

ID THEFT VIA THE INTERNET: FALSE PRETENSES

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

Senate Bill 149 with House committee amendments

Senate Bill 150 as passed by the Senate

Sponsor: Sen. Bruce Patterson

House Committee: Judiciary

Senate Committee: Judiciary

Complete to 9-8-09

A SUMMARY OF SENATE BILLS 149 AND 150 AS REPORTED BY THE HOUSE JUDICIARY COMMITTEE 4-23-09

Together, the bills would:

- Add to the list of criminal conduct prohibited under the Identity Theft and Protection Act.
- Increase the penalties for certain violations of the act.
- Prohibit certain conduct and make that conduct subject to civil suits.
- Allow the attorney general to investigate certain prohibited conduct and compel persons under investigation to appear and produce related evidence.
- Place the increased maximum sentence in the sentencing guidelines.

Senate Bill 150 is tie-barred to Senate Bill 149, and both bills would take effect 90 days after enactment.

Senate Bill 149

The bill would amend the Identity Theft Protection Act (MCL 445.63 et al) to do the following:

Revise definition of "personal identifying information." The act 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 identification card number, Social Security number, place of employment, employee ID number, employer or taxpayer ID number, government passport number, health insurance ID number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number, or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

Under the bill, "personal identifying information" also would include any other account password in combination with sufficient information to identify and gain access to a person's financial account, and a person's automated or electronic signature or biometrics.

Criminal prohibitions. The act currently prohibits a person from doing any of the following:

- Obtaining or possessing, or attempting to obtain or possess, personal identifying information of another person with the intent to use it to commit identity theft or another crime.
- Selling or transferring, or attempting to sell or transfer, someone else's personal identifying information if the person knows or has reason to know that the specific intended recipient will use or attempt to use the information, or further transfer it 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 is a felony punishable by up to five years' imprisonment and/or a maximum fine of \$25,000.

The bill would also prohibit a person from doing any of the following with the intent to use the personally identifying information to commit identity theft or crime:

- Making any electronic mail or other communication under false pretenses purporting to be by or on behalf of a business, without its authority or approval, and using that electronic mail or other communication to induce, request, or solicit any individual to provide personal identifying information.
- Creating or operating a webpage that represented itself as belonging to or being associated with a business, without the business's authority or approval, and inducing, requesting, or soliciting any user of the internet to provide personal identifying information.
- Altering a setting on a user's computer or similar device or software program through which the user could search the internet and causing the internet user to view a communication that represented itself as belonging to or being associated with a business, and that had been created or was operated without the authority or approval of that business, and inducing, requesting, or soliciting any internet user to provide personal identifying information.

A violation of the current and proposed prohibitions would be punishable by imprisonment for not more than 10 years and/or a fine of not more than \$500,000.

"False pretenses" would include "a false, misleading, or fraudulent representation, writing, communication, statement, or message, communicated by any means to another person that the maker of the representation, writing, communication, statement, or message knows or should have known is false or fraudulent." The false pretense could be a representation regarding a past or existing fact or circumstance or a representation regarding the intention to perform a future event or to have a future event performed.

"Webpage" would mean a location that has a uniform resource locator or URL with respect to the world wide web or another location that can be accessed on the internet.

Civil action. Another section of the bill would also prohibit a person from taking the actions described above even without the intent to use the personal identifying information to commit identity theft or another crime. In those cases civil actions could be taken in response.

The attorney general or an interactive computer service provider harmed by such a violation could bring a civil action against a person who committed the violation. A person bringing an action could recover one of the following:

- Actual damages, including reasonable attorney fees.
- In lieu of actual damages, reasonable attorney fees plus the lesser of \$5,000 per violation or \$250,000 for each day that a violation occurred.

The prohibition would not apply to a law enforcement officer engaged in the performance of official duties or any other individual authorized to conduct lawful investigations, while engaged in a lawful investigation.

"Interactive computer service" would mean an information service or system that enables computer access by multiple users to a computer server, including a service or system that provides access to the internet or to software services available on a server.

Attorney general investigations. If the attorney general had reason to believe that a person had committed one of the proposed violations, with or without intent to commit identity theft or another crime, he or she could investigate the person's business transactions. The attorney general could require the person to appear, at a reasonable time and place, to give information under oath and to produce documents and evidence necessary to determine whether the person was in compliance with the requirements.

Exemption from liability. Under the bill, an interactive computer service provider could not be held liable under any provision of Michigan law for removing or disabling access to an internet domain name controlled or operated by the registrar or by the provider, or to content that resided on an internet website or other online location controlled or operated by the provider, that the provider believed in good faith was used to engage in a violation of the act.

The bill specifies that the act would not apply to a telecommunications provider's or internet service provider's good faith transmission or routing of, or intermediate temporary storing or caching of, personal identifying information.

Senate Bill 150

The bill would amend the Code of Criminal Procedure (MCL 777.14h) to increase the maximum term of imprisonment from 5 years to 10 years for soliciting, obtaining,

possessing, selling, or transferring personal identifying information of another or falsifying a police report with intent to commit identity theft. The bill would also raise the crime from a Class E felony against the public order to a Class D felony.

HOUSE COMMITTEE ACTION:

An amendment to Senate Bill 149 was adopted that eliminated a provision crediting any damages collected by the attorney general for the costs of investigating, enforcing, and defending the act. In addition, amendments were adopted that eliminated the minimum term of imprisonment of one year and the minimum fine of not less than \$5,000 for violations of prohibited conduct.

BACKGROUND INFORMATION:

In "Conning the Curious", an article about Internet "phishing" in the January-February AARP Bulletin, the author details a spam email that flooded inboxes in the fall of 2008. The subject line read, "We have hijacked your baby". Those who opened the email found a demand of \$50,000 for the return of their child, written in poor English, and a closing line that baited readers: "We has attached photo of your fume [family]." According to the article, "[t]hose who clicked on the attachment unleashed a computer virus designed to steal the user's passwords and gain access to online bank accounts and other personal information." The use of such techniques by scammers to obtain information needed to commit identity theft is on the increase.

Senate Bill 149 would address the conduct illustrated above whereby individuals use email or other communication under false pretenses (e.g., pretending to be from a bank or other legitimate business), look-a-like webpages of legitimate businesses or agencies, or technology that takes an Internet user to a look-a-like webpage instead of the real site in order to solicit individuals to provide their personal identifying information with the sole intent to use that information to commit identity theft or other crimes. Enactment of the bill would increase the penalties for committing crimes currently prohibited in the Identity Theft Protection Act and apply the new penalties to the new crime categories. In addition, the bill would create a civil action against a person who violated the prohibitions that would allow the attorney general, as well as Internet service providers (ISP), to collect for damages if harmed by the criminal conduct. Further, the bill would encourage ISPs to assist in attempts to stop those who would engage in the prohibited conduct by providing liability for any ISP who removed or disabled an Internet site believed in good faith to be engaging in a violation of the act. The companion bill, Senate Bill 150, would place the maximum term of imprisonment for the prohibited acts within the sentencing guidelines.

FISCAL IMPACT:

Senate Bill 149 would have an indeterminate fiscal impact on the judicial branch. Any fiscal impact would be a function of the court costs associated with prosecuting new cases. Any penal fine revenue would go to the support of public libraries.

POSITIONS:

The Department of State Police indicated support for the bills. (8-19-09)

Comcast indicated support for the bills. (8-19-09)

The ACLU of Michigan indicated support for the bills. (8-19-09)

AT&T indicated support for the bills. (8-19-09)

Legislative Analyst: Susan Stutzky
Fiscal Analyst: Ben Gielczyk

■ 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.