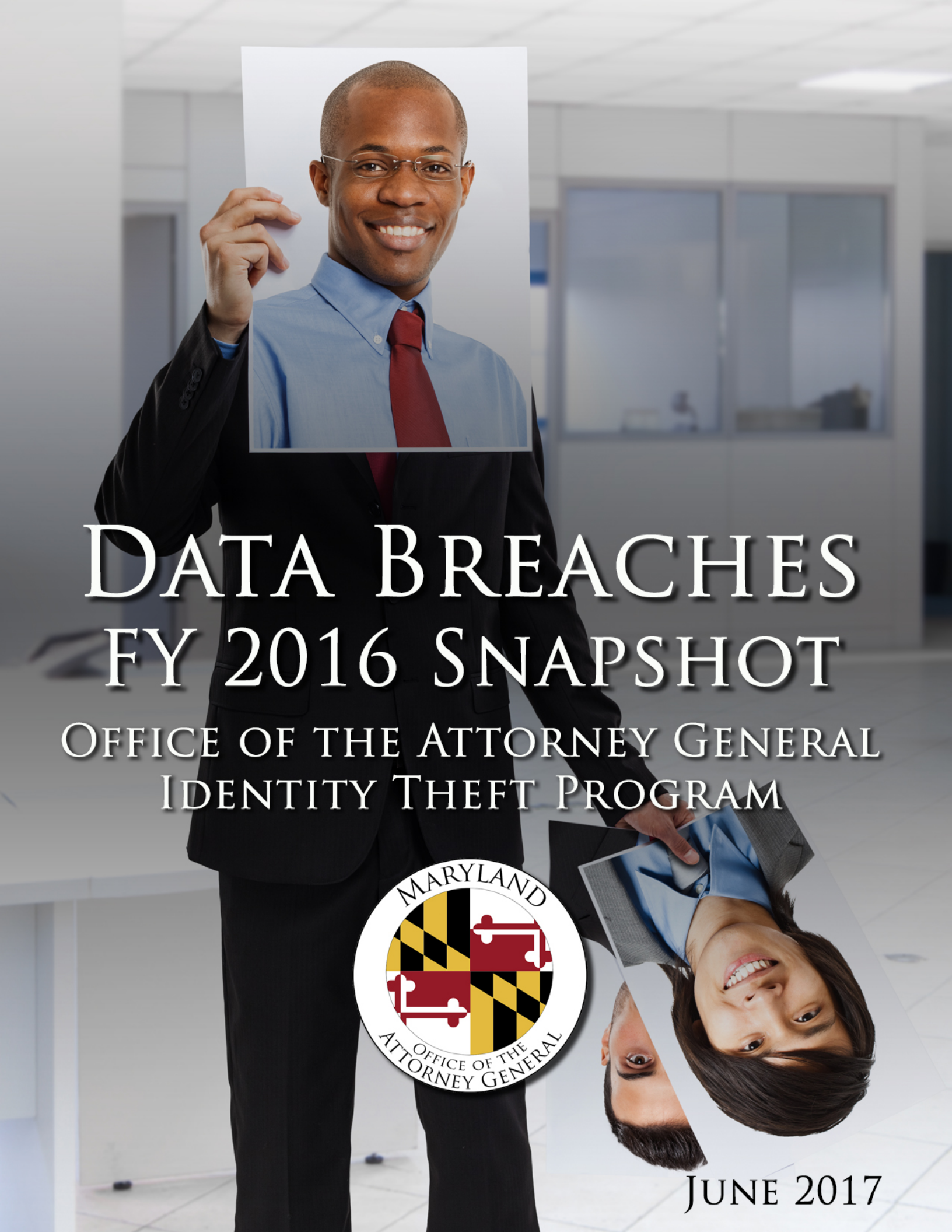


Data Breaches
FY 2016 Snapshot
Office of the Attorney General
Identity Theft Program

June 2017

I. Introduction

This report is responsive to a recommendation of the Maryland Cybersecurity Council to publish data on breaches affecting the State's citizens in particular.[1] While there are many studies on data breach frequency, these data are typically national in scope. The goal in producing data specific to Maryland is to sharpen public awareness and to aid policymakers. This Report represents an initial response. In subsequent years, the intention is to provide more data, analysis and context.

