requested.
-- The date or dates a copy or copies of the record were issued.
-- The name of each applicant who requested the record.
-- The address, e-mail address, telephone number, and other identifying information

of each applicant who requested the record.
-- Payment information regarding each request.

A State or local registrar that verifies information from a vital record under Section 2881(2) for an individual who provides proof that he or she is a victim of identity theft may give the individual all of the following information about any previous requests concerning that public record that is available to the registrar:

-- Whether or not a certified copy or copies of the record were requested.
-- The date or dates a copy or copies of the record were issued.

For purposes of this provision, it is sufficient proof that an individual is a victim if he or she supplies the registrar with a copy of a police report showing the claim of identity theft and, if available, an affidavit of identity theft in a form developed by the State registrar in cooperation with the Attorney General.

A law enforcement agency may request an administrative use copy of a vital record from the State registrar in the manner allowed under Section 2891 of the Public Health Code (MCL 333.2891). A law enforcement agency may request an administrative use copy of a vital record from a local registrar in the manner described in Section 2891, if the request for the administrative use copy is in writing and contains both of the following:

-- A statement that the agency requires information from a vital record beyond the information the local registrar may verify under the provisions described above.
-- The agency's agreement that it will maintain the administrative use copy of the vital record in a secure location and will destroy the copy by confidential means when it no longer needs the copy.

(Section 2891 allows the State registrar or a local registrar, upon receiving a written request and payment of a prescribed fee, to conduct a search for a vital record for certain individuals or agencies authorized to receive a certified copy, administrative use copy, or a statistical use copy.)

Repealer

The bill repealed Section 285 of the Michigan Penal Code (former MCL 750.285). That section prohibited 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 was a felony, punishable by up to five years' imprisonment, a maximum fine of $10,000, or both.

Under former Section 285, "personal identity information" meant 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

Under the bill, conduct prohibited under former Section 285 of the Michigan Penal Code (obtaining personal identity information without authorization), a violation of the Identity Theft Protection Act, or a violation of law committed in furtherance of or arising from the same transaction as such a violation or conduct, may 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 lives.

If a person is charged with more than one violation of the Identity Theft Protection Act, and those violations may be prosecuted in

more than one jurisdiction, any of those jurisdictions is a proper jurisdiction for all of the violations.

Senate Bill 795

Prohibited Uses of Social Security Numbers

The bill prohibits a person from intentionally doing any of the following with the Social Security number of an employee, student, or other individual:

-- Publicly displaying all or more than four sequential digits of the Social Security number.
-- Using all or more than four sequential digits of the Social Security number as the primary account number for an individual (although this prohibition does not apply until January 1, 2006, if the person is using the number on an ID badge or card, membership card, or permit or license as of March 1, 2005).
-- Requiring an individual to use or transmit all or more than four sequential digits of his or her Social Security number over the internet or a computer system or network, unless the connection is secure or the transmission is encrypted.
-- Requiring an individual to use or transmit all or more than four sequential digits of his or her Social Security number to gain access to an internet website or a computer system or network unless the connection is secure, the transmission is encrypted, or a password or other unique personal ID number or other authentication device also is required for access.
-- Including all or more than four sequential digits of the Social Security number in or on any document or information mailed or otherwise sent to an individual, if it is visible on or, without manipulation, from outside of the envelope or packaging.

The bill also prohibits a person from intentionally visibly printing all or more than four sequential digits of an individual's Social Security number on any ID badge or card, membership card, or permit or license. If, however, a person has implemented or implements a plan or schedule that establishes a specific date by which the person will comply with this prohibition, it does not apply to that person until January 1, 2006, or the completion date specified in that plan or schedule, whichever is earlier.

