Legislative Analysis

Mitchell Bean, Director
Phone: (517) 373-8080
http://www.house.mi.gov/hfa

IDENTITY THEFT

House Bill 6169 as enrolled
Public Act 457 of 2004
Sponsor: Rep. William Van Regenmorter

House Bill 6172 as enrolled
Public Act 458 of 2004
Sponsor: Rep. Matt Milosch

House Bill 6174 as enrolled
Public Act 459 of 2004
Sponsor: Rep. Mike Nofs

House Bill 6177 as enrolled
Public Act 460 of 2004
Sponsor: Rep. Sal Rocca

Senate Bill 220 as enrolled
Public Act 461 of 2004
Sponsor: Sen. Valde Garcia

Senate Bill 657 as enrolled
Public Act 462 of 2004
Sponsor: Sen. Cameron S. Brown

Senate Bill 792 as enrolled
Public Act 452 of 2004
Sponsor: Sen. Michael Bishop

Senate Bill 793 as enrolled
Public Act 453 of 2004
Sponsor: Sen. Gerald Van Woerkom

Senate Bill 795 as enrolled
Public Act 454 of 2004
Sponsor: Sen. Nancy Cassis

Senate Bill 798 as enrolled
Public Act 455 of 2004
Sponsor: Sen. Alan Sanborn

Senate Bill 1384 as enrolled
Public Act 456 of 2004
Sponsor: Sen. Alan L. Cropsey

House Committee: Criminal Justice
1st Senate Committee: Judiciary
2nd Committee: Economic Development, Small Business and Regulatory Reform (SB 220)

Second Analysis (4-6-05)

BRIEF SUMMARY: As a package, the bills would:

- Create the Identity Theft Protection Act to make it a felony to use personal identifying information to obtain goods and services without consent.
- Repeal the current identity theft statute.
- Prohibit businesses from denying credit or public utility service to victims of identity theft and establish penalties for violations.
- Clarify the jurisdiction where ID thefts could be prosecuted.
- Extend the statute of limitations for ID thefts to six years after the crime was committed or the identity of the thief was established.
- Create the Social Security Number Privacy Act to prohibit certain uses of SSNs, establish penalties for violations, and provide remedies.

- Establish the right of a victim of ID theft to obtain a police report.
- List ID theft as an unlawful practice of trade or commerce.
- Prohibit—as an unlawful practice of trade or commerce—issuing receipts containing more than the last four digits of a credit card account.
- Prohibit requiring a consumer to provide an SSN as a condition for doing business.
- Prohibit and create penalties for photographing, recording, or electronically transmitting personal identifying information taken, without consent, from credit, debit, and ATM cards and other devices.

FISCAL IMPACT: In most cases, the bills do not appear to have a major fiscal impact. For the impact of each bill, see the Fiscal Information section later in the analysis.

THE APPARENT PROBLEM:

Despite various criminal and consumer protection laws, the problem of identity theft continues to increase. In 2003, the Federal Trade Commission (FTC) recorded almost 215,000 cases of identity theft nationwide, an increase over the 161,836 cases reported in 2002. Identity theft is the practice of using another person's personal information - such as a social security number (SSN), birthdate, mother's maiden name, bank account number, or driver's license number - to make fake IDs, open credit card accounts, open cellular phone accounts, access a person's existing credit card or bank accounts or open new accounts, take out loans (that are not paid back), and conduct any number of personal and business transactions without the knowledge or consent of the person whose name and identity information were used. Often, the victim of identity theft is unaware until he or she attempts to obtain a new credit card, secure a mortgage for a home or a loan for a car, or rent a new apartment. The person then discovers that he or she now has a poor credit rating for unpaid debts incurred in his or her name.

Reportedly, victims of identity theft spend about 600 hours and more than $1,000 trying to clear their names, and it can take many months and even years to undo the damage. When an identity thief is arrested or convicted for a crime, the victim of the identity theft may find that he or she is denied employment for jobs requiring criminal background clearance; some victims have even been arrested and prosecuted for crimes committed by the persons who stole their identities. Businesses are not exempt from identity theft either, and losses due to such theft are generally passed on to consumers. The FTC estimated in a report published in September, 2003, that ID theft cost businesses and consumers $53 billion in 2002.

