Department of Legislative Services

Maryland General Assembly
2008 Session

FISCAL AND POLICY NOTE
Revised

Senate Bill 60 (Senator Kelley, *et al.*)
(Task Force to Study Identity Theft)

Judicial Proceedings Judiciary

Identity Fraud - Prohibitions, Evidence, and Penalties

This bill increases the maximum incarceration penalty for felony identity fraud, establishes two identity fraud offenses, and expands the evidence that may be considered in identity fraud criminal proceedings.

Fiscal Summary

State Effect: Potential minimal increase in general fund revenues and expenditures due to the bill's penalty provisions. Potential operational efficiencies for the District Court due to decreased court time needed to admit the evidence affected by the bill and fewer contested hearings.

Local Effect: Potential minimal increase in revenues and expenditures due to the bill's penalty provisions. Potential operational efficiencies for circuit courts due to decreased court time needed to admit the evidence affected by the bill and fewer contested hearings.

Small Business Effect: None.

Analysis

Bill Summary: This bill increases the maximum imprisonment penalty for felony identity fraud from 5 to 15 years.

In addition, the bill establishes that it is a crime for a person to intentionally, willfully, and without authorization copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database that was unlawfully accessed. A violator is

guilty of a misdemeanor and is subject to maximum penalties of imprisonment for three years and/or a fine of $1,000.

The bill authorizes, in a criminal case or juvenile proceeding involving identity fraud, the introduction of the affidavit of a lawful credit cardholder as substantive evidence that the credit card or credit card number of the credit cardholder was taken, used, or possessed without the authorization of the credit cardholder.

The bill also 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 applies the penalties for identity fraud violations to these offenses.

Current Law:

Unauthorized Database Access: A person may not intentionally, willfully, and without authorization access or attempt to access, cause to be accessed, or exceed authorized access to all or part of a computer network, language, software, system, services, or database. A violation of this provision is a misdemeanor and the violator is subject to maximum penalties of imprisonment for three years and/or a fine of $1,000.

A person may not commit unlawful access with the intent to cause the malfunction or interruption of any or all parts of a computer, network, language, software, services, or data. A person may not commit authorized access with the intent to alter, damage, or destroy all or any part of data or program stored, maintained, or produced by a computer, network, software, system, services, or database. A person may not intentionally, willfully, and without authorization possess, identify, or attempt to identify a valid access code, or publicize or distribute a valid access code to an unauthorized person. If the aggregate amount of loss is $10,000 or more, the violator is guilty of a felony and is subject to maximum penalties of imprisonment for 10 years and/or a fine of $10,000. If the aggregate loss is less than $10,000, the violator is guilty of a misdemeanor and is subject to maximum penalties of imprisonment for five years and/or a fine of $5,000.

Access achieved in a prohibited manner under a single scheme or a continuing course of conduct may be considered one violation. A defendant may be tried in any county in Maryland where the act was performed or the accessed computer was located.

Credit Card Evidence: An affidavit sworn to by a lawful credit cardholder may be introduced as substantive evidence that the credit card or credit card number was taken, used, or possessed without the credit cardholder's authorization. This provision applies

to a criminal case or juvenile proceeding for the following offenses: (1) credit card theft; (2) credit card counterfeiting; (3) obtaining property by counterfeiting, theft, or misrepresentation; (4) honoring a stolen or counterfeit credit card with the intent to defraud the issuer or the cardholder; (5) completing a credit card or possessing a device to reproduce credit cards without consent; (6) receiving property by stolen counterfeit or misrepresented credit card; (7) publishing the number or code of a telephone credit card; or (8) unauthorized use and disclosure of a credit card or payment device number.

The State must provide at least 10 days notice to the defendant before a proceeding in which the State intends to introduce into evidence an affidavit of a credit card holder under the bill. On written demand of the defendant filed at least five days before the proceeding, the State must require the presence of the affiant as a prosecution witness.

Skimming Devices: State law does not prohibit the possession or use of a re-encoder or skimming device that is used to access, read, scan, memorize, or store personal identifying information or payment device numbers.

Identity Fraud Generally: 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 contains 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 numerous law enforcement agencies including the U.S. Secret Service; the U.S. Postal Inspection Service; the Federal Bureau of Investigation; the State's Attorney's offices from Baltimore City and Baltimore, Montgomery, and Prince George's counties; and the police departments of Baltimore and Prince George's counties.

