Data Breaches
FY 2022 Snapshot

Office of the Attorney General
Identity Theft Program

August 31, 2023

Contents

Data Breaches: FY 2022 Snapshot

Introduction

This is the fourth 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 and 2022, 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 the data element is not encrypted* or otherwise made unusable. The data elements are social security number or other taxpayer ID, passport number,

[1] Reports for FY 2016, FY 2018, and FY 2020 can be found at the Maryland Cybersecurity Council website under "Other Reports from the Office of the Maryland Attorney General", https://www.umgc.edu/mdcybersecuritycouncil.

[2] See Maryland Cyber Security Council, *Initial Activities Report (July 1, 2016)*, Recommendation 6 (p. 13), https://www.umgc.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) and the 2022 session (SB 643/HB 962). Chapter 518 updated 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. Chapter 503 added forms of genetic information as "personal information".

or other federal identification number, driver's license number or other State ID number, 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, biometric data that could be used to authenticate access to a system, and genetic information that is not protected by a method that would render it unreadable or unusable.

- 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 does 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 Act 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 2022 Overview

For the fiscal year, 1, 350 unique entities—businesses, nonprofits, units of government—reported breaches. The total number of reported residents affected was 940,654. Fourteen entities did not report the number of residents affected by their breach.[1]

As cautioned in previous reports, this number likely overstates the number of unique residents impacted. This is because breaches are reported independently by each entity, 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 four snapshot reports to date comes to more than 6.2 million.

As has been the case, the entities involved in the FY 2022 breaches vary widely. Included are a payment platform, automotive groups, unions, school districts, banks, insurance companies,

[1] Prior to October 2022, entities were not required to report the number of Maryland residents affected.

mortgage companies, health care providers, law firms, colleges and universities, cities, counties, and state departments, among others. National and regional brands are among the entities reporting breaches.

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.

Of the 1, 336 unique entities reporting the number of Maryland residents affected,[2] ten account for 64% of that number. The largest breach by far was reported by PayPal, impacting more than 233,000 Maryland residents. The majority of breaches were much smaller. The average number of residents affected by a breach was 705. Half of the reported breaches impacted fewer than six residents.

Table 1
Compromised Data[3]

Name With	# Reported Residents Affected	# Reported Entities Breached
Social security number	613,877	1,047
Social security number and date of birth	97,755	262
Social security number, date of birth, phone, and address	18,023	33
Biometric information	35,381	9
Medical or health information (e.g., clinical records. treatment history, diagnoses, prescription information)	75,221	150
Banking and financial information (e.g., account numbers, transaction records, investment account numbers, often with other data elements, such as social security number, address, tax information, username, and password)	160,305	395
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.	90,170	196

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

[2] This is the total number of entities reporting (1,352) less the entities (14) that did not indicate the number of residents affected by the breach. See Footnote 1.

[3] The analysis in this table and the next is preliminary, and the numbers should be treated as approximate magnitudes. The original dataset was de-duplicated. Sequential pivot tables were used to filter the data on keywords. There is terminological variation in how breached information and the cause of breach were reported. While care was exercised to take this variation into account, the filters used may nonetheless have overstated or understated the results by a relatively small margin.

required to be reported may have been exposed or breached during a given fiscal year. This is especially true of medical entities using the HIPAA exception under MPIPA and only reporting breaches to the U.S. Department of Health and Human Services. Activity tracking data (geolocation, web use) and biometric data are examples of data not covered by mandated reporting.

One objective of the breach notification statute is to ensure consumers are alerted so that they can take measures to protect themselves, such as by freezing their credit reporting accounts if they have not already done so. In the last two sessions, bills have been introduced to reduce consumer risk by giving consumers more control over the data commercially held about them by providing consumers more rights with respect to their data. These include the rights to know, correct, delete, and prohibit the sale or sharing of their data.[4]

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.

Table 2
How Breaches Occurred

Selected Causes as Reported	# Entities Reporting Cause of Breach	# Maryland Residents Reported as Affected
"Unauthorized access"	751	740,626
"Malware"	47	15,576
"Ransomware", "encryption attack", "malware encryption"	225	107,494
Totals	**1,023**	**863,696**

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

Of the 751 entities attributing their breach to "unauthorized access", fully 330 identified compromised "email" as how the breach occurred. This was followed by 225 entities attributing their breach to unauthorized access to a computer system or network. While only 14 entities specified "phishing" as the cause of their breach, it is likely that those entities reporting "email" as the cause are referring to phishing.

'Malware' and 'ransomware' are less about "how a breach occurred" and more descriptive of the payload delivered through the intrusion, whether phishing or other means. With few exceptions, the reports did not detail the species of malware or ransomware involved.

[4] Examples are SB 11 (Online Consumer Personal Information Privacy) in 2022 and HB 807/SB 987 (Consumer Protection - Online and Biometric Data Privacy in 2023. These bills were not enacted.

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