In recent years, the majority of states have enacted tougher penalties for stealing someone else's identity. Michigan enacted specific penalties for ID-theft related crimes in 1999 (though in 2002, the state ranked sixth in the nation for identity thefts). In December 2003, Congress updated the Fair Credit Reporting Act to provide some protections to identity-theft victims. In July of 2004, the federal Identity Theft Penalty Enhancement Act, which, among other things, adds two years to prison sentences for crimes involving the use of stolen credit cards and other stolen personal data, was signed into law.

Yet, concerns remain. For instance, many victims find that police agencies are reluctant to take ID theft complaints due to lack of clarity over jurisdiction. However, without a police report, victims are unable to avail themselves of federal remedies or to prove to creditors that they were not responsible for debts incurred in their names. Some people are concerned about the widespread use of social security numbers as personal account numbers for health care services and college student numbers and would like to see restrictions on their use by businesses and other institutions. Also, credit card numbers imprinted on receipts at retail establishments, gas stations, restaurants, and hotels make easy targets for would-be thieves to gather sensitive information. In addition, some criminals go as far as using cameras and other recording devices to record and/or transmit pin numbers and account numbers at ATMs. In short, many feel that state laws should go further to reduce the opportunities for ID theft by restricting use of personal identifiers, deter would-be criminals through increased penalties, clarify jurisdictional issues, and enable victims of ID theft to obtain police reports and vital records in a timely manner.

THE CONTENT OF THE BILLS:

The bills would take effect March 1, 2005.

Senate Bill 792

The bill would create the Identity Theft Protection Act. The bill would define "identity theft" as engaging in an act or conduct prohibited in Section 5(1) of the bill. Section 5(1) would make it a crime to use or attempt to use personal identifying information of another person without that person's consent – either with the intent to defraud or otherwise violate the law or by concealing, withholding, or misrepresenting the identity of the individual using or attempting to use the information to commit any unlawful act or to obtain credit, goods, services, money, property, a vital record, medical records or information, or employment. "Consent" would not include authorizing use of personal identifying information if the person granting permission knew that the information would be used to commit an unlawful act.

However, if a person violated Sec. 5(1) by concealing, withholding, or misrepresenting his or her identity, any of the following would be a defense in a civil action or an affirmative defense in a criminal proceeding: the person gave a bona fide gift for the person whose personal information had been used; the person had acted in the lawful pursuit or enforcement of a person's legal rights; the action taken had been authorized or required by state or federal law, rule, regulation, or court order or rule; or the person acted with the consent of the person whose personal identifying information had been used, unless the person giving consent knew the information would be used to commit an unlawful act.

In Section 7, the bill would also specifically prohibit a person from doing any of the following:

- Obtaining or possessing (or attempting to do so) personal identifying information of another person with the intent of using that information to commit identity theft or another crime.
- Selling or transferring (or attempting to do so) personal identifying information of another if he or she 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 crime.
- Falsifying a police report of identity theft, or knowingly creating, possessing, or using a false police report of identity theft.

A violation of the bill's prohibitions under Sections 5 and 7 would be a felony punishable by imprisonment for not more than five years or a fine of not more than $25,000, or both. (Under certain conditions, this penalty would not apply to a violation of a statute or rule administered by a regulatory board, commission, or an officer with authority under state or federal law as specified in the bill if the act were committed by a person subject to and regulated by that statute or rule, or by another person who had contracted with another to use the other person's personal identifying information.) Penalties for violations of Sections 5 and 7 would apply whether the victim or intended victim were dead or alive at the time of the violation. A person could still be charged with, convicted of, or sentenced for any other violation of law committed using information obtained in violation of the bill as well as for any other violation of law committed by the person while violating or attempting to violate the bill's provisions.

It would be a defense in a civil action or an affirmative defense in a criminal proceeding for a violation of Sections 5 and 7 if a person lawfully transferred, obtained, or attempted to obtain the personal identifying information of another for the purpose of detecting, preventing, or deterring identity theft or another crime or the funding a criminal activity. The defendant would bear the burden of proof by preponderance of the evidence to support that defense.

