CPD Written Testimony SB643 SUPPORT.pdf
Uploaded by: Hanna Abrams
Position: FAV

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

SB643 MCRC Testimony 2022.pdf
Uploaded by: Isadora Stern
Position: FAV

Maryland Consumer Rights Coalition

Testimony to the Senate Finance Committee
SB 643: Commercial Law – Maryland Personal Information Protection Act – Revisions
Position: Favorable

March 16, 2022

Senator Kelley, Chair
Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, Maryland 21401
Cc: Members, Senate Finance Committee

Honorable Chair Kelley and Members of the Committee:

The Maryland Consumer Rights Coalition (MCRC) is a statewide coalition of individuals and organizations that advances economic rights and financial inclusion for Maryland consumers through research, education, direct service, and advocacy. Our 8,500 supporters include consumer advocates, practitioners, and low-income and working families throughout Maryland.

We are writing in support of SB 643. This bill increases the protection of Marylanders' personal information. SB 643 ensures that businesses that store personal information maintain reasonable security and are required to notify consumers of security breaches. This is a common-sense consumer protections bill that is much needed as data breaches have become the norm.

The FY 2020 report of the Attorney General 's Identity Theft Program indicates that 871 unique entities—businesses, nonprofits, units of government—reported breaches involving Maryland residents. The cumulative number of separately reported Maryland residents affected for the last three snapshot reports to date comes to more than 5.2 million.[1]

While data breaches have become a new norm so has security breach notice. SB 643 further expands notice of breaches affecting personal information by broadening the types of sensitive information which, if breached, must trigger notification. By adding genetic information and a more inclusive definition of 'health information' to the law, consumers' most private personal information will be protected.

Maryland residents deserve to know when their sensitive personal information is hacked. For these reasons, we support SB 643 and urge a favorable report.

Best,

Isadora Stern
Policy Associate

[1] https://www.umgc.edu/documents/upload/data-breaches-fy-2020-snapshot-pdf.pdf

2020-03-16 Letter to Finance SB643 -pdf.pdf
Uploaded by: Jane Santoni
Position: FAV

SANTONI, VOCCI & ORTEGA LLC

201 West Padonia Road, Suite 101A, Timonium, Maryland 21093
Telephone: 443-921-8161• Facsimile: 410-525-5704
www.svolaw.com

Jane Santoni
jsantoni@svolaw.com

Matthew Thomas Vocci
mvocci@svolaw.com

Chelsea Ortega
cortega@svolaw.com

March 16, 2022

Maryland General Assembly
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Re: SB 643
Maryland Personal Information Protection Act.
Position: Favorable

Dear Senators Kelly, Feldman and Members of the Finance Committee,

I am writing in support of SB 643, Maryland Personal Information Protection Act.

I am an attorney who has been representing consumers in Maryland for 20 years. I am writing on my own behalf and on behalf of the Maryland Association of Justice, which also supports this bill.

In my work, I have seen first-hand what happens when someone's personal information is not properly protected. This can negatively affect a person's finances, credit reports, reputation, and more. We shudder at the thought of someone breaking into our homes and stealing our goods, but a violation of our privacy is similar. It should not be carelessly handled or left unprotected.

This bill offers common sense protections. I hope you will vote favorably for it.

Very truly yours,

Jane Santoni

Jane Santoni

SB 643- Commercial Law – Maryland Personal Informa

Uploaded by: Robin McKinney

Position: FAV

SB 643- Commercial Law – Maryland Personal Information Protection Act – Revisions
Senate Finance Committee
March 16, 2022
SUPPORT

Chair Kelley, Vice-Chair, and members of the committee, thank you for the opportunity to submit testimony in support of Senate Bill 643. This bill will expand the Maryland Personal Information Protection Act (MPIPA).