II. Statutory Overview

There are two significant data breach laws in Maryland. The first, the Maryland Personal Information Protection Act[2] (MPIPA) became effective in 2008 and applies to private businesses. The second, Protection of Information by Government Agencies[3], became effective on July 1, 2014 and is applicable to state government agencies, which were not previously subject to the requirements established under MPIPA. The breach laws require a business or government unit to:

- Implement "reasonable steps" to protect against unauthorized access to or use of personal information when destroying records[4];
- Implement reasonable security procedures and practices when storing and using personal information[5];
- Conduct an investigation if a security breach occurs; and
- Notify the Office of the Attorney General (OAG), and depending on the nature of the breach, notify affected Maryland residents, credit reporting agencies, and media outlets about a security breach.[6]

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 2016 Overview

There were 564 data breaches affecting more than 600,000 Maryland residents in Fiscal Year 2016 (FY 2016). The actual number of Maryland residents affected is not known because state law does not require businesses or government units to report the number of Maryland

---

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

[2] 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 go into effect January 1, 2018.

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

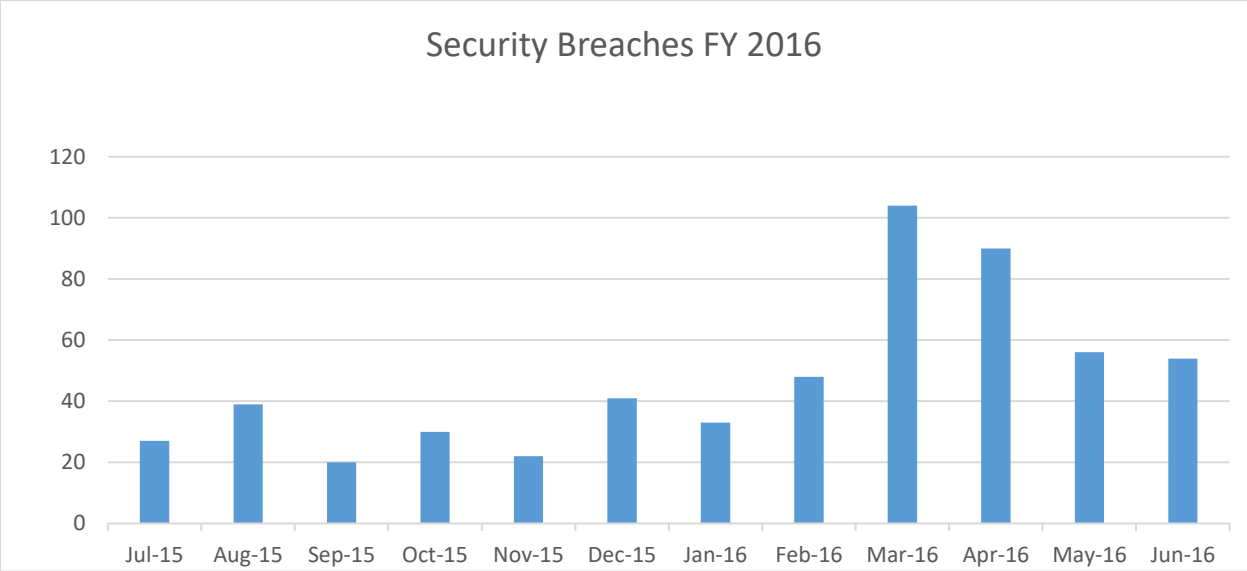
[4] Chapter 518 applies this requirement to employee records in addition to customer records.

[5] 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.