Regarding trade or commerce, a person would be prohibited from the following:

- Denying credit or public utility service to, or reducing the credit limit of, a consumer solely because he or she had been the victim of identity theft. (A consumer would be presumed to be a victim of identity theft if he or she provided a copy of a police report evidencing the claim of being a victim of identity theft and a completed copy of a standardized affidavit of identity theft developed and made available by the Federal Trade Commission or an affidavit of fact that was acceptable to the person for that purpose.)
- Soliciting to extend credit to a consumer without an existing line of credit, or who had not applied for a line of credit within the preceding year, via 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. In addition to any other penalties or remedies allowed under law, a credit card issuer, financial institution, or other lender that violated this

provision – and not the consumer – would be liable for the amount of the check and certain fees if used by an unauthorized user.

- Soliciting to extend credit to a consumer who did not have a credit card, or who had not applied for one within the preceding year, by sending the consumer a credit card. A credit card issuer, financial institution, or other lender that violated this provision would be liable for charges, interest, or finance charges if the card were used by an unauthorized person.
- Extending credit without exercising reasonable procedures to verify the identity of the consumer. Compliance with regulations issued by the U.S. Department of Treasury for depository and other financial institutions under the USA Patriot Act would be considered compliance with this provision. This provision would not apply, however, to a purchase of a credit obligation in an acquisition, merger, purchase of assets, or assumption of liabilities or changes to or review of an existing credit account.

A violation of the above would be a misdemeanor punishable by imprisonment for not more than 30 days, a fine of not more than $1,000, or both. This penalty would not affect the availability of any civil remedy for a violation of the bill, the Michigan Consumer Protection Act, or any other state or federal law.

If necessary to enforce the bill or prevent identity theft, a law enforcement agency or victim of identity theft could verify information from a vital record from a local registrar as provided by Section 2881(2) of the Michigan Public Health Code. A state or local registrar could provide to an individual offering proof of being a victim of identity theft the following information:

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

Providing the registrar with a copy of a police report evidencing the claim of being a victim of identity theft along with (if available) an affidavit of identity theft would be sufficient proof. The affidavit of identity theft would be in a form developed by the state registrar in cooperation with the attorney general.

A state or local registrar could also provide the following information to a law enforcement agency:

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

Under provisions of the health code, a law enforcement agency can request an administrative use copy of a vital record from a state registrar. Under the bill, an

administrative use copy could also be requested from a local registrar if the request was in writing and contained a statement that the agency required information from a vital record beyond the information the local registrar can verify under the bill and contained the agreement by the law enforcement agency that it will maintain the administrative use copy in a secure location and destroy the copy by confidential means once it is no longer needed.

The bill also would repeal Section 285 of the Michigan Penal Code. Section 285 currently makes it a five-year felony to obtain personal identity information of another with the intent to unlawfully use that information.

House Bill 6169

The bill would amend the Code of Criminal Procedure (MCL 777.14h and 777.16o) to specify that the crimes of identity theft and of obtaining, possessing, selling, or transferring personal identifying information of another or falsifying a police report with intent to commit identity theft would carry a statutory maximum term of imprisonment of five years. Both crimes would be Class E felonies against the Public Order.

Furthermore, the bill would delete the current reference to a violation of Section 750.285 of the Michigan Compiled Laws, which would be repealed by Senate Bill 792. The bill would also make a technical change; a violation of MCL 750.303 would refer to gaming instead of gambling.

Senate Bill 793

The bill would add a new section to Chapter II of the Code of Criminal Procedure (MCL 762.10c) to specify that a violation of the Identity Theft Protection Act or conduct prohibited under former Section 285 of the Michigan Penal Code (which would be repealed by Senate Bill 792), or a violation committed in furtherance of or that arose from the same transaction, could be prosecuted in one of the following jurisdictions:

- Where the offense occurred.
- Where the information used to commit the violation was illegally used.
- Where the victim resided.

If a person were charged with more than one violation and the violations could be prosecuted in more than one jurisdiction, then any of the above jurisdictions would be considered a proper jurisdiction for all of the violations.

Senate Bill 795

The bill would create the Social Security Number Privacy Act to prohibit certain uses of social security numbers (SSN), establish penalties for violations, and provide remedies. The bill would apply to a person, association, company, elementary or secondary public

or nonpublic school, vocational school, college or university, trade school, state or local governmental agency or department, or other legal entity.

