Data Breaches
FY 2020 Snapshot

Office of the Attorney General
Identity Theft Program

May 25, 2021

Contents

Data Breaches: FY 2020 Snapshot

Introduction

This is the third in a series of 'snapshots' summarizing the type, frequency, and causes of data breaches affecting Maryland residents.[1] The breaches captured in each snapshot are those required to be reported by law to the Office of the Maryland Attorney General and to the Maryland residents specifically involved. The publication of these reports originated in a recommendation of the Maryland Cybersecurity Council to track the impact of breaches on Maryland residents and to inform policymaking.[2]

Statutory Summary

There are two significant data breach statutes in Maryland.

A. The first is the Maryland Personal Information Protection Act (MPIPA).[3] Enacted in 2008 and amended in 2017, the law spells out the notification requirements in cases where the "personal information" of Maryland residents held by businesses and nonprofits is breached, regardless of where the breached entity is located.

MPIPA defines two categories of "personal information":

- First name or first initial and last name *that are linked with* one or more data elements described in the statute *where either the name or the data element are not encrypted* or otherwise made unusable. The data elements are social security number or other taxpayer ID,

[1] See *Data Breaches: FY 2016* and *Data Breaches: FY 2018* at the Maryland Cybersecurity Council website under "Other Reports from the Office of the Maryland Attorney General", https://www.umgc.edu/administration/leadership-and-governance/boards-and-committees/maryland-cybersecurity-council/index.cfm

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

[3] 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.

passport number or other federal identification number, driver's license or other State ID, account numbers, credit or debit card numbers with information (e.g., security codes or passwords) that would allow access to a financial account, health information, health insurance policy or certificate numbers or subscriber ID numbers with other information that would allow access to health information, and biometric data that could be used to authenticate access to a system.

- Username or e-mail address combined with a password or security question and answer that would enable access to an individual's e-mail account.

MPIPA's notification provisions apply across the supply chain regardless of whether the breach occurred with the owner or licensee of personal information or a vendor maintaining the data for the owner or licensee. Under the Act, firms are not required to report a breach if they determine that the breach did not create "a likelihood that personal information has been or will be misused". In these cases, the information used to reach that determination must be preserved for three years and is subject to review by the Office of the Attorney General. The statute avoids increasing regulatory burdens by exempting entities already subject to the breach notification requirements of Gramm-Leach-Bliley and the federal Health Insurance Portability and Accountability Act of 1996 (HIPPA).

B. The second statute is the Protection of Information by Government Agencies Act[4], which became effective in 2014 and is applicable to government units. The Act extends breach notification requirements to the State executive branch, boards, commissions, public institutions of higher education, and political subdivisions such as municipalities, counties, county boards of education, and multicounty agencies. In general, the Act defines "personal information" held by government agencies in a manner similar to MPIPA and provides for similar exceptions to notification. The Act likewise recognizes that government entities may use third parties to hold data and extends the notification provisions to third-party breaches.

Fiscal Year 2020 Overview

For the fiscal year, 871 unique entities—businesses, nonprofits, units of government—reported breaches.[5] The total number of reported residents affected was 630,867. This likely overstates the number of unique residents impacted since breaches are reported separately by each entity involved, making it probable that some residents were affected by more than one breach. This is particularly true when viewed longitudinally. The cumulative number of separately reported Maryland residents affected for the three snapshots to date comes to more than 5.2 million.

[4] Md. Code Ann. State Govt § 10-1301 through §10-1308. Chapter 518 did not make changes to the Government Agency statute. With respect to public institutions of higher education, Md. Code Ann. State Govt § 10-1301 through §10-1308 was amended by the General Assembly in the 2020 session by House Bill 1122, https://mgaleg.maryland.gov/2020RS/chapters_noln/Ch_429_hb1122T.pdf. The changes take effect in 2024 but will not impact the snapshot reporting.

[5] Forty-four entities had two or more separate breach reports in the Office of the Attorney General's database and were de-duplicated in the report file to produce "unique entities breached". For each entity, the total number of residents affected was carried forward.

