# Department of Legislative Services

Maryland General Assembly
2004 Session

## FISCAL AND POLICY NOTE
**Revised**

House Bill 191 (Delegate Lee, *et al.*)
Judiciary Judicial Proceedings

---

**Task Force to Study Identity Theft**

---

This bill establishes a Task Force to Study Identity Theft. The task force is charged with studying problems associated with identity theft in Maryland and privacy laws in other states. The task force must also consult with relevant federal agencies, agencies in other states, and identity theft experts. The task force is required to submit an interim report to the General Assembly by December 31, 2004 and make findings and recommendations for possible remedies to identity theft to the General Assembly by December 31, 2005. The Department of Labor, Licensing, and Regulation (DLLR) is required to provide staff to the task force.

The bill is effective July 1, 2004 and terminates on January 31, 2006.

## Fiscal Summary

**State Effect:** Any expense reimbursements for task force members are assumed to be minimal and absorbable with existing resources. Staffing can also be provided within existing resources.

**Local Effect:** Minimal. The bill calls for two local representatives to serve on the task force.

**Small Business Effect:** Minimal.

## Analysis

**Current Law:** 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, in order 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 the payment of debts or other legal obligations.

A person who violates this identity fraud prohibition is guilty of a felony and is subject to imprisonment not exceeding five years, a fine not exceeding $25,000, or both, if the benefit, credit, goods, services, or other thing that is the subject of the crime is valued at $500 or more. If the benefit or other thing has a value of less than $500, then the violator is guilty of a misdemeanor and is subject to imprisonment for up to 18 months, a maximum fine of $5,000, or both.

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, a maximum fine of $25,000, or both.

A person who knowingly and willfully assumes the identity of another to avoid identification, apprehension, or prosecution for a crime is guilty of a misdemeanor and subject to imprisonment for up to 18 months, a maximum fine of $5,000, or both.

If a violation is committed pursuant to a scheme or continuing course of conduct, whether from the same or several sources, the conduct may be considered one offense. The value of goods or services may be aggregated to determine whether the violation is a felony or misdemeanor.

A violator of any of these prohibitions is also subject to a court order for restitution and paying costs related to restoring a victim's identity.

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.

A person generally commits the crime of theft when the person willfully or knowingly: (1) obtains unauthorized control over property with the intent to deprive the owner of the property; or (2) uses, conceals, or abandons property in a manner that deprives or probably will deprive the owner of the property. If the value of the property is $500 or more, a violator is guilty of a felony and is subject to a maximum fine of $25,000, imprisonment for up to 15 years, or both. If the property's value is less than $500, a violator is guilty of a misdemeanor and is subject to a maximum fine of $500, imprisonment for up to 18 months, or both. The violator must also return the stolen property or make appropriate restitution.

**Background:** Identity theft is commonly regarded as one of the fastest growing crimes in the United States. As soon as the general public adopts some safeguards to prevent identity theft, it seems the thieves are hard at work thinking up new scams to subvert the protections employed. For example, on January 20, 2004, *The Washington Post* contained an article about a relatively new credit card scam called "phishing." Most people are aware that credit card numbers, home addresses, and other identifying information should not be given to an unsolicited caller or through unsolicited e-mail. With phishing, the thief impersonates a credit card fraud investigator, but does not ask the person to provide a credit card number, home address, or Social Security number. Instead, the thief merely asks the person to confirm identifying information the thief has already obtained, with the goal of getting the person to divulge the three digit security code number that is on the back of most credit cards. Increasingly, merchants won't accept charges that are not made in person without this code. Because the security code is not the actual card number, people have divulged this information, believing that they were conferring with a genuine fraud investigator. The National Consumer League's Fraud Information Center began tracking the phishing scam in late 2003.