The CASH Campaign of Maryland promotes economic advancement for low-to-moderate income individuals and families in Baltimore and across Maryland. CASH accomplishes its mission through operating a portfolio of direct service programs, building organizational and field capacity, and leading policy and advocacy initiatives to strengthen family economic stability. CASH and its partners across the state achieve this by providing free tax preparation services through the IRS program 'VITA', offering free financial education and coaching, and engaging in policy research and advocacy. **Almost 4,000 of CASH's tax preparation clients earn less than $10,000 annually. More than half earn less than $20,000.**

MPIPA is instrumental to providing Maryland consumers protection from data breaches. Data breaches are disturbingly common incidents that impact consumers across Maryland. In 2021, Maryland had over 800 instances of data breaches with some impacting thousands of Marylanders.[1] Many Marylanders' names, Social Security Numbers, birth dates, addresses, driver's license numbers, and more were exposed. Strengthening the MPIPA will ensure that consumers are notified of a data breach earlier and expand the ways that businesses who collect data are required to report. Significant damages to consumers' finances can happen when their personal information is in the wrong hands. Quicker notification and more extensive attempts to notify consumers will position them to respond to any threats in a fast and efficient manner. The faster consumers can address these threats, the less finance damage they will experience. **Given the frequency and severity of data breaches, the CASH supports better protections for consumers' information, and proper notice in the case of a security breach.**

The Consumer Protection Division of the Office of Attorney General is dedicated to helping Marylanders with complaints, scams and other consumer protection areas. Providing them with more information will allow for them to track and respond to data breaches more efficiently.

SB 643 will strengthen the MPIPA by:

- Covering additional types of personal information
- Expanding the types of businesses that are required to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized use
- Shortening the period within which certain businesses must provide required notifications to consumers after a data breach
- Requiring additional information to be provided to the Office of the Attorney General (OAG) after a breach has occurred.

These measures are necessary in order to ensure Maryland remains a national leader in consumer protection policy. ***We therefore urge this Committee to return a favorable report on SB 643.***

[1] Maryland Information Security Breach Notices

SB_ 643_T.ROWE PRICE_FWA.pdf
Uploaded by: Bryson Popham
Position: FWA

Bryson F. Popham, P.A.

Bryson F. Popham, Esq.

191 Main Street
Suite 310
Annapolis, MD 21401
www.papalaw.com

410-268-6871 (Telephone)
443-458-0444 (Facsimile)

March 16, 2022

The Honorable Delores G. Kelley and the Honorable Susan C. Lee
Senate Finance Committee Members
3 East, Miller Senate Office Building
Annapolis, Maryland 21401

RE: Senate Bill 643 - Commercial Law - Maryland Personal Information Protection Act – Revisions – FAVORABLE WITH AMENDMENTS

Dear Chair Kelley, Senator Lee and the Members of the Committee,

I am writing to you on behalf of my client, T. Rowe Price Group, Inc. T. Rowe Price is a global financial services company headquartered in Baltimore, Maryland, with an additional campus in Owings Mills, Maryland, and other offices in the United States and abroad. T. Rowe Price is a familiar name to Finance Committee members as one of the largest mutual fund complexes in the industry. T. Rowe also serves an important role as a service provider to other parties. For example, the company often provides record keeping services for employers who may sponsor a 401(k) plan, and it also provides administrative services for the Maryland 529 Plan.

T. Rowe Price is keenly aware of the importance of maintaining the security of the personal information that is the subject of Senate Bill 643 and its crossfile, House Bill 962. The amendment that is offered for Committee's consideration, and attached to this letter, provides a method for accelerating the notices required under the bill.

On page 4 of the bill, beginning at line 19, a requirement to notify an individual that a security system has been breached, and that the personal information of the individual may be misused, must be given within 45 days after discovery or notification of the breach.

On the same page, beginning at line 33, there is an additional 10-day notification requirement to the owner or licensee of the personal information. Therefore, the total notification period to the necessary parties can take as long as 55 days.

The amendment offered by T. Rowe Price is technical in nature; however, it provides an important mechanism whereby notices can be sent to both the affected individual and the owner or licensee of the personal information at the same time. For a record keeper or similar service provider such as T. Rowe Price, this is a more efficient method of delivering required notices and, as noted above, it will likely result in all necessary notices being delivered prior to the time limits set forth in the bill.

Therefore, we respectfully recommend a favorable report on Senate Bill 643, together with the attached amendment.