Under the bill, the specified entities could **not** intentionally do any of the following with all or more than four sequential digits of the SSN of an employee, student, or other individual:

- Publicly display the SSN. "Publicly display" would mean, except as otherwise provided in the bill, to exhibit, hold up, post, or make visible or set out for open view to members of the public or in a public manner. It would include open view on a computer device, computer network, website, or other electronic medium or device.
- Use the SSN as the primary account number for an individual. However, the bill would provide several exceptions for specified administrative uses (i.e., to verify an individual's identity related to an account, transaction, product, employment, or service; investigate a claim, credit, criminal, or driving history; detect, prevent, or deter identify theft or other crime; lawfully pursue or enforce a person's legal rights; lawfully investigate, collect, or enforce a child or spouse support order; or 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) or if certain conditions were met (i.e., the use began prior to the bill's effective date or the use was ongoing and continuous).
- Visibly print the SSN on any ID badge or card, membership card, or permit or license. A person or entity that has implemented or does implement a plan or schedule establishing a specific date for compliance with this provision would not be subject to this provision until January 1, 2006 or the completion date specified in the plan or schedule, whichever was earlier.
- Require an individual to transmit the SSN over the Internet or a computer system or network unless the connection was secure or the transmission encrypted.
- Require an individual to use or transmit the SSN to gain access to an Internet website or computer system or network unless the connection was secure, the transmission encrypted, or a password or other unique personal ID number or authentication device was first required to gain access to the website or computer system or network.
- Include the SSN in or on a document or information mailed or sent to an individual if the digits were visible on or, without manipulation, from outside the envelope or packaging.
- Beginning January 1, 2006, except as allowed in the bill, include the SSN in any document or information mailed to an individual.

Knowingly violating the above prohibitions would be a misdemeanor punishable by imprisonment for not more than 93 days, a fine of up to $1,000, or both. Further, a civil action could be brought to recover actual damages. If the person knowingly violated the bill's prohibitions, an individual could recover actual damages or $1,000, whichever was greater, and could also recover reasonable attorney fees. Not later than 60 days before filing a civil action, an individual would have to 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.

The above prohibited acts would not apply to a use of all or more than four sequential digits of a SSN that was authorized or required by state or federal statute, rule, or regulation, by court order or rule, or pursuant to legal discovery or process or use by a Title IV-D agency, law enforcement agency, court, or prosecutor as part of a criminal investigation or prosecution.

A specified entity that obtained one or more SSN in the ordinary course of business would have to create a privacy policy that, at the least, ensured confidentiality of the SSNs; prohibited unlawful disclosure; limited accessibility to information or documents containing SSNs; described proper disposal of documents containing SSNs; and established penalties for violations of the privacy policy. The privacy policy would have to be published in an employee handbook, in a procedures manual, or in one or more similar documents, which could be made available electronically. This provision would not apply to a person (business) who possessed SSNs in the ordinary course of business and in compliance with the Fair Credit Reporting Act or Gramm-Leach-Bliley Act. The civil actions discussed above would not apply to violations of a privacy policy created under the bill's provisions or in compliance with these two federal statutes if the entity had taken reasonable measures to enforce its policy and to correct and prevent the reoccurrence of any known violations.

In addition, all or more than four sequential digits of a SSN contained in a public record would be exempt from disclosure under the Freedom of Information Act.

House Bill 6172

The bill would amend the Code of Criminal Procedure (MCL 767.24) to establish a six-year statute of limitations for identity theft. Specifically, an indictment could be found and filed within six years after an offense of identity theft or attempted identity theft had been committed. If evidence had been obtained but the individual committing the offense had not been identified, an indictment could be found and filed at any time up to six years after the person was identified.

The bill also contains an amendment to the code that applies to the extension or tolling of limitations periods in general. It provides that when an extension or tolling of the limitations period is provided for an offense, it applies to any violations for which the limitations period has not expired when the extension or tolling takes effect.

Senate Bill 1384

The bill would amend the Crime Victim's Rights Act (MCL 780.754a et al.) to establish the right of a victim of identity theft to obtain a police report from a law enforcement agency in a jurisdiction where the alleged crime could be prosecuted as provided by provisions of the Code of Criminal Procedure that would be added by Senate Bill 793.

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

These bills would all amend the Michigan Consumer Protection Act. The act has a long list of unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce that are unlawful. The bills would all amend the same section of the act (MCL 445.903) as follows:

House Bill 6174 would add a violation of Section 11 of the Identity Theft Protection Act, which would be created by Senate Bill 792, to the list of offenses constituting unlawful practices of trade or commerce.

