Department of Legislative Services

Maryland General Assembly
2016 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 658 (Senator Benson)
Finance Rules and Executive Nominations

Retail Business Owners - Automated Teller Machines - Notice of Skimming Device

This bill requires the owner of a retail business who has knowledge that an automated teller machine (ATM) located on the premises of the business has an illegal skimming device installed on or near it to immediately notify the operator of the ATM about (1) the existence of the skimming device and (2) the location and other identifying information about the ATM to assist the operator in identifying the affected ATM. The bill does not apply to the owner of a retail business that is a bank or a credit union.

Fiscal Summary

State Effect: The bill does not materially affect State finances or operations.

Local Effect: The bill does not materially affect local government finances or operations.

Small Business Effect: Minimal.

Analysis

Current Law: An operator of an ATM must adopt procedures for evaluating the safety of the location of the ATM before it is installed. Generally, an operator of an ATM that is not located inside of a building must install and maintain a video camera that views and records an image of a user as the user performs a transaction. There are limited specified exceptions.

The Criminal Law Article defines a "skimming device" as a scanner, skimmer, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store,

temporarily or permanently, personal identifying information or a payment device number encoded on the magnetic strip or stripe of a credit card.

A person may not knowingly, willfully, and with fraudulent intent to obtain a benefit, credit, good, service, or other thing of value or to access health information or health care, use a skimming device to access, read, scan, obtain, memorize, or store personal identifying information or a payment device number on the magnetic strip or stripe of a credit card without the consent of the individual authorized to use the credit card.

A person may not knowingly, willfully, and with fraudulent intent possess, obtain, or help another possess or obtain a re-encoder device or a skimming device for the unauthorized use, sale, or transfer of personal identifying information or a payment device number. A person who violates either provision is subject to specified fines and lengths of imprisonment.

Background: According to the Consumer Sentinel Network (a consortium of national and international law enforcement and private security entities), the Federal Trade Commission received 332,646 identity theft complaints in calendar 2014, compared to 290,099 in calendar 2013. In Maryland, residents reported 5,734 instances of identity theft in 2014, or 95.9 complaints per 100,000 population, ranking Maryland tenth in the nation for identity theft. The most common type of identity theft in Maryland was government documents or benefits fraud, which comprised 35% of all complaints. The second most prevalent type of identity fraud involved credit card fraud, representing 18% of all complaints.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Labor, Licensing, and Regulation; Department of State Police; Federal Trade Commission (Consumer Sentinel Network); Department of Legislative Services

Fiscal Note History: First Reader - March 8, 2016
min/mcr Revised - Senate Third Reader - April 12, 2016

Analysis by: Stephen M. Ross

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