Based on the recommendations from law enforcement organizations, as well as businesses and other witnesses, the task force unanimously recommended that the penalties for identity fraud be increased and expanded. The task force specifically recommended that the felony penalties for identity fraud be commensurate with the existing felony penalties for credit card fraud. The task force heard testimony that a barrier to apprehending more identity fraud criminals is that these cases require more extensive investigation than traditional fraud cases. Financial records must be secured from banks, credit card companies, Internet providers, and others. Eyewitnesses and perpetrators are often scattered across states or may be overseas. Task force witnesses testified that it was difficult to justify the greater effort for apprehension and prosecution of identity thieves when a typical credit card fraud case could require less effort and result in a greater penalty for the offender.

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.

The task force received several recommendations, particularly from State's Attorneys, for reform of the rules of evidence to improve prosecution of identity fraud cases. Testimony provided to the task force indicated that State's Attorneys had a difficult time getting identity fraud victims to come to Maryland to appear as witnesses especially if the credit card company had provided financial reimbursement. Some cases are relatively low level, in terms of the amount stolen or the possible penalties, making it difficult to justify the effort of guaranteeing the personal appearance of accountholders, who are able to only testify that he or she held the account that was compromised. Because of these difficulties, the State is unable to proceed, but is also unable to get the court to grant a continuance so that evidence can be obtained. As a result, charges are often dropped in identity fraud cases. The task force believes that the use of a witness affidavit will assist with the prosecution of identity theft cases and will create parity with the credit card crimes for which affidavits are already authorized. Even if the defense objects to the affidavit and demands presentation of the witness, a court may be more willing to grant a continuance so that the witness may be produced at a later time.

In written testimony presented to the Task Force to Study Identity Theft, the Baltimore City State's Attorney informed the task force that identity thieves often hack into computer databases that store vast amounts of identity-related data. Under current law, the altering, damaging, and unauthorized access to a computer database is prohibited, but copying or possessing the data is not prohibited. Expanding the law to criminalize copying or possessing the contents of a database that was compromised by unauthorized access could aid law enforcement efforts to apprehend identity thieves.

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: The Administrative Office of the Courts advises that the expenditure savings that could result from admitting a credit cardholder's affidavit as evidence in criminal or juvenile proceedings depends on the vigilance of the State's Attorney in making sure that the affidavit is a true attestation of the credit cardholder. To the extent that identity fraud cases result in restitution hearings, the use of affidavits would also substantively establish the crime and decrease the number of contested hearings.

The Office of State's Attorneys advises that the use of credit card affidavits as provided in the bill could result in savings as a State's Attorney would be able to submit the affidavit as evidence, rather than reimbursing the alleged victim (especially if the victim does not live in Maryland) for travel, lodging, and other expenses to make a personal appearance to testify at trial.

General fund expenditures could increase minimally as a result of the bill's incarceration penalty due to more people being committed to Division of Correction (DOC) facilities for longer periods of time and increased payments to counties for reimbursement of inmate costs. The number of people convicted of this proposed crime is expected to be minimal.

The Maryland State Commission on Criminal Sentencing Policy provided information on the disposition of identity fraud perpetrators, as shown in **Exhibit 1**. Cases with both single and multiple counts were included. Cases with multiple offenses were included only if the identified offense was the most serious offense.

Exhibit 1
Identity Theft Offenses/Disposition
January 1, 2002 through December 31, 2006

Offense	Convictions	Number Incarcerated	Average Total Sentence Imposed	Average Total Sentence Less Suspended Sentence
Possess, Obtain Personal Identifying Information, or Assume Another's Identity (Benefit Less than $500)	20	6	11.1 months	6.1 months
Possess, Obtain Personal Identifying Information, or Assume Another's Identity (Benefit $500 or Greater)	22	10	39.7 months	11.4 months
Intent to Manufacture, Distribute, or Dispense Personal Identifying Information	7	4	49.5 months	22.8 months

Source: Maryland State Commission on Criminal Sentencing Policy

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. The Division of Parole and Probation advises that this bill could potentially impact the length of an offender's supervision. The fiscal 2008 cost to supervise an offender for one year is about $1,555.

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: A similar bill, HB 1044 of 2007, was heard in the House Judiciary Committee and then withdrawn.

Cross File: HB 1113 (Delegate Lee, *et al.*) (Task Force to Study Identity Theft) – Judiciary.

Information Source(s): Judiciary (Administrative Office of the Courts), Commission on Criminal Sentencing Policy, Department of Public Safety and Correctional Services, Federal Trade Commission, Department of Legislative Services

Fiscal Note History: First Reader - February 8, 2008
ncs/jr Revised - Enrolled Bill - April 22, 2008

Analysis by: Karen D. Morgan

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