

Department of Legislative Services
Maryland General Assembly
2008 Session

FISCAL AND POLICY NOTE

House Bill 564 (Delegate McComas, *et al.*) (Task Force to Study Identity Theft)
Judiciary

Identity Fraud - Prohibition of Unauthorized Skimming and Re-Encoding Devices

This bill prohibits a person from using a “re-encoder” or “skimming device” to access, read, or scan personal identifying information or a payment device number. The bill also prohibits the knowing, willful possession, with fraudulent intent, of such a device for the unauthorized use, sale, or transfer of personal identifying information or a payment device number and establishes penalties.

Fiscal Summary

State Effect: Potential minimal increase in general fund revenues and expenditures due to the bill’s penalty provision.

Local Effect: Potential minimal increase in revenues and expenditures due to the bill’s penalty provision.

Small Business Effect: None.

Analysis

Bill Summary: A re-encoder means an electronic device that places encoded personal identifying information or a payment device number from a credit card onto a different credit card and includes any electronic medium that allows such a transaction to occur.

A skimming device means a scanner, skimmer, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, either temporarily or permanently, personal identifying information or a payment device number that is encoded on a credit card.

Under the bill, a person may not knowingly, willfully, and with fraudulent intent to obtain a benefit, credit, good, service, or other thing of value, use a re-encoder to place encoded information from the magnetic stripe or strip of a credit card onto the magnetic stripe or strip of a different credit card without the consent of the individual authorized to use the credit card from which the personal identifying information or payment device number is being re-encoded. A person may not use a skimming device to access, read, obtain, memorize, or store personal identifying information from a credit card without the consent of the person authorized to use the credit card that is accessed by the device. A violator who obtains a good, service, or other thing of value of at least \$500 is guilty of a felony and is subject to maximum penalties of five years imprisonment and/or a fine of \$25,000. If the value, good, or service obtained has a value of less than \$500, the violator is guilty of a misdemeanor and is subject to maximum penalties of 18 months imprisonment and/or a fine of \$5,000.

A person may not knowingly, willfully, and with fraudulent intent possess, obtain, or help another possess or obtain a re-encoder or skimmer device for the unauthorized use, sale, or transfer of personal identifying information or a payment device number. A violator of this provision is guilty of a misdemeanor and is subject to maximum penalties of 18 months imprisonment and/or a fine of \$5,000.

Current Law: The term “personal identifying information” means: a name, address, telephone number, driver’s license number, Social Security number, place of employment, employee identification number, mother’s maiden name, bank or other financial institution account number, date of birth, personal identification number, credit card number, or other payment device number.

A person may not knowingly, willfully, and with fraudulent intent possess, obtain, or help another to possess or obtain any individual’s personal identifying information without the consent of that individual to use, sell, or transfer the information to get a benefit, credit, good, service, or other thing of value in the name of that individual. A person may not knowingly and willfully assume the identity of another to avoid identification, apprehension, or prosecution for a crime or with fraudulent intent to get a benefit, credit, good, service, or other thing of value or to avoid payment of debts or other legal obligations. A person may not knowingly and willfully claim to represent another person without the knowledge and consent of that person, with the intent to solicit, request, or take any action to otherwise induce another person to provide personal identifying information or a payment device number.

If the benefit, credit, good, service, or other thing that is the subject of the crime is valued at \$500 or more, then a person who violates this identity fraud provision is guilty of a felony and is subject to maximum penalties of imprisonment for five years and/or a fine of \$25,000. If the benefit or other thing has a value of less than \$500, or if a person knowingly and willfully assumes the identity of another to avoid identification,

apprehension, or prosecution for a crime, then the violator is guilty of a misdemeanor and is subject to maximum penalties of imprisonment for 18 months and/or a fine of \$5,000.

If circumstances reasonably indicate that a person's intent was to manufacture, distribute, or dispense another individual's personal identifying information without the individual's consent, the violator is guilty of a felony and is subject to imprisonment for up to five years and/or a fine up to \$25,000. If the violation is committed pursuant to a scheme or continuing course of conduct, the conduct may be considered one offense. The value of goods or services may be combined to determine whether the violation is a felony or misdemeanor.

Notwithstanding any other provision of law, the State may institute a prosecution for the misdemeanor of identity fraud at any time. Under the Maryland Constitution, a person convicted of the misdemeanor offense of identity fraud is deemed to have committed a misdemeanor whose punishment is confinement in the penitentiary and may reserve a point or question for *in banc* review as provided by the Maryland Constitution. A violator of any of these provisions is subject to a court order for restitution and paying costs, including reasonable attorney's fees, related to restoring a victim's identity. A sentence under the identity fraud provisions may be imposed separate from and consecutive to, or concurrent with, a sentence for any crime based on the acts establishing the violation.

Law enforcement officers may operate without regard to jurisdictional boundaries to investigate identity fraud provisions, within specified limitations. The authority may be exercised only if an act related to the crime was committed in the jurisdiction of an investigative agency or a complaining witness resides in an investigating agency's jurisdiction. Notification of an investigation must be made to appropriate law enforcement personnel.

Background: This bill is one of the measures recommended by the Task Force to Study Identity Theft. The task force was created by Chapters 241 and 242 of 2005 and extended by Chapters 9 and 10 of 2007. Among other things, the task force was directed to • study the problems associated with identity theft in Maryland, including the adequacy of current Maryland law in deterring identity theft; • consult with relevant State and federal agencies and other experts on identity theft; and • make recommendations regarding possible remedies to identity theft, including statutory changes.

