Department of Legislative Services

Maryland General Assembly
2008 Session

FISCAL AND POLICY NOTE

House Bill 284 (Delegates Ali and Feldman)
Economic Matters

Consumer Loyalty Card Privacy Act

This bill prohibits a merchant from sharing or selling personal information or marketing information about a consumer in the State. Violation of the bill is an unfair or deceptive trade practice under the Maryland Consumer Protection Act and subject to its civil and criminal penalties.

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: None.

Analysis

Bill Summary: The bill allows a merchant that offers a consumer loyalty card to consumers to share the name and address of a consumer with a third party for the sole purpose of mailing information about the card to the consumer. The third party may not use a consumer's name and address for any other purpose. The bill defines a "consumer loyalty card" as any card, plate, coupon book, or other device issued by a merchant to a consumer that may be used to track a consumer's purchases. "Marketing information" is

defined as the detailed purchasing history of a consumer loyalty cardholder compiled by a merchant. Under the bill, "personal information" is defined as the following unencrypted information capable of being associated with a consumer: • a name; • an address; • a telephone number; • a driver's license number; • a financial account number, including a credit or debit card number; • a required security code or password that would permit access to a consumer's financial account; or • an electronic mail address. "Personal information" does not include information that a consumer has consented to have publicly disseminated or listed. The provisions of the bill do not apply to merchants with less than 50 employees.

Current Law: Chapter 523 of 2007, the Personal Information Protection Act, requires businesses to implement and maintain reasonable and appropriate security procedures and practices to protect personal information from unauthorized access, use, modification, or disclosure. A business that owns or licenses computerized data that includes personal information of a Maryland resident must take specific steps when it discovers or is notified of a breach of the security of a system. Specifically, the business must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information has or will be misused as a result of the breach. If, after the investigation, the business reasonably believes that the breach has resulted or will result in the misuse of personal information of a Maryland resident, the business must notify the individual of the breach. Generally, the notice must be given as soon as reasonably practicable after the business conducts the required investigation. The notification may be delayed • if a law enforcement agency determines that it will impede a criminal investigation or jeopardize national security; or • to determine the scope of the breach, identify the individuals affected, or restore the system's integrity.

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 the Act. 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: The prospect of being victimized through the loss or theft of personal information held by merchants or private data collection companies has captured national attention. A 2005 security breach the ChoicePoint Corporation highlighted this issue, after the breach led to the release of personal information relating to over 160,000

individuals. Since the ChoicePoint breach, the Privacy Rights Clearinghouse has documented over 450 instances of security breaches involving the unauthorized exposure of at least 97 million records containing personal information, including data obtained from merchants.

Additional Information

Prior Introductions: Similar bills were introduced in 2007. HB 739 received a hearing in the House Economic Matters Committee but was later withdrawn. SB 467 received an unfavorable report from the Senate Finance Committee.

Cross File: None.

Information Source(s): Office of the Attorney General (Consumer Protection); Department of Legislative Services

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

Analysis by: Alexander M. Rzasa

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