BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief
Consumer Protection Division

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

March 16, 2022

TO: The Honorable Delores G. Kelley, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 643– Personal Information Protection Act - SUPPORT

The Office of the Attorney General supports Senate Bill 643 ("SB 643"), which amends the Maryland Personal Information Protection Act ("MPIPA") and provides much-needed protections to Maryland consumers. Specifically, SB 643 does the following:

- Requires companies that collect genetic information, but are not healthcare providers, to maintain it securely.
- Eliminates some loopholes that had previously allowed companies to delay notifying consumers about the breaches for months, and shortens some other notification deadlines.
- Requires companies that have the necessary contact information to notify consumers about breaches directly.

MPIPA requires companies that collect or store consumers' personal information to: (1) reasonably protect it, and (2) notify consumers, and the Attorney General's Office if there is a data breach that exposes that information.[1] MPIPA does not prevent businesses from collecting personal information—it only provides that, if the business collects it, the business has an obligation to protect that personal information. These baseline protections, however, only apply to data that fits within MPIPA's definition of personally identifiable information ("PII").[2] SB 643

[1] Md. Code. Ann., Com. Law §§ 14-3503; 14-3504 (2013 Repl. Vol. and 2019 Supp.).
[2] Currently, MPIPA defines personal information, in Md. Code Ann., Com Law § 14-3501(e)(1), as:
(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:
1. A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government;
2. A driver's license number or State identification card number;

amends MPIPA to update the definition of PII to include genetic information. The bill also clarifies the notification requirements following a breach. The amendments to MPIPA in SB 643 were the result of extensive negotiations during the 2020 session between the Attorney General's Office and industry representatives that were guided by Delegate Carey's and Senator Lee's offices.

The Bill Makes Necessary Updates to Keep Pace with Data Collection Practices

Currently, no federal or state law directly addresses data security issues resulting from direct-to-consumer genetic testing companies. The privacy risk posed by exposing a person's genetic information is, in many ways, even higher than that posed by financial information. Any disclosure of genetic information could have life-long consequences for the individuals concerned—you cannot change your genomic code. Unlike other PII, once genetic information is exposed, there is not a simple fix like being reissued a new credit card.

SB 643 requires companies to protect genetic information using the same data security practices as other sensitive information. Although the Health Insurance Portability and Accountability Act ("HIPAA") protects genetic information, it only applies to entities providing medical care. An increasing number of direct-to-consumer genetic testing companies offer individuals the opportunity to learn about their ancestry, genealogy, inherited traits, and health risks for a low cost and a swab of saliva. This presents an opportunity, but poses serious privacy risks because these companies have no statutory obligations to maintain this highly sensitive information securely. SB 643 extends the obligation to maintain genetic information securely that applies to healthcare providers to private companies by using the definition of "genetic information" found in federal health statutes.[3]

Genetic information deserves protection whether managed by a healthcare provider or by a company not covered by HIPAA's protections. Adding it to MPIPA simply means that companies that collect this information, and frequently profit from it, must reasonably protect it, and let consumers know if it has been stolen.

The Bill Updates How The AG Is Notified About Breaches

In addition to protecting personal information, MPIPA requires companies to notify consumers and the Attorney General's Office after it has been exposed. This allows consumers to take quick action to protect their information, such as changing passwords, freezing credit reports,

---

3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account;
4. Health information, including information about an individual's mental health;
5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; or
6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or

(ii) A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account.

[3] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH and GINA, 2013, § 160.103.

notifying financial institutions, and monitoring accounts. The Attorney General's Office needs to know about a breach quickly so that we can advise the throngs of consumers that call us asking for guidance on what to do and, when appropriate, take enforcement actions. The current law permits businesses to delay notification in two ways – (1) businesses are permitted an opportunity to first investigate the breach, and then (2) they have 45 days from the date of the conclusion of their investigation to issue their notice. This framework allows for too much of a time-lag between the discovery of the breach and the notification deadline. It also does not require companies to provide necessary information that would assist the Attorney General's Office in providing guidance to Marylanders. SB 643 will correct both of these issues.

Notifying Consumers About Breaches Earlier Allows Them to Protect Themselves

The longer a business waits to notify consumers about a breach, the greater the risk of harm and identity theft. This bill updates the timeline for providing notice and brings Maryland in line with the recent developments in this area. Companies are taking advantage of the current law. Right now, MPIPA requires notice "as soon as reasonably practicable, but not later than 45 days after the business concludes [its] investigation" into the breach. Md. Code Ann., Com. Law § 14-3504(b)(3). The triggering event to start the clock is after a company *concludes* an investigation into whether or not the data is likely to be misused. Companies have been elongating the investigation step and delaying its conclusion in order to postpone providing notice. This bill updates the triggering event for notification to when a business discovers a breach. **Numerous other states, including but not limited to Colorado, Florida, New Mexico, Ohio, Tennessee, Vermont Washington, and Wisconsin, use discovery of the breach as the trigger that starts the notification clock.**

When a hacker takes information, the likelihood is that the information will be misused. This bill recognizes this reality by shifting the default presumption in evaluating whether notification is necessary: it requires businesses to notify consumers unless they determine that the breach *does not* create a likelihood of misuse. In other words, businesses will have to notify consumers of a breach unless they can conclude there is not going to be harm to consumers.