Very truly yours,

Bryson F. Popham

By:

AMENDMENTS TO SENATE BILL 643
(First Reading File Copy)

Amendment No. 1:

On page 4, in line 35, after "than" insert **(I),** and in line 36, after "system" add:

"OR (II) THE TIME THAT THE BUSINESS NOTIFIES THE INDIVIDUAL ON BEHALF OF THE BUSINESS THAT OWNS OR LICENSES THE PERSONAL INFORMATION IN ACCORDANCE WITH SUBSECTION (B) OF THIS SECTION."

Rationale:

This additional language will permit the simultaneous notification of an affected individual and the owner or licensee of personal information, thus enhancing the timeliness of notices required under the bill.

MD SB643 Testimony- RELX - FWA .pdf
Uploaded by: Caitlin McDonough
Position: FWA

March 16, 2022

The Honorable Delores Kelley
Chair, Senate Finance Committee
Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Re: Senate BILL 643 – THE MARYLAND PERSONAL INFORMATION PROTECTION ACT (Oppose unless Amended)

Dear Chair Kelley and Members of the Finance Committee:

I am writing on behalf of LexisNexis Risk Solutions ("LexisNexis"), a leading provider of credential verification and identification services for government agencies, Fortune 1000 businesses, and the property and casualty industry, to express concerns with Senate Bill 643, as introduced. We appreciate Senator Lee's efforts to refine existing law and bring the law up to date to ensure robust consumer protections. We are very cognizant of the importance of data security from our work with public and private sector organization in Maryland to detect and prevent identity theft and fraud. LexisNexis respectfully requests that the Committee consider amending the proposed legislation to clarify definitions and remove proposed changes to the notification requirements.

Senate Bill 643 amends MPIPA to require that a business that maintains Maryland personal information that it does not own or license and that incurs a data breach, notify the owner or licensee of the personal information exposed within 10 days of discovering or being notified of the breach. While well-intentioned, this change would set a burdensome standard that would be challenging to meet in the context of complex security incidents. Existing law is better aligned with the contractually established mechanisms for notice between businesses in the marketplace. Additionally, the requirement for the business to notify upon the discovery or notification of the breach adds to the challenging process. Requiring the notification after the business determines a breach allows for a more thorough investigation to be done in a timely manner. We join with other industry stakeholders in requesting there be more time and flexibility for businesses that maintain Maryland personal information and that may incur a breach to adequately determine the incident scope.

Under MPIPA, notification required under 14-3504(b) and 14-3504(c) may be delayed if a law enforcement agency determines the notification will impede a criminal investigation or jeopardize homeland or national security. However, notification is required as soon as practicable and not later than 30 days after law enforcement determines it will not impede a criminal investigation. Senate Bill 643 amends the law to require that notification be given as soon as reasonably practicable, but not later than 7 days after law enforcement determines it will not impede a criminal investigation or jeopardize homeland or national security. This does not provide sufficient time for a business that is obligated to wait for law enforcement to conclude its own investigation and provide information that is necessary for the business to undertake an impact assessment of the security incident and work towards the other components of delivering consumer notice. Nearly every other state breach notification law permits delayed notification in the context of a law enforcement investigation. The overwhelming majority of

such laws do not establish any corresponding time frame for notification following the conclusion of a law enforcement investigation.

The definition of "health information" in current law is "any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 regarding an individual's medical history, medical condition, or medical treatment of diagnosis." Senate Bill 643 removes "created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996" from the definition. This new definition is overly broad and should be refined to cover entities covered by the Health Insurance Portability and Accountability Act.

LexisNexis takes this opportunity to thank Senator Lee for her ongoing work on this issue and legislation and remains committed to working with him and the Committee to refine this legislation. Thank you for your consideration of LexisNexis' feedback on the proposed legislation.

Please let us know if we can answer any questions or provide any additional information.

