Department of Legislative Services

Maryland General Assembly
2013 Session

FISCAL AND POLICY NOTE

House Bill 1219 (Delegate Cullison, *et al.*)
Economic Matters

Consumer Protection - Required Notice by Financial Institutions - Nonpublic Personal Information

This bill requires a financial institution that discloses to an affiliate or a nonaffiliated third party the nonpublic personal information of a consumer to also include a specified notice in each billing statement or statement of account activity that is sent to the consumer.

The bill's stated intent is to further the purposes of protecting nonpublic personal information as provided for in the federal Gramm-Leach-Bliley (GLB) Act.

Fiscal Summary

State Effect: Any enforcement of the bill's changes can be handled with existing budgeted resources.

Local Effect: None.

Small Business Effect: Minimal.

Analysis

Bill Summary: The aforementioned notice must state (1) that nonpublic personal information may be disclosed to an affiliate or a nonaffiliated third party; (2) that the consumer may direct the financial institution not to disclose the nonpublic personal information to an affiliate or a nonaffiliated third party; and (3) how the consumer can find the financial institution's privacy policy for nonpublic personal information. The bill requires that the notice be clear and conspicuously placed near the top of each billing statement or statement of account activity and be in at least 12-point font.

The bill specifies that the terms "affiliate," "consumer," "financial institution," "nonaffiliated third party," and "nonpublic personal information" have the identical meaning stated within the GLB Act.

Current Law/Background: Under the GLB Act and the subsequent Safeguards Rule issued by the Federal Trade Commission, financial institutions must take measures to ensure the security and confidentiality of nonpublic customer information. The Safeguards Rule requires a company to develop a written information security plan that:

- designates one or more employees to coordinate its information security program;
- identifies and assesses the risks to customer information in each relevant area of the company's operation;
- evaluates the effectiveness of the current safeguards for controlling the risks to customer information;
- designs and implements a safeguards program and regularly monitors and tests it;
- selects service providers that can maintain appropriate safeguards and oversees their handling of customer information; and
- evaluates and adjusts the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The GLB Act grants states the ability to afford any person greater protection of nonpublic information.

Under the Maryland Personal Information Protection Act, to protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of a Maryland resident is required to implement and maintain reasonable and appropriate security procedures and practices. A business that uses a nonaffiliated third party as a service provider and discloses personal information about a Maryland resident under a written contract with the third party must require, by contract, that the third party implement and maintain reasonable security procedures and practices that are (1) appropriate to the nature of the disclosed information and (2) reasonably designed to help protect the information from unauthorized access, use, modification, disclosure, or destruction.

A business that owns or licenses computerized data that includes personal information of a Maryland resident, upon the discovery or notification of a breach of the security of a system, must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information has been 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. If the business determines that notification is not required, the business must maintain the records related to the determination for three years.

A business that maintains computerized data that includes personal information that it does not own or license must notify the owner or licensee of the personal information of a breach and share information relevant to the breach if it is likely that it has resulted or will result in the misuse of personal information of a Maryland resident. Generally, the notice must be given as soon as reasonably practicable after the business discovers or is notified of the breach.

Additional Information

Prior Introductions: None.

Cross File: None.

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

Fiscal Note History: First Reader - March 11, 2013
mc/kdm

Analysis by: Michael F. Bender

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