[6] Chapter 518 alters the trigger for notice by requiring notice to be given if the breach "creates a likelihood that personal information has been or will be misused."

residents who are affected by the data breaches. The number of residents reported is voluntary and therefore may be incomplete. This limitation is important since it means that year-on-year comparisons may include reporting differences rather than changes in the number of residents affected.

With this limitation in mind, the data set indicates that the 564 data breaches in 2016 represents a 41% increase from reported breaches in Fiscal Year 2015. The FY 2016 data breach monthly breakdown is as follows:



Entities reporting breaches cut across all sectors: banking, health insurance providers, the hospitality industry, law offices, and accounting firms, among others.[7]

IV. Data breach trends and examples

A. "Spear Phishing"

The months with the most reported data breaches were March 2016 and April 2016, respectively. More than half of the data breaches reported in March and April were the result of a hacking technique called "spear phishing." Spear phishing, is often highly preventable and is potentially extremely damaging to those whose information was compromised. In many instances, the hackers impersonate someone within the company, and then target a particular employee or group of employees via email. If the scheme is successful, unwitting company employees will either install malware into the computer network or actually send personal information directly to the hackers via email. The information targeted in the March and April breaches was frequently centered on employee 2015 W-2 income and tax statements. In such a case, the compromised information can include tax information, social security numbers, tax identification numbers, direct deposit information, and much else.

[7] See Maryland Information Security Breach Notices at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx

Spear phishing attacks are preventable because they rely, in part, on human behavior – and the willingness of the target to respond to requests. Training and education can reduce much of the risk associated with this hacking technique.

Victims of spear phishing are particularly vulnerable because they are at risk for at least three types of financial identity fraud. Depending on the particular information compromised, victims may be at risk for:

- Existing account fraud – Hackers may now have access to established financial accounts such as bank accounts;
- New account fraud – Hackers may use information to open new accounts, such as credit cards; and
- Tax fraud – Hackers are able to file a fraudulent tax return in the name of the victim.

B. Retail Malware

Data breaches caused by malicious software, or "malware,") were frequently reported by both online and brick and mortar retail entities. The malware, surreptitiously installed, is designed to capture payment card information when the customer checks out. The information captured generally includes card number(s), expiration date, name, and address. A retail malware data breach exposes data breach victims to the risk of existing account fraud. In FY2016 more than 50 data breaches were caused by malware.

C. Lost or stolen devices, inadvertent error

It would be folly to suppose that all data breaches are the result of hackers or technological sophistication. In fact, nearly 10% of the reported data breaches were the result of what could be called "old fashioned" techniques. Data breaches of this variety may be the result of human error or the secondary consequence of a related crime. Examples of this breach might include:

- stolen computer after a burglary or car break-in; or
- attaching the wrong file to an email, or perhaps sending mail or email to the wrong recipient.

Data breaches of this variety may lull victims into a false sense of security because the information was not sought out specifically by identity thieves. However, the inability to control the compromised information results in the uncertainty that the individuals affected by the data breach face much of the same risk for identity theft.

D. Unauthorized Access or Improper Use

This variety of data breach is generally the result of an employee improperly accessing or retaining personal information. In many instances where an employee improperly retained or used information, the breach notice noted the involvement of law enforcement or that the employee has been terminated.

E. Credit monitoring

More than 80% (464) of the data breach notices contained credit monitoring offers. Most of the credit monitoring offers were for a duration of 12-24 months. The details of each particular credit monitoring offer differ greatly in what is monitored, by whom, and for how long.

V. Conclusion

As noted, this report represents an initial effort to compile and analyze data on breaches that were reported to the Maryland Office of the Attorney General. While the data is limited, it nonetheless provides some evidence of the problem's scope and its causes.

VI. More Information

For questions about this Report, please contact:

Office of the Attorney General
Identity Theft Program
200 Paul Place
Baltimore, Maryland 21202
401-576-6491
idtheft@oag.state.md.us