Respectfully submitted,

Jeffrey Shaffer
Manager, Government Affairs, Mid-Atlantic
RELX (parent company of LexisNexis Risk Solutions)
1150 18th Street, NW, Suite 600
Washington DC, 20036
Mobile: 202-286-4894
Email: Jeffrey.shaffer@relx.com

SB643 - CGDP - Support w Amendment .pdf
Uploaded by: Caitlin McDonough
Position: FWA

COALITION FOR GENETIC DATA PROTECTION

March 16, 2022

The Honorable Delores Kelley
Chair, Senate Finance Committee
Miller Senate Office Building, 3 East
1 Bladen Street
Annapolis, MD 21401

RE: SENATE BILL 643 – COMMERCIAL LAW – MARYLAND PERSONAL INFORMATION PROTECTION ACT – REVISIONS – SUPPORT WITH AMENDMENTS

Dear Chair Kelley and Members of the Committee

On behalf of the Coalition for Genetic Data Protection (CGDP), a national coalition of the leading consumer genetic testing companies including 23andMe and Ancestry, we are writing to support Senate Bill 643 with amendments. Over the past several years, we have carefully considered the privacy and data protection issues incumbent with direct-to-consumer genetic testing services and agree with the bill sponsor and the proposed legislation that the genetic data held by our companies should be treated in the same manner as other personal information in the unlikely event of a data breach.

CGDP fully supports SB643 with an amendment to modernize the definition of "genetic information" included in the bill as introduced. The definition in the proposed legislation is from the 2008 federal "Genetic Information Nondisclosure Act" or GINA. That definition is outdated, limited in how it envisions genetic data is collected and used on behalf of modern consumers, and tailored specifically to anti-discrimination protections. The CGDP proposes the following definition be amended into the bill instead:

(III) Genetic Data means any data, regardless of its format, that results from analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material.

1. **Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other sources, and any information extrapolated, derived, or inferred therefrom.**

The proposed replacement definition better encapsulates all forms of genetic data, more accurately reflects the way genetic data is collected, held and used by modern direct-to-consumer genetic testing services, and is consistent with the definitions used in data breach statutes in other states, including California. The CDGP believes that, with the inclusion of the suggested definition, SB643 would ensure that consumers' genetic data is subject to the secure and protective treatment required for other forms of personal information under the existing Maryland Personal Information Protection Act.

CGDP

We take this opportunity to thank the bill sponsors and the Office of the Attorney General for working with us on amendments that significantly address our definitional concerns. We continue to work with the OAG to determine exactly how an entity that maintains genetic data, as defined in the bill, in a deidentified manner will comply with the provisions of the bill that require us to determine the number of impacted Maryland residents impacted by a breach. Deidentified data, by definition, means that we do not know whom the genetic data belongs to and, therefore, are unable to determine their state of residence. We appreciate the ongoing discussion on this point and look forward to additional guidance from the Consumer Protection Division on the best manner to comply.

The CGDP respectfully requests the Committee's favorable consideration of House Bill 962 with the suggested definitional amendment and clarification.

Sincerely,

Eric Heath
Chief Privacy Officer
Ancestry

Jacquie Haggarty
VP, Deputy General Counsel & Privacy Officer
23andMe

Steve Haro
Executive Director
Coalition for Genetic Data Protection

SB643_FAV_Lee_2022.pdf
Uploaded by: Susan Lee
Position: FWA

Susan C. Lee
Legislative District 16
Montgomery County

Majority Whip

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

Chair
Maryland Legislative Asian American
and Pacific Islander Caucus

President Emeritus
Women Legislators of the
Maryland General Assembly, Inc.

THE SENATE OF MARYLAND
Annapolis, Maryland 21401

James Senate Office Building
11 Bladen Street, Room 223
Annapolis, Maryland 21401
410-841-3124 · 301-858-3124
800-492-7122 *Ext.* 3124
Susan.Lee@senate.state.md.us

March 16, 2022

Senate Finance Committee

Senate Bill 643 – FAVORABLE– Personal Information Protection Act

Senate Bill 643 is a data breach notification update for Maryland's Personal Information and Protection Act (MPIPA). The provisions of this legislation aim to improve the security of how information that is sensitive about individuals is stored, and then how notice is provided to affected consumers. To meet the threshold of security required to be exempt from any notification requirements under law, a business merely has to put the personal information behind a firewall or encrypt it. If you use EITHER of those methods for to protect personal information, this law will not apply to you, however, if you fail to protect data, and it is breached, you would have to disclose that fact and provide notice to the parties who could be harmed.