Senate Bill 220 would add to the list of offenses the issuing or delivering of a receipt when a credit card or debit card was used for payment in a consumer transaction if the receipt displayed any part of the expiration date of the card or more than the last four digits of the consumer's account number. This would not apply to receipts on which the account number or expiration date is handwritten, mechanically imprinted, or photocopied.

The above would apply to consumer transactions occurring on or after March 1, 2005. However, if a credit or debit card receipt for a transaction is printed by an electronic device, the bill would apply July 1, 2005 if the device had been in service on or before March 1, 2005. If the electronic device is placed in service after March 1, 2005, the bill's provisions would apply July 1, 2005 or the date the device was placed in service, whichever was later.

Senate Bill 657 would add to the list of offenses constituting unlawful trade practices the act of 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 the following applied:

- The selling, leasing, providing, terms of payment, or transaction included an application for or an extension of credit to the consumer.
- The disclosure was required or authorized by applicable state or federal statute, rule, or regulation.
- The disclosure was requested by a person to obtain a consumer report for a permissible purpose described in Section 604 of the Fair Credit Reporting Act.
- The disclosure was requested by a landlord, lessor, or property manager to obtain a background check of the individual in conjunction with the rent or leasing of real property.
- The disclosure was requested from an individual to effect, administer or enforce a specific telephonic or other electronic consumer transaction that is not made in person but requested or authorized by the individual if it was to be used solely to confirm the identity of the individual through a fraud prevention service database. The consumer good or service would still have to be provided upon verification of his or her identity if he or she refused to provide his or her SSN but provided other information or documentation that could be used by the person to verify his

or her identity. The person could inform the consumer that verification through other means than use of the SSN could cause a delay in providing the service or good.

[The bill would incorporate the amendments to the act made by House Bill 6174 and Senate Bill 220, but would not incorporate the amendments added by Senate Bill 798.]

In addition, the bill would specify that its provisions would not apply to either of the following:

- Providing a service related to the administration of health-related or dental-related benefits or services to patients, including provider contracting or credentialing. The bill specifies that this provision is intended to limit the application of the rest of the bill's provisions and is not intended to imply that the Michigan Consumer Protection Act would otherwise apply to health-related or dental-related benefits.
- An employer providing benefits or services to an employee.

Senate Bill 798 would add to the list of offenses denying credit or public utility service to, or reducing the credit limit of, a consumer who was a victim of identity theft under the Identity Theft Protection Act, if the person denying the credit or public utility service knew that the consumer had been a victim of identity theft. A person would be presumed to be a victim of identity theft if he or she possessed a valid police report evidencing his or her claim.

(Note: When bills amending the same section of a statute are signed into law on the same day, the bill that was filed last with the Secretary of State supersedes the bills signed and filed before it. Since Senate Bill 657 was the last bill of these four to be filed, the language in Senate Bill 657 supersedes and replaces the amendments made to Section 903 by Senate Bills 798 and 220 and House Bill 6174. However, whereas Senate Bill 657 incorporated the same language added by Senate Bill 220 and House Bill 6174, it did not incorporate the language added by Senate Bill 798; therefore, in effect this provision will not become law.)

House Bill 6177

The bill would add a new section to the Michigan Penal Code to prohibit a person who was not party to a transaction involving a financial transaction device from 1) secretly or surreptitiously photographing or otherwise capturing or recording, electronically or by any other means; or 2) distributing, disseminating, or transmitting – electronically or by other means – personal identifying information from the transaction without the consent of the individual. A violation would be a misdemeanor punishable by imprisonment for up to one year, a fine of not more than $1,000, or both. In addition, a person could be charged with, convicted of, or punished for any other violation of law committed by the person while violating or attempting to violate the new offense.

The bill would not prohibit the capture or transmission of personal identifying information in the ordinary and lawful course of business, and would not apply to a Michigan or federal peace officer while in the lawful performance of his or her duties.

"Financial transaction device" is defined in Section 157m of the code and includes an electronic funds transfer card; credit card; debit card; point-of-sale card; and various cards, plates, codes, account numbers, personal identification numbers, driver's license numbers, etc. used to obtain money, credit, goods, services, or providing access to a deposit account. "Personal identifying information" is defined in House Bill 6168 and Senate Bill 792, which would create the Identity Theft Protection Act.

