Data Breaches
Calendar Year 2024 Snapshot

Office of the Attorney General
Identity Theft Program

July 20, 2026

Contents Page

Data Breaches: 2024 Snapshot

Introduction

This is the fifth 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 previous years can be found at the Maryland Cybersecurity Council website under "Maryland Data Breach reports" at 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.

Calendar Year 2024 Overview

For the year, 1,615 unique entities—businesses, nonprofits, units of government—reported breaches. The total number of reported Maryland residents affected was 5,078,949. Sixteen entities did not report the number of residents affected by their breach.

As cautioned in previous reports, the total number of residents affected likely overstates the number of unique residents impacted. This is because breaches are reported independently by each entity, making it highly probable that some residents were affected by more than one breach in that calendar year. This is particularly true when viewed longitudinally over the five snapshot reports.

As has been the case, the entities involved in the 2024 breaches vary widely. Represented are critical infrastructure (communications, healthcare, banking and finance, government, manufacturing), colleges, universities, and school districts; nonprofits (religious organizations, trade

associations), law firms, insurance companies, and many other types of businesses. While the majority of entities reporting breaches are not national or regional brands, most of the entities reporting the largest breaches are. For the year, the five largest breaches accounted for 72% of the reported Maryland residents impacted.

Table 1

Largest Breaches Reported in Calendar Year 2024

Entity Breached	Reported # Maryland Residents Impacted	Personal Identifying Information Compromised
Comcast Cable Communications LLC	1,388,883	Name, Social Security number, driver's license number, date of birth, username and hashed password and/or secret questions and answers
Change Healthcare Inc.	1,300,000	Name, address, date of birth, phone number, email, health insurance data, health data, billing, insurance claims and payment data, and Social Security number, driver's license or state ID number
loanDepot, LLC	384,647	Name, address, email address, financial account numbers, social security number, phone number, and date of birth
Evolve Bank & Trust	315,005	Name, Social Security number, bank account number, and contact information
AT&T Inc.	295,716	Name, email address, mailing address, phone number, social security number, date of birth, AT&T account number, and AT&T passcode

The fact that only five entities account for 72% of reported impacted residents means that most of breaches were much smaller in scale. This is reflected in the low numbers for the mean and the median. Including the large breaches above, the average. number of reported residents impacted was 3,186. The median is seven, meaning that fifty percent of the breaches compromised the data of 7 or fewer residents.

One takeaway from the data is that because of the connected strings of personal information that have been compromised, the questions often used by banks and credit card companies to verify customers over the phone typically target categories of information that have often been compromised.

A second takeaway is that there are categories of sensitive data for which State law does not mandate reporting of breaches to OAG. Examples are geolocation data or web use.

Accordingly, it is unknown from the breach notifications the extent to which such information of Maryland residents may have been exposed or breached during a given calendar year.

Finally, 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 2024 legislative session, the State enacted the Maryland Online Data Privacy Act which aims to reduce risk created by a breach by giving consumers more control over the data commercially held about them. The Act provides for certain consumer rights, including the rights to know, correct, delete, and prohibit the sale or sharing personally identifying data.[1]

Means of Compromise

The State breach data includes reported information about "how the data breach occurred". The following table captures the most frequently recurring explanations provided by entities for breaches, accounting for the majority of breach cases. The data naturally echo specific types of attacks—ransomware, malware, phishing—that appear in media reports.

Table 2
How Breaches Occurred

Selected Causes as Reported	# Entities Reporting Cause of Breach
'Unauthorized access to computer/IT networks or systems'	860
'Unauthorized email access', 'phishing'	301
'Ransomware', 'Malware'	180
Total	**1,341**

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.

[1] Ch. 454, Acts of 2024 (SB 541/HB 567).

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 St. Paul Place
Baltimore, Maryland 21202
410-576-6491
idtheft@oag.state.md