Department of Legislative Services

Maryland General Assembly
2017 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 647 (Senator Kagan)
Finance

Consumer Protection - Disclosure of Social Security Number - Prohibition

This bill prohibits a person from (1) requiring a consumer to disclose the consumer's Social Security number (SSN) to the person as a condition for the purchase or lease of consumer goods or the purchase of consumer services or (2) including a blank field or text box for a SSN on a contract for (or a form associated with) the purchase or lease of consumer goods or the purchase of consumer services.

The bill's prohibition of SSN disclosure does not apply to a person requesting or requiring a consumer to disclose the consumer's SSN to apply for (or obtain) an extension of consumer credit.

Violation of the bill is an unfair or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions.

Fiscal Summary

State Effect: The bill's imposition of existing penalty provisions does not have a material impact on State finances or operations. If the Consumer Protection Division of the Office of the Attorney General (OAG) receives fewer than 50 complaints per year stemming from the bill, the additional workload can be handled 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: Minimal.

Analysis

Bill Summary: The bill defines a "consumer" as an actual or prospective purchaser, lessee, or recipient of consumer goods, consumer services, or consumer credit. "Consumer credit," "consumer goods," and "consumer services" mean, respectively, credit, good, and services that are primarily for personal, household, family, or agricultural purposes.

Current Law/Background: State law does not impose restrictions on businesses that request or require the disclosure of an SSN. However, businesses are required under the Maryland Personal Information Act (MPIPA) to take precautions related to personal information of customers, and to provide notice of information breaches. Similarly, Chapter 304 of 2013 requires units of State and local government to protect personal information and to provide notice of breaches. Both laws define "personal information" as an individual's first name (or first initial) and last name in combination with specified data elements – including a person's SSN. In addition, OAG must be notified of a security breach under both laws.

Maryland Personal Information Protection Act

Chapters 531 and 532 of 2007 (MPIPA) require businesses to protect an individual's personal information and to provide notice of a security breach relating to an individual's personal information. When a business is destroying a customer's records containing the customer's personal information, the business must take reasonable steps to protect against unauthorized access to or use of the personal information, taking specified considerations into account.

To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of a Maryland resident must 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. This provision applies to a written contract that is entered into, on, or after January 1, 2009.

Private-sector Use of Social Security Numbers

According to the Social Security Administration (SSA), the original purpose of the SSN was to enable SSA to maintain accurate records of the earnings of individuals who worked in jobs covered under the Social Security program. The card was never intended to serve

as a personal identification document – that is, it does not establish that the person presenting the card is actually the person whose name and SSN appear on the card.

However, the simplicity and efficiency of using a unique number that most people already possess has encouraged widespread use of the SSN by both government agencies and private enterprises, especially as they have adapted their recordkeeping and business systems to automated data processing. Use of the SSN as a convenient means of identifying people in large systems of records has increased over the years, and its expanded use appears to be an enduring trend. Generally, there are no restrictions in federal law precluding the use of the SSN by the private sector, so businesses may ask individuals for an SSN whenever they wish.

With the existence of many purposes for legally requiring an SSN, the need for a U.S. resident to possess one has become nearly universal. The universality of SSN ownership has, in turn, led to adoption of the SSN by private industry as a unique identifier. Unfortunately, this universality has led to abuse of the SSN. Most notoriously, the SSN is a key piece of information used to commit identity theft.

Identity Theft in Maryland

An individual's SSN is a highly sensitive identifier which, if obtained by a third party, can be used for identity theft. According to the Federal Trade Commission (FTC), identity theft occurs when someone uses an individual's personally identifying information (*e.g.*, the person's name, SSN, or credit card number) without the person's permission in order to commit fraud or other crimes.

In March 2017, the Consumer Sentinel Network, a consortium of national and international law enforcement and private security entities, released the *Consumer Sentinel Network Data Book* for calendar 2016. In calendar 2016, FTC received 399,225 identity theft complaints nationwide compared to 490,226 in calendar 2015 and 332,647 in calendar 2014.

In Maryland, residents reported 8,251 instances of identity theft in 2016, or 137.1 complaints per 100,000 population, ranking Maryland seventh in the nation for identity theft. In 2015, Maryland ranked fourth in the nation for identity theft. The most common type of identity theft in Maryland was employment- or tax-related fraud, which comprised 39% of all complaints. The second most prevalent type of identity fraud involved credit card fraud and represented 31% of all complaints.

According to OAG, there were 790 security breach incidents in 2016 that required notifications to be sent to Maryland consumers, compared to 482 in 2015 and 333 in 2014.

Exhibit 1 shows the number of security breaches reported to OAG as well as the number of identity complaints received by FTC.

Exhibit 1
Security Breaches and Identity Theft Complaints in Maryland
2014-2016[1]

	2014	2015	2016	Average (2014-16)
Security Breaches Reports	333	482	790	**535**
Identity Theft Complaint Reports	5,734	11,006	8,251	**8,330**

[1]Security breaches are reported to the Office of the Attorney General (OAG) and are totaled by fiscal year; identity theft complaints are reported to the Federal Trade Commission (FTC) and are totaled by calendar year. Numbers reflect those reported to OAG or FTC as of March 11, 2017.

Source: Office of the Attorney General; Federal Trade Commission

Unfair or Deceptive Trade Practices under the Maryland Consumer Protection Act

An unfair 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 which has the capacity, tendency, or effect of deceiving or misleading consumers. The prohibition against engaging in any unfair 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 $1,000 for the first violation and up to $5,000 for each subsequent 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.

Additional Information

Prior Introductions: HB 529 of 2016, a similar bill, was heard in the House Economic Matters Committee and then withdrawn. HB 416 of 2015, a similar bill, was withdrawn without a hearing. In 2014, HB 676, another similar bill, was withdrawn after being heard in the House Economic Matters Committee.

Cross File: None.

Information Source(s): Office of the Attorney General (Consumer Protection Division); Congressional Research Service; Federal Trade Commission; Social Security Administration; Department of Legislative Services

Fiscal Note History: First Reader - March 13, 2017
kb/kdm

Analysis by: Eric Pierce

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