BACKGROUND INFORMATION:

Consumers can find information on protecting themselves from identity theft or help if they are victims of identity theft at the following sites:

The Office of the Attorney General: www.michigan.gov

Federal Trade Commission: www.consumer.gov/idtheft/

Identity Theft Prevention and Survival Site: www.identitytheft.org

Identity Theft Resource Center: www.idtheftcenter.org

FBI Internet Fraud Complaint Center: www.jfccfbi.gov

Social Security Administration: www.ssa.gov; 800-772-1213

U.S. Department of Justice Identity Theft and Fraud Information: www.usdoj.gov/criminal/fraud/idtheft.html

U.S. Postal Inspection Service: www.usps.com/websites/depart/inspect/

U.S. Secret Service: www.secretservice.gov

Privacy Rights Clearinghouse: www.privacyrights.org; 619-298-3396

FISCAL INFORMATION:

Senate Bill 792 would have an indeterminate impact on the state and local units of government; fiscal impact likely would be minimal, assuming that there was little change in the numbers of convictions or the types of sentences imposed for identity theft offenses. In 2002, there were 53 felony convictions under the current identity theft law which carries the same maximum penalties (five year prison term) as proposed by the bills under analogous provisions. Of those 53 sentences, 11 were state prison terms, 37 were probation, 3 were jail, and 2 were "other" (delayed or suspended sentences, Holmes

Youthful Trainee Act, etc.). Costs of prison and felony probation supervision fall to the state, while those of jail fall to the affected county. The Department of Corrections (MDOC) puts the annual cost of felony probation at $1,977 per offender. Costs of prison incarceration depend on security level and vary widely between facilities; the MDOC reports the average annual cost per prisoner in FY 2004-05 to be $29,090. Jail costs vary from county to county. Increasing maximum fines from $10,000 to $25,000 could increase revenues for local libraries, who are the constitutionally-designated recipients of penal fines.

House Bill 6169 would amend sentencing guidelines consistent with Senate Bill 792 and therefore would have no direct fiscal impact.

Senate Bill 793 would have no fiscal impact on the state, and an indeterminate fiscal impact on local units of government, depending on where violations were prosecuted.

House Bills 6177 and Senate Bill 795 would have no fiscal impact on the state, and an indeterminate fiscal impact on local units of government. Costs of misdemeanor sanctions would fall to local units of government, and would vary according to the county involved. Penal fine revenue is constitutionally dedicated to local libraries.

By extending the statute of limitations on identity theft violations, House Bill 6172 could enable more convictions to be obtained for those violations, with accompanying costs for the state and local units of government, depending on the numbers of convictions and the penalties imposed. If additional penal fine revenues were collected, those revenues would go to local libraries.

Senate Bill 1384 would have an indeterminate fiscal impact on local law enforcement agencies, depending on the numbers and length of police reports requested.

House Bill 6174 and Senate Bills 220, 657, and 798 would have an indeterminate fiscal impact on state and local units of government. It is not known what costs for enforcement would be, and the amount of revenue generated from penalty fines would depend on the number of violations.

ARGUMENTS:

For:

Identity theft affects individuals and society at large. Costs incurred by individuals and businesses total in the billions every year. Lives are shattered as credit and reputations are damaged. Though there are steps that individuals can take to protect the personal information used by ID thieves, more needs to be done at the state level to ensure that appropriate protections and remedies are available in law. It is unlikely that all attempts to steal another's identity for criminal purposes can be thwarted, but the bill package as a whole addresses many existing weaknesses.

Response:

According to recent research by a Michigan State University professor, up to 70 percent of identity theft can be traced back to an employee or business owner stealing personal identifying information from customers. Yet, some of the bills have been watered down considerably since their introduction, to the point of appearing to protect businesses more than consumers. In particular, according to media reports, health-related and financial industries appear to account for the majority of identity theft that originates with employees. However, provisions that would have greatly restricted even the internal use of social security numbers have been relaxed in response to industry claims of increased costs. If allowances must be made to reduce administrative burdens on businesses caused by restrictions on the use of personal identifiers, then businesses should also be held more accountable in assuming the losses to customers caused by their employees' criminal use of that information.

