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 149 and 150 (as enacted)
Sponsor: Senator Bruce Patterson
Senate Committee: Judiciary
House Committee: Judiciary

PUBLIC ACTS 318 & 319 of 2010

Date Completed: 2-24-11

RATIONALE

The practice of "phishing" is a relatively new twist on the existing and growing crime of identity theft. Phishing involves attempting to acquire, or acquiring, sensitive information such as on-line usernames or passwords, credit card numbers, or personal identifying information, by baiting computer users with false information that appears to be from a legitimate, trustworthy entity. In phishing scams, which typically are carried out by e-mail or instant messaging, on-line communications purporting to be from such entities as banks or other financial services websites, reservation and payment sites, or popular commercial or common-use websites, are commonly used to lure unsuspecting victims into linking to other websites and providing financial or personal identity information. Not all phishing requires the use of a fake website, though. Sometimes, messages that claim to be from a bank, for example, instruct users to dial a telephone number regarding problems with an account. When the phone number is called, voice prompts tell users to enter their account number or personal identification number (PIN).

While public awareness, computer user training, and on-line security measures have been used to combat phishing scams, some people feel that the Identity Theft Protection Act should include specific prohibitions against, and significant penalties for, attempting to obtain personal information through false pretenses.

CONTENT

Senate Bill 149 amends the Identity Theft Protection Act to do all of the following:

- **-- Prohibit communicating under false pretenses to request personal identifying information, creating or operating an unauthorized webpage to solicit personal identifying information, or altering a computer or software setting to solicit personal identifying information, with or without the intent to commit identity theft or another crime.**
- **-- Apply criminal penalties for identity theft violations to violations described above that include intent to commit identity theft or another crime.**
- **-- Allow the Attorney General, or an interactive computer service provider, to bring a civil action against a person who committed a violation described above without intent to commit identity theft or another crime.**
- **-- Exempt a law enforcement officer engaged in his or her official duties, or any other investigator engaged in a lawful investigation, from the prohibition that does not include intent to commit identity theft or another crime.**
- **-- Exempt an interactive computer service provider from liability under the Act for certain actions.**
- **-- Expand the definition of "personal identifying information".**

Senate Bill 150 amends the Code of Criminal Procedure to revise the sentencing guidelines description of certain identity theft violations.

The bills will take effect on April 1, 2011. Senate Bill 150 was tie-barred to Senate Bills 149 and 223 (Public Act 315 of 2010).

(Senate Bill 223, which also will take effect on April 1, 2011, amends the Identity Theft Protection Act to specify graduated penalties for second and third or subsequent violations of the Act; increase the maximum term of imprisonment for certain misdemeanor violations; and subject certain property to forfeiture for a violation of the Act.)

Senate Bill 149

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 includes 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 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. A second violation is punishable by up to 10 years' imprisonment and/or a maximum fine of $50,000. A third or subsequent violation is punishable by up to 15 years' imprisonment and/or a maximum fine of $75,000. (As noted above, Public Act 315 of 2010 adds these penalties for repeat offenses.)

Subject to the same penalties, the bill also prohibits a person from doing any of the following with the intent to use the personal identifying information to commit identity theft or another 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 represents 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 may search the internet and causing the internet user to view a communication that represents itself as belonging to or being associated with a business, and that has been created or is operated without the authority or approval of that business, and inducing, requesting, or soliciting any internet user to provide personal identifying information.

Under the bill, "false pretenses" includes "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 may 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" means 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

The bill prohibits a person from taking an action that would be a criminal offense under the bill (as described above), but without intent to use the personal identifying information to commit identity theft or another crime.

The Attorney General or an interactive computer service provider harmed by a violation may bring a civil action against a person who violates the prohibition. A person bringing an action may 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 occurs.

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

The bill defines "interactive computer service" as 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 Investigation

If the Attorney General has reason to believe that a person has committed one of the violations described above, with or without intent to commit identity theft or another crime, the Attorney General may investigate the person's business transactions. The Attorney General may 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 is in compliance with the requirements.

