BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.
(410) 576-6566 (F)

WRITER'S DIRECT DIAL NO.
(410) 576-7296

February 12, 2020

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

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 201 – Personal Information Protection Act - SUPPORT

The Office of the Attorney General supports Senate Bill 201 ("SB 201"), which provides much-needed protections to Maryland Consumers. The Office of the Attorney General supports the bill's amendments to the Maryland Personal Information Protection Act ("MPIPA").

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

It is no longer possible to participate in society without providing personal information to private companies and other third parties that reveal intimate details of one's life, either alone or in combination with other information.

MPIPA has a relatively limited scope. It simply 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] These baseline protections, however, only apply to data that fits within MPIPA's definition of personally identifiable information ("PII").[2] SB 201 amends MPIPA to update the definition of PII to include

[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;
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

new types of sensitive personal data that companies are collecting and clarifies the notification requirements following a breach.

SB 201 adds three types of personal information to the information that companies are required to protect using the same data security practices as other similarly sensitive information. The first is activity-tracking data. Wearable devices and mobile apps are collecting very sensitive information about our habits and daily lives. They track our location, our exercise and fitness habits, vital statistics, diet, weight, and even fertility cycles. Marylanders legitimately expect this kind of information to be private, and companies should be required to maintain this information securely.

The second type of personal information that SB 201 aims to protect is genetic information. An increasing number of companies offer consumers the opportunity to learn about their ancestry, genealogy, inherited traits, and health risks for a low cost and a swab of saliva. This presents a very exciting opportunity, but poses serious privacy risks. These companies do not always consider themselves "covered entities" under the Health Insurance Portability and Accountability Act ("HIPAA") and the current statutory definition of "personal information" does not presently include genetic information. Therefore a company that collects this highly personal, sensitive information could suffer a breach that is not covered under the existing law. The privacy risk posed by exposing a person's genetic information is, in many ways, even higher than that posed by financial information. You cannot change your genetic makeup; once genetic information is exposed, there is not a simple fix like being reissued a new credit card. In fact, the risks of exposing sensitive genetic information are so high that in December 2019 the Pentagon advised members of the armed forces not to use home DNA testing kits.

Third, SB 201 protects non-public social media information. Social media companies allow users to restrict the audience that can receive and view information that users posts. Users can also choose to share their information with the general public. SB 201 does not cover information made generally available to the public through social media. But, where social media companies invite users to share private information by creating spaces in which people feel safe sharing nonpublic information, for example sharing information with just your virtual friend, consumers have a legitimate expectation of privacy. This bill requires companies to maintain security practices that protect this non-public information the same way they are required to protect other personal information.

These three categories of information deserve protection. Adding them 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.

<u>The Bill Updates How We Are Notified About Breaches</u>

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

---

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.

take quick action to protect their information, such as changing passwords, freezing credit reports, 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 201 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. The European Union's celebrated General Data Protection Regulation ("GDPR") requires companies to provide notice within seventy-two (72) hours of discovering a breach (Article 33), and so do the New York Department of Financial Services Cybersecurity Regulations (N.Y. Comp. Codes R. Regs. Tit. 23 § 500.17). This bill does not go that far – it requires notification to occur with 30 days of discovery of a breach.

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). There are two problems with the current law. First, 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.

The second problem with the current law is that companies have been ignoring the operative clause: "as soon as reasonably practicable," and instead focusing only on the "45 days," often waiting right up until 45 days to provide notice. Such needless delay is harmful to consumers, as it provides criminals more time to exploit consumers' data before consumers are alerted that they are at risk. If consumers are informed, they can take steps to protect themselves. That is why the bill requires notifications within 30 days of discovery of a breach. 30 days is fair.[3] It is over ten times longer than the recent developments in this area in Europe (GDPR), and is

[3] The previous proposed bill suggested notification 10 days after discovery of a breach. This was extended to 30 days based on feedback from business representatives.

identical to the notification timeline in Colorado[4] and Florida.[5] Thirty days after discovery may sound like a short period of time, but the bill recognizes that businesses may need time to determine the scope and impact of a breach and provides time to do this. MPIPA Section 14-3504(d)(1)(ii) allows companies to delay notification "to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system." Companies will not have to rush to report a breach before they know what happened. Instead, the law allows time to make a determination. The point is to eliminate the reasons for delaying notification that companies are abusing now, such as business reasons, convenience, and the public relations impact. Breach notifications routinely come on Friday afternoons, which demonstrates that they are not currently coming "as soon as reasonably practicable," rather they are coming when companies hope fewer people will notice.

SB 201 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 30-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 201 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 three days after the law enforcement agency "green light" public breach notification.

Ensuring That Consumers Receive and Absorb Notice of Breach

SB 201 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

[4] C.R.S. § 6-1-716.
[5] Fla. Stat. § 501.171(3)(a).

requirements are met); and (2) substitute notice, which typically just means posting notice on the company's website and notifying statewide media.

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, so this bill removes the option of either direct notice or substitute notice, and instead requires both.[6]

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.[7] 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 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

[6] Currently, under MPIPA, a company can use substitute notice if direct notice would cost more than $100,000 or there are more than 175,000 affected consumers. Md. Code Ann., Com. Law § 14-3504(e).
[7] Md. Code. Ann., Com. Law. § 14-3504(h).