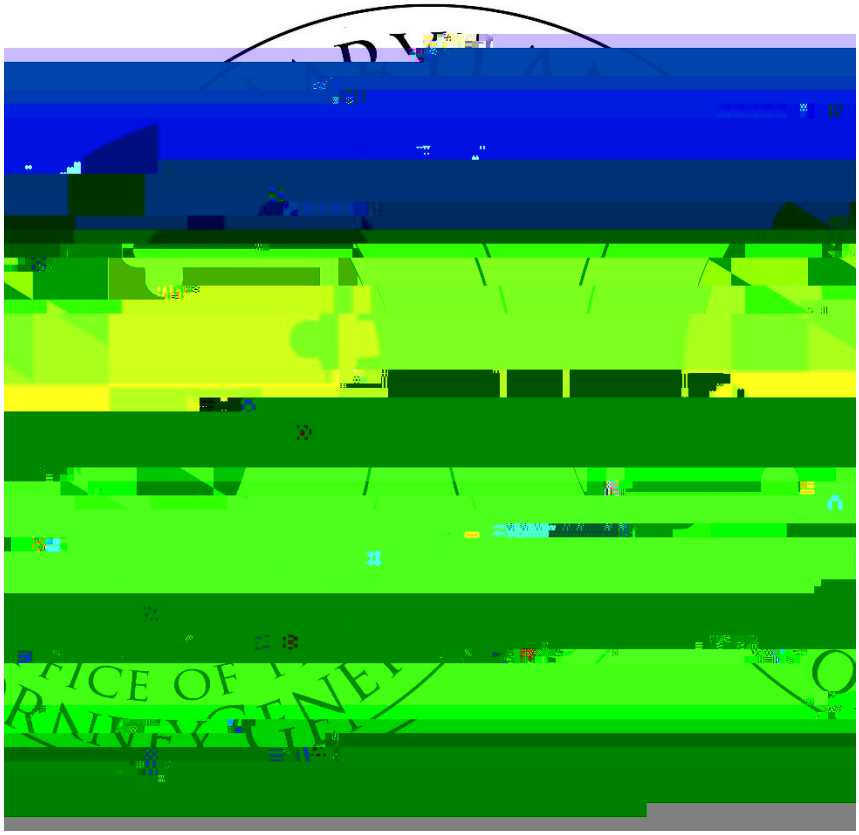
Data Breaches
FY 2020 Snapshot



Office of the Attorney General
Identity Theft Program

May 25, 2021

Data Breaches: FY 2020 Snapshot

Introduction

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 s

where the breached entity is located.

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

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 -mail account.

Means of Compromise

The State data includes 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.

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
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