Currently, MPIPA requires notice "as soon as reasonably practicable, but not later than 45 days after the business *concludes* [its] investigation" into the breach. This bill triggers the notification clock to start counting when a business *discovers* a breach. Many other states use this same trigger including but not limited to Colorado, Florida, New Mexico, Ohio, Tennessee, Vermont, Washington, and Wisconsin. SB 643 also updates the notice timeline when there is an investigation, but an amendment clarifies there would still be the underlying threshold of 45 days. Amendments further clarify that the notification requirements for genetic information that is de-identified to satisfy industry implementation concerns.

This is not a rehash of the larger consumer protection issue of control over your data, this bill wouldn't prevent doctor evil from using your DNA to make a mini-me, but it would require him to put that data behind a firewall. Other laws may apply to attempted world domination. There is a need to protect how data is used, but this bill is only about how data is stored, and the minimum requirement of notice if it has been compromised. The new provision about genetic data is focused on encouraging encryption of your genetic information, and then letting you know if it has been acquired by someone unlawfully.

This is and has been a consensus bill for some time, but we are bending backwards even more now with this year's version. There are pro-industry group changes like the clarification that you need both the name and the personal information to trigger a notification requirement that is ambiguous in the current law. The statute merely requires reasonable protection of personal data, and notification to consumers and Consumer Protection Division at the Attorney General's office if there is a data breach.

The cross-file HB 962 has already passed the House and the amendment that was attached to further the compromise can be viewed here and will also be uploaded for the committee's file of course. This was a compromise in 2020, and again last year, but this session we have the time to get it passed so that at least data is protected by the companies that have control over it, because it is not yet controlled by the consumer until we pass more sweeping legislation like the Online Consumer Protection and Child Safety Act. This is the low hanging fruit that could create a rot if we don't pick it quickly.

For these reasons, I respectfully request a favorable report on SB 643 as amended to conform to the House cross-file language.

SB 643_Commercial Law - Maryland Personal Informat
Uploaded by: Maddy Voytek
Position: UNF

MARYLAND
Chamber of Commerce

LEGISLATIVE POSITION:
Unfavorable
Senate bill 643
Commercial Law – Maryland Personal Information Protection Act – Revisions
Senate Finance Committee

Wednesday, March 16, 2022

Dear Chairwoman Kelley and Members of the Committee:

Founded in 1968, the Maryland Chamber of Commerce is the leading voice for business in Maryland. We are a statewide coalition of more than 5,500 members and federated partners working to develop and promote strong public policy that ensures sustained economic recovery and growth for Maryland businesses, employees, and families.

The purpose of the State's data breach law is to require that state residents be notified when there has been an unauthorized acquisition of certain types of unencrypted, computerized personal information (PI) that could lead to a risk of financial harm or identity theft. HB 962 seeks to change this law in a manner that causes concerns to the broader business community.

Some of the primary concerns with SB 643 include:

- There are several changes in the bill with respect to specified time periods for providing notices of a data breach. The bill cuts notification time in more than half and creates serious challenges for businesses that are dealing with other complications from the breach.
- The bill also removes language referencing investigations that are conducted when a breach is suspected. This means that notification must happen when a breach is suspected instead of determined. Investigations are vital to determining if a breach truly happened and what information was compromised. By removing the investigative requirement businesses risk causing widespread panic among the public when a breach may not have actually occurred.
- 14-3504(h)(2)(II) requires that a business provide precise information to the Attorney General as to how a breach occurred. SB 643 is different from previous version in that this information would not be required to become public, however, we remain concerned that this information could be accessed by bad actors providing a roadmap on how security systems were compromised.

The Maryland Chamber of Commerce greatly appreciates the work done on this legislation over the years by the sponsor. We remain committed to working alongside other stakeholders

impacted by the outcomes of SB 643 and the sponsor to find a solution that meets the intent of this legislation in an effective and sensible manner without undue burden.

For these reasons, the Maryland Chamber of Commerce respectfully requests an **unfavorable report** on **SB 643**.