For:

Senate Bill 792 would increase the penalties for identity theft and would expand their application. For example, the bill would now criminalize the selling or transferring of personal identifying information (when knowing the information would be used illegally) and falsely filing a report of identity theft, which apparently some do in order to avoid responsibility for debts they have incurred. "Personal identifying information" would be defined to include such things as mother's maiden name, driver's license numbers, and bank account numbers. The last is particularly important as some thieves use such information to access and drain checking and savings accounts. A person could be prosecuted for identity theft if they targeted a business as well as an individual.

The bill would also add important protections in law for victims of identity theft. A business or utility could not deny credit or service to a victim of identity theft solely because he or she had been so victimized. The types of information that could be included in certain types of unsolicited credit and credit card offers would be restricted; this should reduce the ability to use stolen mail as a means to obtain enough personal identifying information to open lines of credit in another's name. In addition, a business would have to execute procedures to verify the identity of a consumer before extending credit; reportedly, some lenders do very little to ensure that the person getting the credit is the person whose name is on the account. A business could be fined up to $1,000 for each violation and a person representing the business could be imprisoned for up to 30 days.

The bill would also establish the right in law of an ID theft victim to learn whether or not certified copies of his or her birth records or other records had been requested or issued. Law enforcement agencies could obtain administrative use copies of vital records (i.e., birth or death records), as well as other information such as the names and addresses of persons requesting copies of the vital records of an identity theft victim needed to enforce the bill or investigate or prevent ID theft. Yet, legitimate uses of personal identifying information would be also be protected.

For:

Some victims of identity theft report difficulties in filing a policy report because law enforcement agencies are not always clear on which agency has jurisdiction – the agency located in the jurisdiction where the victim lives or the jurisdiction where the identity thief committed the crime. Since many ID theft crimes occur over the Internet or through other electronic means, the crimes may be committed many miles away or in another state. ID thefts can and should be reported to federal agencies, but Senate Bill 793 would also clarify for state law enforcement agencies that identity theft crimes could be prosecuted in any or all of three different places: where the offense occurs, where the victim lives, or where the information is used illegally to violate the Identity Theft Protection Act. This should enable victims to quickly and easily file police reports. Senate Bill 1384 would establish an ID theft victim's right to obtain a copy of the police report. Having copies of police reports to send to credit bureaus and financial institutions are a necessary first step in the arduous process of clearing a damaged name and credit.

For:

In general, the statute of limitations for most criminal offenses and civil actions are two to three years from the time of the violation. In ID theft cases, however, it may be months or years before a person realizes he or she is a victim of ID theft. And, unlike many types of crimes, a victim of ID theft may have never come in physical contact with the offender because the personal identifying information used to commit the fraud may have been taken off the Internet, from dumpsters in an alley, or from files in a business far from the victim; the commission of the fraud itself may well have been committed in another city or state. Therefore, it can be a long and painstaking process for law enforcement to trace an ID theft crime back to the perpetrators.

House Bill 6172 will aid prosecutors and victims by extending the statute of limitations for ID theft crimes to six years from the date of the commission of the crime or six years after the identity of the ID thief becomes known.

For:

Some criminals use digital, electronic, or photographic means to capture and/or transmit personal identifying information such as PINs and account numbers when customers use ATMs or debit and credit card numbers from swipe machines. House Bill 6177 would specifically prohibit such conduct and subject a perpetrator to up to a year in jail and/or a $1,000 fine.

For:

Several bills in the package would amend the provision of the Consumer Protection Act designating practices as unlawful because they are unfair, unconscionable, or deceptive. House Bill 6174 and Senate Bill 798 would specify that a violation of the Identity Theft Protection Act would be an unlawful method or practice in the conduct of trade or commerce and so would trigger penalties and remedies under the Consumer Protection Act.

In addition, Senate Bill 220 would prohibit businesses from displaying the entire credit or debit card account number, or the card's expiration date, on a receipt. This should decrease the chance that a consumer's account number could be stolen and used by an employee of the establishment or by a person who either found or stole the receipt. (For instance, it is not unusual for gasoline customers who "pay at the pump" to forget to take their receipts out of the pump before driving away.) Businesses would be given ample time to retool their devices so that no more than the last four digits would appear on a receipt.