As has been the case, the entities involved in the FY 2020 breaches vary widely. Included are banks, insurance companies, real estate firms, mortgage companies, financial advisory firms, law firms, grocery chains, hospitals, colleges and universities, charities, churches, manufacturers, and municipalities, among others. National and regional brands are among the entities reporting breaches. The four largest breaches reported were CafePress, Inc. (367, 247 residents), StockX LLC (51,477), Jambav, Inc. (48,811), and Foods, Inc. (17,359).

The table below provides a selective breakout of the personal information breached. These categories bleed into each other. For example, many data files with name and social security number often include medical, banking or payment card information, and visa versa. Moreover, any of these categories may contain other data elements, such as physical address, date of birth, driver's license and/or passport number, email addresses and passwords, among other sensitive information.

Name With	# Reported Residents Affected	# Reported Entities Breached
Social security number	439,290	588
Medical or health information (clinical records. treatment history, diagnoses, prescription records, substance abuse records)	39,516	153
Banking and financial information (account numbers, transaction records, investment account numbers) often with other data elements, such as social security number, address, tax information, username, and password, among others	29,523	214
Payment card information (credit and debit), sometimes with other data elements, such as social security number, address, date of birth, email address(es), bank account information, among others.	55,629	153

Note that the breaches captured in the State data are those required to be reported by law. Consequently, it is unknown to what extent sensitive information of Maryland residents not required to be reported may have been exposed or breached during the fiscal year. Examples are activity tracking data (geolocation, web use) and genetic test information. Several bills have been proposed in recent sessions of the General Assembly to expand the categories of sensitive information for which breaches must be reported.[6]

[6] See 2019 SB 786 (SS 14-3501ff), 2020 SB 201/HB 237, and 2021 SB 112/HB 148. None were passed by the General Assembly.

Means of Compromise

The State data includes reported information about "how the data breach occurred". The following table captures the most frequently recurring explanations for breaches, accounting for the majority of breach cases.[7]

Cause as Reported	# Entities Reporting Cause of Breach	# Maryland Residents Reported as Affected
Unauthorized access	524	491,821
Phishing	84	13,578
Inadvertent exposure of data	39	2,055
Theft	26	1,815
Malware	93	31,029
Ransomware	51	6,996
Totals	**817**	**547,294**

The data naturally echoes the many reasons for breaches that are highlighted in media reports.

Unauthorized access was variously described as the result of credential sharing, hacking websites or systems, or failing to rescind the access of employees who left an organization, among other reasons. Inappropriate access not only involved data held by organizations for their own business purposes but also sensitive third-party data. Email accounts, databases, and servers were identified as targets of unauthorized access.

None of the reports involving phishing provided details, such as to whom or at what level of the organization the attack was addressed or the particular vehicle for the malware, whether an attachment or a link.

Entities reporting an inadvertent exposure of sensitive information provided a number of different explanations. These include sending the information to the wrong recipient, mistakenly providing employee access to contractor systems, failing to properly redact shared information, and misconfiguring servers, leaving data exposed on the internet.

Theft for the most part referred to the disappearance of a laptop or other device from an office or a car. One reported case involved the theft of documents containing sensitive information that were enroute to a shredding facility.

'Malware' and 'ransomware' are less about "how a breach occurred" and more about what happened after the intrusion, whether by phishing or other means. The reports did not detail the species of malware or ransomware involved.

[7] The causes of breaches are accepted as reported and have not been independently confirmed by forensic analysis.

Steps to Protect Your Identity

Apart from entities holding sensitive data, hackers often target consumers directly. Methods include apps, webpages, and online videos and photos that are compromised. Hackers can also gain access to home networks by exploiting vulnerabilities that might occur in devices on the network, such as virtual assistants, lights, appliances, and security cameras, among others.

The Federal trade Commission offers information to help consumers proactively protect themselves online. This includes guidance about computer and mobile security, networks, apps and devices, and common online scams.

Regarding identity theft in particular, the Office of the Maryland Attorney General's website brings together important information about how Maryland residents can protect themselves from identity theft or overcome the consequences of identity theft when they occur. These resources can be found here.

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