Liability Exemption

Under the bill, an interactive computer service provider may 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 resides on an internet website or other online location controlled or operated by the provider, that the provider believes in good faith is used to engage in a violation the Act.

The bill specifies that the Act does 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

A violation of Section 7 of the Identity Theft Protection Act (which provides for the criminal offense described in Senate Bill 149) is a Class E public order felony, with a statutory maximum sentence of five years' imprisonment. The Code describes the offense as to obtain, possess, sell, or transfer personal identifying information of another or falsify a police report with intent to commit identity theft. The bill also refers to "solicit".

MCL 445.63 et al. (S.B. 149)
777.14h (S.B. 150)

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

Those who practice phishing, or "phishers", send an e-mail or pop-up message that claims to be from a business or organization with which the recipient may have dealings, according to OnGuard Online (http://onguardonline.gov, a website maintained by the Federal Trade Commission to provide practical tips from the Federal government and the technology industry to help guard against internet fraud and protect personal information). The

phishers' message may ask the recipient to update, validate, or confirm account information, perhaps even warning of dire consequences for failure to reply. Typically, the message directs the computer user to a website that appears to be legitimate but actually is a counterfeit whose sole purpose is to trick the person into divulging personal information so the phishers can run up financial charges or commit crimes in the name of the victim.

The nature of phishing scams, i.e., using electronic communication to target victims, makes it a particularly efficient method for perpetrators to secure personal identifying information in order to commit identity theft. Obtaining or attempting to obtain this information through phishing techniques should be specifically prohibited and subject to criminal penalties and civil remedies. According to the National Conference of State Legislatures (NCSL), 22 other states have antiphishing laws on the books. Senate Bills 149 and 150 provide for Michigan to join those states by prohibiting communicating under false pretenses to request personal identifying information, creating or operating an unauthorized webpage to solicit personal identifying information, or altering a computer or software setting to solicit personal identifying information. The bills will help to combat identity theft in this era of increased use of electronic communication.

Supporting Argument

Senate Bill 149 will encourage internet service providers (ISPs) to assist in the fight against phishing by providing that an ISP may not be held liable for removing or disabling access to an internet site that the provider believes in good faith was used to engage in a violation of the Identity Theft Protection Act.

Supporting Argument

In addition to protecting against identity theft through phishing scams, Senate Bill 149 acknowledges the use of similar techniques in legitimate investigations by law enforcement agencies or private investigators. The bill specifies that the prohibitions do not apply to a law enforcement officer engaged in the performance of official duties or any other individual authorized to conduct lawful investigations while that individual is engaged in such an investigation.

Legislative Analyst: Patrick Affholter

FISCAL IMPACT

Senate Bill 149 will result in some staffing costs to the Office of Attorney General associated with bringing civil actions against and/or investigating the business transactions of people violating the new prohibitions. The majority of these costs, however, may be recovered through any damages awarded to the Attorney General's office.

Senate Bills 149 and 150 (S-1) will have an indeterminate fiscal impact on State and local government. In 2006, 420 offenders were sentenced under the Identity Theft Protection Act. Of these offenders, 118 were sentenced to prison, 246 were sentenced to probation, 38 were sentenced to jail, and 18 received other types of sentences such as delayed and suspended sentences or Holmes Youthful Trainee Act probation. Currently, an offender convicted of the Class E offense will receive a sentencing guidelines minimum sentence range of 0-3 months to 24-38 months. To the extent that the bills result in increased convictions or incarceration time, local governments will incur the costs of incarceration in local facilities, which vary by county. The State will incur the cost of felony probation at an annual average cost of $2,500, as well as the cost of incarceration in a State facility at an average annual cost of $35,000. Additional penal fine revenue will benefit public libraries.

Fiscal Analyst: Joe Carrasco
Matthew Grabowski