Beginning January 1, 2006, the bill prohibits a person from intentionally including all or more than four sequential digits of an employee's, student's, or other individual's Social Security number in any document or information mailed to a person, unless any of the following apply:

-- State or Federal law, rule, regulation, or court order or rule authorizes, permits, or requires that a Social Security number appear in the document.
-- The document is sent as part of an application or enrollment process initiated by the individual.
-- The document is sent to establish, confirm the status of, service, amend, or terminate an account, contract, policy, or employee or health insurance benefit, or to confirm the accuracy of a Social Security number of an individual who has an account, contract, policy, or employee or health insurance benefit.
-- The document or information is a public record and is mailed by a public body in compliance with the Freedom of Information Act; is a copy of a public record filed or recorded with a county clerk or register of deeds office and is mailed by that office to a person entitled to receive that record; or is a copy of a vital record recorded as provided by law and is mailed to a person entitled to receive that record.
-- The document or information is mailed by or at the request of an individual whose Social Security number appears in the document or information, or at the request of his or her parent or legal guardian.
-- The document or information is mailed in a manner or for a purpose consistent with the Federal Gramm-Leach-Bliley Act, the Federal Health Insurance Portability and Accountability Act, or the Insurance Code.

The bill's Social Security number prohibitions do not apply to use of all or more than four sequential digits of a Social Security number that is authorized or required by State or Federal stature, rule, or regulation, by court order or rule, or pursuant to legal discovery or process. The prohibitions also do not apply to use of all or more than four sequential digits of a Social Security number by a Title IV-D agency, law enforcement agency, court, or prosecutor as part of a criminal investigation or providing those

digits to one of those entities as part of a criminal investigation or prosecution. (Title IV-D agency refers to an entity in Michigan performing child support enforcement functions.)

The bill specifies that it is not a violation of the prohibitions against mailing, or using as a primary account number, all or more than four sequential digits of a Social Security number if the use is an administrative use in the ordinary course of business, by a person or a vendor or contractor, to do any of the following:

-- Verify an individual's identity, identify an individual, or perform another similar administrative purpose related to an existing or proposed account, transaction, product, service, or employment.
-- Investigate an individual's claim, credit, criminal, or driving history.
-- Detect, prevent, or deter identity theft or another crime.
-- Lawfully pursue or enforce a person's legal rights, including an audit, collection, investigation, or transfer of a tax, employee benefit, debt, claim, receivable, or account or an interest in a receivable or account.
-- Lawfully investigate, collect, or enforce a child or spousal support obligation or tax liability.
-- Provide or administer employee or health insurance or membership benefits, claims, or retirement programs or administer the ownership of shares of stock or other investments.

It also is not a violation if a use of all or more than four sequential digits of a Social Security number as a primary account number began before March 1, 2005, and the use is ongoing, continuous, and in the ordinary course of business. If the use is stopped for any reason, this exception no longer applies.

Criminal & Civil Liability

A person who violates the prohibitions against displaying or using a Social Security number, with knowledge that the conduct violates the Social Security Number Privacy Act, is guilty of a misdemeanor punishable by up to 93 days' imprisonment, a maximum fine of $1,000, or both.

An individual may bring a civil action against a person who violates the prohibitions regarding the use of a Social Security number and may recover actual damages. If the person knowingly violates those prohibitions, an individual may recover actual damages or $1,000, whichever is greater, and attorney fees. Except for good cause, at least 60 days before filing a civil action, an individual must make a written demand to the person for the amount of his or her actual damages, with reasonable documentation of the violation and the actual damages caused by it.

The civil remedy provision does not apply to a person for conduct by an employee or agent of the person in violation of a privacy policy created pursuant to the bill or in compliance with the Fair Credit Reporting Act or the Gramm-Leach-Bliley Act, if the person has taken reasonable measures to enforce the privacy policy and to correct and prevent the reoccurrence of any known violations.

Privacy Policy

Beginning January 1, 2006, a person who obtains one or more Social Security numbers in the ordinary course of business must create a privacy policy that does at least all of the following concerning the numbers the person possesses or obtains:

-- Ensures the confidentiality of the numbers to the extent practicable.
-- Prohibits unlawful disclosure of the numbers.
-- Limits who has access to information or documents that contain the numbers.
-- Describes how properly to dispose of documents that contain the numbers.
-- Establishes penalties for violating the privacy policy.

A person who creates a privacy policy must publish it in an employee handbook, in a procedures manual, or in one or more similar documents, which may be made available electronically.

The bill's privacy policy requirements do not apply to a person who possesses Social Security numbers in the ordinary course of business and in compliance with the Federal Fair Credit Reporting Act or the Gramm-Leach-Bliley Act.