Furthermore, Senate Bill 657 would prohibit a business from requiring a consumer to provide his or her social security number as a condition to buying a product or receiving a service unless the purchase, provision, payment, or transaction was part of an application for or an extension of credit or was otherwise required or authorized by state or federal law. In addition, it would provide statutory authority for consumers to provide other information to establish their identities in lieu of giving out their SSNs, although they may have to wait a bit longer before receiving the requested goods or services. Along with the provisions contained in the Social Security Number Privacy Act, which would be created by Senate Bill 795, this prohibition should reduce the number of situations in which a consumer must provide his or her SSN. Any reduction in the usage of SSNs to transact business should begin to decrease the ability of would-be thieves to obtain and use SSNs to commit identity theft.

For:

The Social Security Number Privacy Act, created by Senate Bill 795, would protect consumers from identity theft by restricting the use of social security numbers. Under the bill, colleges could no longer use SSNs as student numbers or print exam scores next to SSNs on a publicly displayed list; health insurers couldn't use SSNs as subscriber or member numbers except as allowed by the bills; SSNs could not be displayed on ID badges or cards (i.e., health insurance cards), membership cards, permits, or licenses; and businesses would be restricted in their use of SSNs in mailings. When inclusion of an SSN in a mailing was allowed under the bill, the individual or business would have to ensure that the SSN was not visible from the outside of the envelope.

Companies doing business over the Internet could not require all or more than four sequential digits to be transmitted unless they provided a secure site or encrypted the transmission. In addition, companies that currently require submission of an SSN for entry onto a website would have to first ensure that the connection was secure, the transmission encrypted, or require the use of a unique password to gain initial entry to the site before requiring the use of a SSN to access a particular account.

Furthermore, the bill would clarify that SSNs, or more than four sequential digits of a SSN, would not be allowed to be disclosed under the Freedom of Information Act. This would clarify that even court documents, which sometimes contain SSNs, would have to be redacted to protect the individuals involved from identity theft.

The 93-day maximum term of imprisonment imposed for a violation would trigger certain fingerprint and recordkeeping requirements, including sending a copy of the prints

to the FBI for a search of the national fingerprint database. A victim would also be given the statutory right to bring a civil suit to recover actual damages or, if the violation was committed knowingly, at least $1,000.

As a whole, the bill's provisions should decrease access to SSNs and deter would-be thieves with the criminal penalties and civil remedies, thereby increasing protection to consumers without overly burdening businesses.

For:

Senate Bill 795, which creates the Social Security Number Privacy Act, was amended to address concerns raised by insurance companies and financial institutions regarding the use of SSNs for administrative purposes. For example, insurance companies that administer 401k plans may receive a check from an employer along with a list of SSNs and dollar amounts – the dollar amounts being a particular employee's 401k contribution. Industry members believed earlier versions of the bill did not make it clear if this practice would be allowed. Using any other type of identifier could result in errors (such as a contribution being credited to the wrong employee) as well as increased costs and workload (redoing computer and accounting software to create a different personal identifier, but then also having to generate tax records with the SSN). Similarly, other businesses wondered if they could legally transmit SSNs that are part of delinquent accounts to collection agencies without incurring penalties under the bills.

The enrolled version addresses these concerns by including, as part of the allowable administrative use of SSNs, services provided to employers or others that involve providing or administering employee or health insurance or membership benefits, claims, or retirement programs, as well as administering ownership of stock or other investments (i.e., 401k plans).

Further, some businesses wanted a provision eliminated that would have required all businesses that obtain SSNs in the ordinary course of business to develop written privacy policies (the contention was that this provision is duplicative of other regulatory statutes and also would be burdensome for small businesses to adhere to). Under the bill, certain businesses that are regulated by the Fair Credit Reporting Act or Gramm-Leach-Bliley Act would be exempted from this requirement. However, since the written privacy policy and other prohibitions of using SSNs represent important consumer safety elements that many businesses do not currently follow, it is important to not eliminate them entirely. After all, some businesses keep documents containing SSNs in unlocked drawers in unlocked offices. Surely the savings to businesses, even small businesses, realized from decreasing incidents of identity theft would more than offset costs associated with incorporating more security measures or establishing a new system to identify customers without using SSNs.

Legislative Analyst: Susan Stutzky
Fiscal Analysts: Marilyn Peterson
Robin Risko

■ This analysis was prepared by nonpartisan House staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.