The task force met six times between November 15, 2006 and December 6, 2007 and heard from law enforcement agencies, bank security officers, citizens, credit card companies, and consumer advocates about the prevalence of identity theft and ways in which the crime could be prevented.

Based on the testimony from bank security organizations, law enforcement organizations, as well as businesses, the task force unanimously recommended that legislation be enacted to make the unauthorized possession and use of re-encoding and skimming devices illegal. The task force heard testimony from victims of identity fraud who suspected that financial account information was obtained without authorization with a skimmer device and was concerned about how the unauthorized use and possession of these devices contributed to the prevalence of identity theft.

According to the National Conference of State Legislatures, 28 states prohibit the unauthorized use or possession of a re-encoder or skimming device to obtain credit card information, as shown in **Exhibit 1**.

Exhibit 1
Credit Card Skimmers/State Legislation

<u>State</u>	<u>Penalty</u>
Arizona	Felony
Arkansas	Felony/Misdemeanor Hybrid
California	Misdemeanor
Connecticut	Misdemeanor
Delaware	Felony
Florida	Felony
Idaho	Felony
Illinois	Felony/Misdemeanor Hybrid
Indiana	Felony
Iowa	Felony
Kansas	Felony
Kentucky	Felony
Louisiana	Imprisonment (<i>similar to felony</i>)
Maine	Class D (<i>similar to misdemeanor</i>)
Michigan	Misdemeanor
Mississippi	Felony
Missouri	Misdemeanor
Nevada	Felony
New Hampshire	Felony/Misdemeanor Hybrid
New Jersey	3 rd or 4 th Degree-(<i>similar to hybrid</i>)
Oregon	Felony
South Dakota	Felony
Texas	Misdemeanor
Utah	Felony
Virginia	Felony/Misdemeanor Hybrid
Washington	Felony
West Virginia	Felony/Misdemeanor Hybrid
Wyoming	Imprisonment and/or fine (<i>similar to hybrid</i>)

Source: National Conference of State Legislatures

The Identity Theft Data Clearinghouse, sponsored by the Federal Trade Commission (FTC) and the Consumer Sentinel, a consortium of national and international law enforcement and private security entities, released *Identity Theft Victim Complaint Data* for calendar 2006 (the latest information available). In calendar 2006, FTC received 246,035 identity theft complaints. In calendar 2005, the number of identity theft complaints was 255,613. In Maryland, residents reported 4,656 instances of identity theft in 2006, or 82.9 complaints per 100,000 population, ranking Maryland eleventh in the nation for identity theft. As has been the case for the last several years, the most common type of identity theft was credit card fraud, which comprised 25% of all complaints. The second most prevalent type of identity fraud involved the opening of new accounts for wireless devices, utilities, and the telephone, at 16% of all complaints.

In November 2007, FTC released a national survey, *The 2006 Identity Theft Survey Report*. FTC reports that the survey suggests that 8.5 million U.S. adults discovered that they were victimized by some form of identity theft in calendar 2005.

State Revenues: General fund revenues could increase minimally as a result of the bill's monetary penalty provision from cases heard in the District Court.

State Expenditures: General fund expenditures could increase minimally as a result of the bill's incarceration penalties due to more people being committed to Division of Correction (DOC) facilities and increased payments to counties for reimbursement of inmate costs. The number of people convicted of these proposed crimes is expected to be minimal.

Persons serving a sentence longer than 18 months are incarcerated in DOC facilities. Currently, the average total cost per inmate, including overhead, is estimated at \$2,600 per month. This bill alone, however, should not create the need for additional beds, personnel, or facilities. Excluding overhead, the average cost of housing a new DOC inmate (including medical care and variable costs) is \$526 per month. Excluding medical care, the average variable costs total \$148 per month.

Persons serving a sentence of one year or less in a jurisdiction other than Baltimore City are sentenced to local detention facilities. For persons sentenced to a term of between 12 and 18 months, the sentencing judge has the discretion to order that the sentence be served at a local facility or DOC. The State reimburses counties for part of their incarceration costs, on a per diem basis, after a person has served 90 days. State per diem reimbursements for fiscal 2009 are estimated to range from \$19 to \$71 per inmate depending upon the jurisdiction. Persons sentenced to such a term in Baltimore City are generally incarcerated in DOC facilities. The Baltimore City Detention Center, a State-operated facility, is used primarily for pretrial detentions.

Local Revenues: Revenues could increase minimally as a result of the bill's monetary penalty provision from cases heard in the circuit courts.

Local Expenditures: Expenditures could increase minimally as a result of the bill's incarceration penalty. Counties pay the full cost of incarceration for people in their facilities for the first 90 days of the sentence, plus part of the per diem cost after 90 days. Per diem operating costs of local detention facilities are expected to range from \$40 to \$129 per inmate in fiscal 2009.

Additional Information

Prior Introductions: None.

Cross File: SB 220 (Senator Kelley, *et al.*) (Task Force to Study Identity Theft) – Judicial Proceedings.

Information Source(s): Judiciary (Administrative Office of the Courts), Department of Public Safety and Correctional Services, Federal Trade Commission, National Conference of State Legislatures, Department of Legislative Services

Fiscal Note History: First Reader - February 11, 2008
mll/jr

Analysis by: Karen D. Morgan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510