Department of Legislative Services

Maryland General Assembly
2008 Session

FISCAL AND POLICY NOTE

House Bill 129 (Delegate Ali, *et al.*)
Economic Matters

Plastic Card Security Act

This bill prohibits a person that accepts an access device in connection with a transaction from retaining specified data after authorization of the transaction. However, data associated with personal identification debit transactions can be retained for up to 48 hours after authorization. Violation of the bill is an unfair or deceptive trade practice under the Maryland Consumer Protection Act, subject to MCPA's civil and criminal penalty provisions.

Fiscal Summary

State Effect: Potential increase in general fund revenues and expenditures due to the bill's imposition of existing penalty provisions. If the Attorney General's Office receives fewer than 50 complaints per year stemming from the bill, the additional workload could be handled with existing resources.

Local Effect: Potential increase in revenues and expenditures due to the bill's imposition of existing penalty provisions.

Small Business Effect: Potential minimal.

Analysis

Bill Summary: The bill amends several provisions of the Maryland Personal Information Protection Act in order to prohibit the storage of personal information following transactions involving electronic access devices such as credit and debit cards. The bill defines an "access device" as a card that is issued by a financial institution and

contains a magnetic stripe, microprocessor chip, or other means for storage of information, including credit cards, debit cards, and stored value cards. The bill defines an "access device security code" as the numerical value that is printed on or contained in an access device and is used to validate the device's information during the device authorization process. "Service provider" is defined as a person that stores, processes, or transmits access device data on behalf of another. The bill also adds definitions of "magnetic stripe data," "microprocessor chip data," "personal identification numbers," and creates a widely inclusive definition of "financial institutions."

If a violation of the bill occurs and there is a security breach of the system of either the violator or the violator's service provider, the violator must reimburse any financial institution that issued an access device affected by the breach. The violator must reimburse an affected financial institution for the costs of reasonable loss mitigation actions, including • cancellation or reissue of an access device; • closure of a deposit, transaction, share draft, or other account and any action to stop payment or block transactions with respect to the account; • opening or reopening of a deposit, transaction, share draft, or other account; • refund or credit made to an access device holder to cover the cost of an unauthorized transaction; and • notification to access device holders. The bill also allows financial institutions to recover from violators the costs for damages paid to access device holders injured by a breach. The costs do not include amounts recovered from a credit card company by a financial institution.

Current Law: Under MPIPA, businesses that own or maintain computerized personal information regarding individuals residing in the State must take reasonable steps to protect against unauthorized access to or use of the personal information. If such a business learns of a security breach of a system containing such data, the business must conduct a good faith, reasonable, and prompt investigation to determine the likelihood personal information has been or will be misused as a result. After the investigation is concluded, if the business determines that misuse of personal information has occurred or is reasonably likely to occur, the business must notify the affected individuals of the breach. Notification may be delayed in order to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system, or if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize national security. Violation of the provisions of MPIPA is an unfair or deceptive trade practice under the Maryland Consumer Protection Act.

The Consumer Protection Division within the Office of the Attorney General is responsible for pursuing unfair and deceptive trade practice claims under the Maryland Consumer Protection Act. Upon receiving a complaint, the division must determine whether there are "reasonable grounds" to believe that a violation of MCPA has occurred. Generally, if the division does find reasonable grounds that a violation has occurred, the

division must seek to conciliate the complaint. The division may also issue cease and desist orders, or seek action in court, including an injunction or civil damages, to enforce MCPA. Violators of MCPA are subject to • civil penalties of $1,000 for the first violation and $5,000 for subsequent violations; and • criminal sanction as a misdemeanor, with a fine of up to $1,000 and/or up to one year's imprisonment.

Background: A number of high-profile security breaches in recent years have highlighted the vulnerability of the vast computer databases that store personal information relating to every aspect of individuals' lives. For example, the TJX Companies, Inc., parent company of TJ Maxx and Marshalls, revealed in 2006 that a security breach had exposed tens of millions of customer credit card numbers to potential fraud. That same year, the Federal Trade Commission announced that ChoicePoint, Inc., a data collection company, would pay a $10 million civil penalty and $5 million in consumer redress for violation of the federal Fair Credit Reporting Act. FTC ruled that the company had failed to implement adequate safeguards against the wrongful release of consumer information and that this failure contributed to a 2005 data breach of thousands of personal records. The settlement requires ChoicePoint to implement new procedures • to ensure that it provides consumer reports only to legitimate businesses for lawful purposes; • to establish and maintain a comprehensive information security program; and • to obtain audits by an independent third-party security professional every other year until 2026.

Under the guidelines adopted jointly by federal banking regulators "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that the misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible."

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Labor, Licensing, and Regulation; Office of the Attorney General (Consumer Protection Division); Department of Legislative Services

Fiscal Note History: First Reader - February 6, 2008
mll/ljm

Analysis by: Alexander M. Rzasa

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