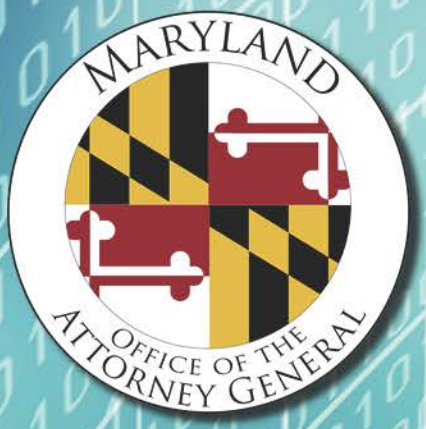
Data Breaches
FY 2018 Snapshot

Office of the Attorney General
Identity Theft Program



July 1, 2019

Table of Contents

Data Breaches: FY 2018 Snapshot

I. Introduction

This is the second in a series of annual reports recommended by the Maryland Cybersecurity Council to summarize the type and frequency of data breaches affecting Maryland residents.[1] This report covers Fiscal Year 2018 (FY 2018). The purpose of the report is to provide a snapshot of the magnitude of data breaches, their causes, and their impact on Maryland residents.

II. Statutory Summary

Breach notices are required in cases defined in statute and are published periodically on the Office of the Maryland Attorney General's (OAG) website.[2] The statutory requirements have been in part updated since the 2016 report.[3] As noted in that report, there are two significant data breach laws in Maryland. The first, the Maryland Personal Information Protection Act (MPIPA), became effective in 2008 and applies to private businesses.[4] The second, Protection of Information by Government Agencies, became effective on July 1, 2014 and is applicable to state government agencies, which were not previously subject to the requirements established under MPIPA.[5] A business or government unit providing notice of a security breach must notify the Maryland Office of the Attorney General prior to providing required notice to the affected Maryland residents, credit reporting agencies, and media outlets.

III. Fiscal Year 2018 Overview

Fiscal Year 2018 covers the period July 1, 2017 - June 30, 2018. During the year, there were 821 total breach notifications to the Office of the Maryland Attorney General. Not surprisingly, the breaches affecting Maryland residents form a catalogue of entities across all sectors, ranging from small to nationally known entities and underscores that for the consumer, there really is no safe harbor. Cases reported include banking, credit unions, investment counseling, retail, hospitality, insurance, mortgage, staffing agencies, postsecondary education, school districts, professional associations, government entities, law offices, dental and medical groups, airlines, and nonprofits, among others.

Taken together, the 821 separate notifications identified 4,049,531 Maryland residents as affected by a breach. Since the total number of residents affected is the sum of the residents reported in each breach notification, the total likely overstates the unique number of residents

---

[1] See Maryland Cybersecurity Council, Initial Activities Report (July 1, 2016), Recommendation 6 (p. 13) at http://www.umuc.edu/mdcybersecuritycouncil

[2] See Protect Yourself from Identity Theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

[3] See Data Breaches FY 2016 Snapshot, Office of the Attorney General Identity Theft Program, under Related Reports from the Office of the Maryland Attorney General at http://www.umuc.edu/mdcybersecuritycouncil

[4] Md. Code Ann. Com. Law § 14-3501 through §14-3508. MPIPA was updated by the General Assembly during the 2017 session (Chapter 518/House Bill 974). Changes made by Chapter 518 went into effect on January 1, 2018. Chapter 518 updates the definition of personal information to include additional forms of identification, health information, biometric data, and information that would allow access to an individual's e-mail account.

[5] Md. Code Ann. State Govt § 10-1301 through §10-1308. Chapter 518 did not make changes to the Government Agency statute

impacted. In fact, it is probable that some number of Maryland residents were affected by breaches at multiple organizations. One reason for believing this is that the massive Equifax, Inc., breach alone impacted 2,964,180 Maryland residents; fully 73% of the sum of all residents covered by the breach notifications.

The following chart illustrates the range of personal information exposed or lost as reported during the fiscal year.

Type of Personal Information Lost or Exposed	Total Maryland Residents Reported As Affected in Breach Notices	# Organizations Involved
Full social security number with at least name	3,575,046	446
Payment card information with other personal identifying information	140,807	193
Bank account number or other banking information with other personal identifying information	10, 349	41
Medical or treatment information with other personal identifying information	65,337	70

IV. Means of Compromise.[6]

A. Phishing.

Phishing occurs when employees are targeted with email messages that have attachments or links that contain malware. Spear phishing occurs when particular employees are targeted, such as those who work in finance or HR. A successful phishing attack can give attackers wide-ranging access to networks and the data that reside on them and even control over physical systems that may be controlled over networks. In FY 2018, 15% (129) of the breaches affecting the personal identifying information of Maryland residents were ascribed to employees falling prey to phishing attacks.

B. Retail Malware.

There are several types of malware that target point-of-sale (POS) devices and are meant to capture credit card information (full name, card numbers, expiration date and address). While the EMV chip used on credit cards is a security improvement, it is not a safeguard against retail malware. Approximately 10% (80) of the reported notifications impacting Maryland residents in FY 2018 concerned breaches due to this form of compromise.

C. Lost or Stolen Devices and Error

Not all data theft or exposure is digital. In 2018, about 4% (30) of the notifications to the Attorney General's office reported that personal identifying information was lost or exposed because a laptop, computer, or other device (e.g. hard drive or cell phone) had been lost or

[6] The categories used for 'means of compromise' and the data counts are determined wholly by how the breaches have been reported by the affected entities and do not reflect any independent forensic information.

stolen. Approximately 10% (78) of the breach notifications were triggered because of an inadvertent sharing of personal identifying information by an employee with the wrong recipient via emailing, faxing, or mailing.

D. Unauthorized or improper access.

By far, this form of compromise led the list in FY 2018. Of the 821 breach notifications in FY 2018, 378 (46%) attributed a breach or exposure to unauthorized or improper access. The most common cases reported in this category involved current or former employees or vendors accessing personal identifying information that they had no legitimate need to access. When this occurs, it can reflect lapses in basic data security procedures; viz. the absence of controls tying data access to work role, of monitoring data access, and of procedures for ensuring that access is terminated when an employee leaves. It can also reflect the theft and illegitimate use of credentials properly belonging to others.

E. Ransomware.

As a new threat, ransomware began to find mention in the major data breach reports in 2013. Ransomware captures data files and encrypts them, denying their use. Payment for the return of the decrypted files is typically demanded in a cryptocurrency, like Bitcoin. In FY 2018, a little over 4% (36) of the breach notifications received by the OAG identified ransomware as the cause of compromise.

V. Steps to Protect Your Identity.

The Office of the Maryland Attorney General's website brings together important information about how Maryland residents can proactively protect themselves from identity theft or overcome the consequences of identity theft when they occur. This includes guides compiled by OAG as well as information provided by the Federal Trade Commission and other entities. These resources can be found at
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

VI. More Information

For questions about this report, please contact:

Office of the Attorney General
Identify Theft Program
200 Paul Place
Baltimore, Maryland 21202
410-576-6491
idtheft@oag.state.md.us