

Department of Legislative Services
Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 443
Finance

(Senator Lee, *et al.*)

Consumer Protection - Security Features for Connected Devices

This bill requires a manufacturer of a “connected device” to equip the device with a reasonable “security feature” that is (1) appropriate to the nature and function of the connected device; (2) appropriate to the information the connected device collects, contains, or transmits; and (3) designed to protect the connected device from unauthorized access, destruction, or modification. A connected device is considered to have a reasonable security feature if it meets these requirements and is equipped with a means for authentication outside of a local area network that includes either (1) a preprogrammed password that is unique to each connected device or (2) a process that requires the user to generate a new means of authentication before the user is granted access for the first time. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA’s civil and criminal penalty provisions. **The bill takes effect January 1, 2021.**

Fiscal Summary

State Effect: The bill’s imposition of existing penalty provisions does not have a material impact on State finances or operations. The Office of the Attorney General, Consumer Protection Division, can handle the bill’s requirements with existing resources.

Local Effect: The bill’s imposition of existing penalty provisions does not have a material impact on local government finances or operations.

Small Business Effect: Potential meaningful.

Analysis

Bill Summary:

Definitions

“Connected device” means a physical object that is capable of connecting to the Internet, directly or indirectly, and assigned an Internet Protocol address or Bluetooth address. “Security feature” means an attribute of hardware, firmware, software, process, procedure, or a combination of those factors that could prevent or lessen the likelihood of failure or compromise of the confidentiality, integrity, or accessibility of a connected device or its stored information.

“Manufacturer” means a person who manufactures or assembles a new connected device for sale or distribution or contracts with another person to do so on that person’s behalf. “Authentication” means a method of verifying the authority of a user, process, or connected device to access resources through an information system. “Unauthorized access” means any use, modification, disclosure, or destruction of any information stored within a connected device that is not authorized by the device’s owner.

Limitations

The bill may not be construed to impose any duty on (1) a manufacturer of a connected device for an unauthorized access that arises from an unaffiliated third-party software or application that a user adds to a connected device; (2) a manufacturer to prevent a user from having full control over a connected device, including by allowing a user to modify the software or firmware running on the connected device; or (3) the operator of an electronic store, an electronic marketplace, or any other means of purchasing or downloading software or applications to enforce compliance with the bill.

Current Law: An unfair, abusive, or deceptive trade practice under MCPA includes, among other acts, any false, falsely disparaging, or misleading oral or written statement, visual description, or other representation of any kind that has the capacity, tendency, or effect of deceiving or misleading consumers. The prohibition against engaging in any unfair, abusive, or deceptive trade practice encompasses the offer for or actual sale, lease, rental, loan, or bailment of any consumer goods, consumer realty, or consumer services; the extension of consumer credit; the collection of consumer debt; or the offer for or actual purchase of consumer goods or consumer realty from a consumer by a merchant whose business includes paying off consumer debt in connection with the purchase of any consumer goods or consumer realty from a consumer.

The Consumer Protection Division is responsible for enforcing MCPA and investigating the complaints of aggrieved consumers. The division may attempt to conciliate the matter, issue a cease and desist order, or file a civil action in court. A merchant who violates MCPA is subject to a fine of up to \$10,000 for each violation and up to \$25,000 for each repetition of the same violation. In addition to any civil penalties that may be imposed, any person who violates MCPA is guilty of a misdemeanor and, on conviction, is subject to a fine of up to \$1,000 and/or imprisonment for up to one year.

Small Business Effect: Any small businesses that manufacture connected devices are subject to the bill's security requirements and, as a result, may incur additional costs in order to comply.

Additional Information

Prior Introductions: None.

Designated Cross File: HB 888 (Delegates Carey and C. Watson) - Economic Matters.

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

Fiscal Note History: First Reader - February 18, 2020
af/ljm

Analysis by: Eric F. Pierce

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