In September 2003, the Federal Trade Commission (FTC) released an *Identity Theft Survey Report*. From March through April of 2003, 4,057 adults were surveyed nationwide to determine the magnitude and impact of identity theft. A total of 4.6% of survey respondents indicated they discovered they were the victims of identity theft in the past year. Extrapolation of this survey result suggests that 9.9 million Americans may have been victimized by some form of identity theft in the past year. When asked about the last five years, 12.7% of the survey respondents indicated that they discovered they were the victims of some form of identity theft involving setting up new accounts, misuse of existing credit cards, or misuse of savings or checking accounts. Extrapolation of these survey results suggests that as many as 27 million Americans may have been victims of some form of identity theft over the last five years.

The Identity Theft Data Clearinghouse, sponsored by FTC and Consumer Sentinel, a consortium of national and international law enforcement and private security entities, released *National and State Trends in Fraud and Identity Theft* for calendar 2003. In 2003, FTC received 516,740 fraud and identity theft consumer complaints. In 2002, the number of complaints received was 404,000. In 2003, there were 214,905 identity theft reports and 301,835 fraud complaints.

Of the 214,905 complaints in 2003, the most common type of identity theft reported was credit card fraud, with a prevalence of 33%. Identity theft relating to phone or utilities fraud occurred in 21% of reported cases, bank fraud occurred in 17%, and employment-related fraud occurred in 11% of reported cases. Other types of identity theft included government documents or benefits, in 8% of reported cases and loan fraud, in 6% of reported cases. FTC reports that identity theft victims are not likely to notify law enforcement. Only 40% of reported victims notified a police department. Eight percent of those victims stated that a police report was not taken after notifying law enforcement. Sixty percent of reported identity theft victims did not notify any police department.

In calendar 2003, the metropolitan area with the highest number of identity theft complaints per 100,000 population was Phoenix-Mesa Arizona, with 5,041 victims and 155 victims per 100,000 population. The Washington, DC metropolitan area ranked twelfth, with 4,936 reported victims and 100.3 victims per 100,000 population. The Baltimore metropolitan area ranked twenty-second, with 1,816 reported victims and 71.1 victims per 100,000 population. The five states with the highest reported incidents of identity theft in calendar 2003 were Arizona, Nevada, California, Texas, and Florida. The five states with the lowest incidences of identity theft were West Virginia, Maine, Vermont, North Dakota, and South Dakota.

Maryland was ranked eleventh out of 50 states for identity theft, with 74.9 victims per 100,000 population and 4,124 reported identity theft victims. The most common type of identity theft in Maryland was credit card fraud, occurring to 1,533 victims. About 37% of identity theft victims reported this form of identity theft. Phone or utilities fraud occurred in 22% of reported cases, and bank fraud occurred in 18% of reported cases. The areas of Maryland that contained the highest reports of identity theft were Baltimore, Silver Spring, Rockville, Gaithersburg, and Bethesda.

All 50 states and the District of Columbia have provisions relating to identity theft. In 1998, the federal government enacted the Identity Theft and Assumption Deterrence Act, which makes it a federal crime to knowingly transfer or use the means of identification of another person with the intent to commit a violation of federal law or a felony under any state or local law. In 2003, the federal government enacted amendments to the Fair Credit Reporting Act called the Fair and Accurate Credit Transactions Act of 2003. The federal law is intended to provide additional deterrence to identity theft, but also contains preemptions of state authority relating to enforcement of identity theft provisions enacted after 2003.

**State Expenditures:** DLLR advises that $44,000 in general fund expenditures for two half-time positions would be needed to staff the task force. The Department of Legislative Services disagrees with this assessment and advises that the task force can be staffed within the existing resources of DLLR. Although the Commissioner of Financial

Regulation is experiencing a staff shortage at this time, there are 66.6 funded but unused positions within all of DLLR.

---

## Additional Information

**Prior Introductions:** None.

**Cross File:** None.

**Information Source(s):** Federal Trade Commission, National Consumer Law Center, National Conference of State Legislatures, Identity Theft Resource Center, National Consumers League, *The Washington Post*, Department of Legislative Services

**Fiscal Note History:** First Reader - January 26, 2004
mh/jr Revised - House Third Reader - March 24, 2004

---

Analysis by: Karen D. Morgan

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