FOIA Exemption

The bill specifies that all or more than four sequential digits of a Social Security number contained in a public record are exempt from disclosure under the Freedom of Information Act.

Senate Bill 1384

The bill amended the Crime Victim's Rights Act to specify that, to facilitate compliance with Federal law (15 USC 1681g) a bona fide victim of identity theft is entitled to file a police report with a law enforcement agency in a jurisdiction where the alleged violation of identity theft may be prosecuted as provided under MCL 762.10c (the section of the Code of Criminal Procedure added by Senate Bill 793), and is entitled to obtain a copy of that report from that law enforcement agency. The bill inserted 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 inquires 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.)

House Bill 6169

The bill included in the sentencing guidelines both identity theft and obtaining, possessing, selling, or transferring another person's personal identifying information or falsifying a police report with intent to commit identity theft. Each offense is categorized as a Class E felony against the public order, with a statutory maximum penalty of five years' imprisonment.

The bill also deleted from the sentencing guidelines the offense of obtaining personal information without authorization, which the Identity Theft Protection Act repealed. That offense was a Class E property felony, with a statutory maximum penalty of five years' imprisonment.

House Bill 6172

Under Section 24 of Chapter VII of 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 may be found and filed within six years after the offense is committed. If evidence of an identity theft violation is obtained and the individual who committed the offense has not been identified, however, an indictment may be found and filed at any time after the offense is committed, but not more than six years after the individual is identified. ("Identity theft" means conduct prohibited under the Identity Theft Protection Act or former Section 285 of the Penal Code. "Identified" means that the individual's legal name is known.)

The bill also specifies that the extension or tolling of the limitations period provided in this section applies to any of the violations for which the limitations period has not expired at the time the extension or tolling takes effect.

House Bill 6177

The bill added Section 539k to the Michigan Penal Code to prohibit a person who is not a party to a transaction that involves the use of a financial transaction device from secretly or surreptitiously photographing, or otherwise capturing or recording, electronically or by any other means, or distributing, disseminating, or transmitting, electronically or by any other means, personal identifying information from the transaction, without the consent of the individual. A violation is a misdemeanor punishable by up to one year's imprisonment, a maximum fine of $1,000, or both. "Financial transaction device" means that term as defined in Section 157m of the Code (e.g., an electronic funds transfer card, a credit card, a debit card, or a point-of-sale card). "Personal identifying information" means that term as defined in the Identity Theft Protection Act.)

The bill specifies that Section 539k does not prohibit a person from being charged with,

convicted of, or punished for any other violation of law he or she committed while violating or attempting to violate the bill.

The bill further states that Section 539k does not prohibit the capture or transmission of person identifying information in the ordinary and lawful course of business. This section also does not apply to a State or Federal peace officer, or the officer's agent, while in the lawful performance of his or her duties.

MCL 445.903 (S.B. 220, 657, & 798 and H.B. 6174)
445.61-445.77 (S.B. 792)
762.10c (S.B. 793)
445.81-445.87 (S.B. 795)
780.754a et al. (S.B. 1384)
777.14h & 777.16o (H.B. 6169)
767.24 (H.B. 6172)
750.539k (H.B. 6177)

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, 3-20-02). 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 have prohibited activity that constitutes identity theft, penalized criminals after the fact, and perhaps deterred some would-be identity thieves, these bills will help to prevent identity theft from occurring in the first place. In addition to recodifying and expanding the penalties enacted by Public Act 386, the bills prohibit certain activities regarding soliciting the extension of credit to someone who does not have an existing account or has 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 shows an entire account number.

Response: 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. Perhaps the law should provide for such a certificate to be issued by a county prosecuting attorney, as proposed by Senate Bill 794 (originally part of this package).

Also, the director of the Michigan State University (MSU) Identity Theft Lab 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", *Lansing State Journal*, 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".

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 of more than four sequential numbers of an employee's, student's, or other individual's Social Security number, Senate Bill 795 will help to protect 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 eliminates this confusion by specifying that a violation of the Identity Theft Protection Act or the former prohibition against obtaining personal identity information, or a violation of another law committed in furtherance of or arising out of those violations, may 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 lives. In addition, under the bill, if a person is charged with more than one identity theft violation that may be prosecuted in more than one jurisdiction, he or she may be prosecuted in any of those jurisdictions for all of the violations.