SB 643 makes other necessary adjustments to the notice timelines to accomplish a quicker exchange of information. The business that owns or licenses the data is responsible for sending a breach notice, and the 45-day timeline discussed above relates to how long that data owner has to notify consumers after it becomes aware of a breach. However, sometimes businesses entrust their data to third parties, and when a breach occurs at that third party, the breach notice still comes from the business that owns or licenses the data. It is important for the data owner to know about the breach as soon as possible. Separate timelines are in place for how long a third party can wait before telling the data owner or licenser. Under the current law, that could *double* the time it takes for a consumer to learn about a breach, just because it occurred at a third party and not a direct owner of the data. That is unjustifiable, and this bill addresses that problem. If the breach of information in the possession of a third party occurs, the bill gives the third party 10 days from its discovery of the breach to notify the data owner, as the breach notice ultimately comes from the data owner. There is no reason to allow the third party to shield the information from the data owner for longer than that.

SB 643 fixes one other timeline loophole. Sometimes the FBI or Secret Service steps in to investigate a breach (often if they suspect it originated from a state actor). MPIPA allows a company to delay providing notice while law enforcement is investigating a breach if it is informed

by the investigating agency that a public breach notification will impede its investigation. That makes sense. But what does not make sense is that MPIPA currently allows a company to delay notice for up to 30 days after getting the go-ahead from the FBI or Secret Service to notify the public. That 30 days is on top of the other already-lengthy timelines for notification. While a law enforcement investigation should toll the timelines for notice, once law enforcement says that it is alright to notify, there is no reason to delay notification for 30 more days. Preparations to notify can, and must, be occurring in parallel with any FBI or Secret Service investigation. To that end, the bill changes that 30-day period to seven days after the law enforcement agency "green lights" public breach notification.

Ensuring That Consumers Receive and Absorb Notice of Breach

SB 643 improves the method of notifying consumers so that more people will receive notice and more people will comprehend the information conveyed.

There are two types of notice in MPIPA: (1) direct notice, which means sending mail directly to each affected consumer (or directly notifying by phone or possibly by email if certain requirements are met); and (2) substitute notice, which typically just means posting notice on the company's website and notifying major print or broadcast media outlets. As a result of feedback we received from other entities, the Sponsor has supplied an amendment that clarifies the way that direct notice will operate.

Direct notice is better and more effective than substitute notice for a number of reasons. Substitute notice is an ineffective means of notifying people without internet access, people who do not watch the news, and the many people that simply do not think general reports apply to them until they are notified directly. This was highlighted in the Equifax breach. Equifax first reported that 143.5 million SSNs had been breached. Equifax provided substitute notice. Later, Equifax discovered that an additional 2.5 million people were impacted. It decided to send the subsequent class direct notice by mail. The Attorney General's Identity Theft Unit received at least as many calls from consumers following the direct notice to 2.5 million people as we received after the substitute notice to the initial 143.5 million people.

When there are major breaches, big companies choose the ineffective substitute notice in order to save money, but it comes at the expense of consumers actually learning about the breaches that put them at risk. Under MPIPA, small companies already have to provide direct notice to each consumer. Big companies that put more people at risk should be held to the same standard; this bill removes the option of either direct notice or substitute notice unless a company lacks the relevant consumer contact information.

And finally, the bill addresses the content of breach notices to the Attorney General. MPIPA already requires a company to notify the Attorney General prior to notifying consumers, but gives no details on what the notice must contain.[4] As a result, we do not always receive the information that we need to properly respond to consumers who call us for help. This bill clarifies what information should be included in the notice to the Attorney General. This makes it easier on companies by taking out the guesswork as to what they should include in their notice and provides our office with the information that we need to assist consumers, including the number of affected Marylanders, the cause of the breach, steps the company has taken to address the

[4] Md. Code. Ann., Com. Law. § 14-3504(h).

breach, and a sample of the notice letters that will be sent to consumers. This information is readily available to companies at the time they provide notice.

For these reasons, we urge a favorable report.

Cc: Members, Finance Committee
The Honorable Susan C. Lee
The Honorable Brian J. Feldman
The Honorable Joanne C. Benson