Supporting Argument

Under the statute of limitations in the Code of Criminal Procedure, a prosecutor generally must file an indictment 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 the person who committed the identity theft might not be readily known. With unknown suspects, it may be difficult or even impossible to prosecute an identity theft violation within six years after the crime is committed. House Bill 6172 alleviates this problem by allowing identity theft to be prosecuted at any time after the offense is committed, but not more than six years after the individual who committed the offense is identified.

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, is not 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, then, actually

might make it more difficult for a service provider to ensure that the proper customer is 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 is someone else.

In addition, prohibiting the disclosure of a person's Social Security number to a third party may 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 wishes to sell its portfolio of loans to another creditor, as is often done with mortgage loans, that portfolio will 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 may result in other violations and will require enormous effort to examine each record and remove the information that may not be disclosed.

Response: While Senate Bill 795 limits the use, display, and disclosure of Social Security numbers, it contains sufficiently broad exceptions to allow use of those numbers in the legitimate practice of business.

Opposing Argument

The prohibitions in Senate Bill 792 against soliciting to extend credit are too broad and will 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 may still seek credit, and creditors may still offer it, under the bill. The bill allows solicitations to extend credit if the customer has an existing line-of-credit or credit card or has applied for credit in the past year. In addition, the prohibition against soliciting to extend credit through the use of an unsolicited check applies only to one that includes 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 prohibits merchants from issuing a receipt that shows any part of a credit or debit card's expiration date or more than the last four digits of the account number. This prohibition should be limited to receipts that are printed electronically.

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

Opposing Argument

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

Response: The vital records provisions of Senate Bill 792 refer to authorization and procedures outlined under the Public Health Code to verify information from, or obtain, a vital record. The bill does not expand access to those records. In addition, Senate Bill 792 requires a law enforcement agency to agree to keep an administrative use copy of a vital record in a secure location and to destroy the record by confidential means when it is no longer needed.

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 Bills 220, 657 & 798 and House Bill 6174

The bills will have an indeterminate fiscal impact on the State and local units of government. Enforcement costs and penalty revenue will depend on the number of transactions in which consumers are unlawfully required to disclose Social Security numbers, or consumers' Social Security numbers are unlawfully displayed. The bills will have an indeterminate impact on the Department of Attorney General related to the Attorney General's responsibilities under the Michigan Consumer Protection Act. The number of additional cases that will result cannot be projected.

Senate Bill 792 & House Bill 6169

The bills will have an indeterminate fiscal impact on State and local government. The new felony of identity theft replaces the 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 2002, 53 people were convicted of that offense. Of those, 11 offenders received incarceration in a State prison, three received incarceration in a local jail, and 39 received probation or some other sentence. 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 $2,000, 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 new offense will be similar to those for the former offense, the change will have no fiscal impact.

There are no data to indicate how many offenders will be convicted of a misdemeanor for committing the trade practices described in the bill. Offenders will receive probation, imprisonment for up to 30 days in a local facility, and/or a fine of up to $1,000. Local units will incur the costs of both misdemeanor probation and incarceration, which vary by county.

Senate Bill 793

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

Senate Bill 795

The bill will 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 will be convicted of the misdemeanor pertaining to the disclosure of Social Security numbers. Offenders will 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 will benefit from any additional penal fine revenue raised due to the penalty.

The bill also may increase local judicial costs by allowing civil actions to be brought for violations of the Act.

Senate Bill 1384

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

House Bill 6172

The bill will have an indeterminate fiscal impact on State and local government. By extending the period for filing an indictment to six years after the identification of an offender, the bill may increase local court costs and both local and State corrections costs to the extent that it allows additional identity theft cases to be prosecuted.

House Bill 6177

The bill will have no fiscal impact on the State and an indeterminate fiscal impact on local government. There are no data to indicate how many people will be convicted of the misdemeanor involving information obtained with a financial transaction device. Local units of government incur the costs of misdemeanor probation and incarceration in local facilities, which vary by county. Public libraries will benefit from any additional penal fine revenue raised.

Fiscal Analyst: Bruce Baker
Bill Bowerman
Bethany Wicksall

A0304\s220ea