AG Written Testimony SB 112.pdf
Uploaded by: Abrams, Hanna
Position: FAV

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 10, 2021

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

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 112– Personal Information Protection Act - SUPPORT

The Office of the Attorney General supports Senate Bill 112 ("SB 112"), which amends the Maryland Personal Information Protection Act ("MPIPA") and provides much-needed protections to Maryland consumers. Specifically, SB 112 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 112

[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;

amends MPIPA to update the definition of PII to include genetic information. The bill also clarifies the notification requirements following a breach.

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. 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 112 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 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 112 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]

In the context of COVID-testing this may be even more critical than ever. With direct-to-consumer testing kits recently being approved by the FDA,[4] any business can administer its own COVID tests. 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 We Are 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, notifying financial institutions, and monitoring accounts. The Attorney General's Office needs to

---

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

[4] *FDA Authorizes First Direct-to-Consumer COVID-19 Test System; Test system is authorized for at-home sample collection with laboratory test processing*, FDA Press Release, Dec. 9, 2020.

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 112 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), as does 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 within 45days 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). 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 112 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 112 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 112 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, so this bill removes the option of either direct notice or substitute notice unless a company lacks the relevant consumer contact information. SB 112 also requires the companies to post a notice on their website and notify major media to ensure that as many affected consumers as possible have access to information about a breach. A data breach should not be a secret; companies should not be able to keep this information hidden.

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.[5] As a result, we do not always receive the

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

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 Lee

SB 112 Commercial Law - Personal Information Prote

Uploaded by: McKinney, Robin

Position: FAV

SB 112- Commercial Law - Personal Information Protection Act - Revisions
February 10, 2021
SUPPORT

Chairwoman Kelley, Vice-Chair and members of the committee, thank you for the opportunity to provide testimony in support of Senate Bill 112. 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 2020, Maryland had over 900 instances of data breaches.[1] Many Marylanders' names, Social Security Numbers, birth dates, addresses, driver's license numbers, and more were exposed. Strengthen the MPIPA will ensure the 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, 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 112 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 112.***

[1] https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx

MDDCCUA SB112 Commercial Law – Personal Informati

Uploaded by: Murray, Rory

Position: FAV

MD|DC
Credit Union Association

Chairwoman Delores Kelley
3 East
Miller Senate Office Building
Annapolis, MD 21401

SB112: Commercial Law – Personal Information Protection Act – Revisions
Testimony on Behalf of MD|DC Credit Union Association
Position: Support

Chairwoman Kelley, Vice-Chair Feldman and Members of the Committee:

On behalf of the MD| DC Credit Union Association and the 77 Credit Unions and their 2.2 million members that we represent in the State of Maryland, we appreciate the opportunity to testify on this legislation. Credit Unions are member-owned, not-for-profit financial cooperatives whose mission is to promote thrift and provide access to credit for provident and productive purposes for our members. The MD|DC Credit Union Association is in support of modifying the current security breach notification requirements.

The current law allows a business to conduct an internal investigation **prior** to 45-day window to notify consumers about a data breach begins. This standard is far too unpredictable because companies can take as long as they would like to conduct an internal investigation. The ambiguity in the current law is harmful to consumers. Removing the provision which allows the internal investigation to be conducted prior to the notification window beginning, will ensure, unless law enforcement directs the business to delay notification, that consumers are aware that their data may have been compromised within 45 days that the business discovers or is notified of the breach. Consumers should have knowledge of a potential compromise of their information as early as possible, and this bill will help accomplish the goal.

Please do not hesitate to contact me at 443-325-0774 or jbratsakis@mddccua.org, or our VP of Advocacy, Rory Murray at rmurray@mddccua.org should you have any questions. Thank you for your consideration.

Sincerely,

John Bratsakis
President/CEO
MD|DC Credit Union Association
8975 Guildford Rd., Suite 190
Columbia, MD 21046

MDDCCUA SB112 Commercial Law – Personal Informati

Uploaded by: Murray, Rory

Position: FAV

MD|DC
Credit Union Association

Chairwoman Delores Kelley
3 East
Miller Senate Office Building
Annapolis, MD 21401

SB112: Commercial Law – Personal Information Protection Act – Revisions
Testimony on Behalf of MD|DC Credit Union Association
Position: Support

Chairwoman Kelley, Vice-Chair Feldman and Members of the Committee:

On behalf of the MD| DC Credit Union Association and the 77 Credit Unions and their 2.2 million members that we represent in the State of Maryland, we appreciate the opportunity to testify on this legislation. Credit Unions are member-owned, not-for-profit financial cooperatives whose mission is to promote thrift and provide access to credit for provident and productive purposes for our members. The MD|DC Credit Union Association is in support of modifying the current security breach notification requirements.

The current law allows a business to conduct an internal investigation **prior** to 45-day window to notify consumers about a data breach begins. This standard is far too unpredictable because companies can take as long as they would like to conduct an internal investigation. The ambiguity in the current law is harmful to consumers. Removing the provision which allows the internal investigation to be conducted prior to the notification window beginning, will ensure, unless law enforcement directs the business to delay notification, that consumers are aware that their data may have been compromised within 45 days that the business discovers or is notified of the breach. Consumers should have knowledge of a potential compromise of their information as early as possible, and this bill will help accomplish the goal.

Please do not hesitate to contact me at 443-325-0774 or jbratsakis@mddccua.org, or our VP of Advocacy, Rory Murray at rmurray@mddccua.org should you have any questions. Thank you for your consideration.

Sincerely,

John Bratsakis
President/CEO
MD|DC Credit Union Association
8975 Guildford Rd., Suite 190
Columbia, MD 21046

RELX Letter Re MD SB112 - favorable with amends.pd
Uploaded by: McDonough, Caitlin
Position: FWA

January 18, 2021

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

Re: MD SB 112 (favorable with amendments to 14-3504(c)(2) and 14-3504(d)(2))

Dear Chair Kelly:

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 insurance industry, to express concerns with the proposed modifications to the Maryland Personal Information Protection Act (MPIPA) included under 14-3504(c)(2) and 14-3504(d)(2) of Senate Bill 112.

We appreciate Senator Lee's efforts in the Senate and Delegate Carey's efforts in the House 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 organizations in Maryland to detect and prevent identity theft and fraud.

Senate Bill 112 amends MPIPA under 14-3504(c)(2), 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 that maintain Maryland personal information and that may incur a breach to adequately determine the incident scope. We share the concerns other industry stakeholders have raised with this provision and want to underscore the critical importance of affording flexibility for businesses under this section of the law.

LexisNexis requests Senate Bill 112 revert to existing law by striking the proposed changes under 14-3504(c)(2).

Under MPIPA, the notification required under 14-3504(b) and 14-3504(c) may be delayed under 14-3504(d)(1)(i) 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.

LexisNexis Risk Solutions Telephone: 202-403-7346 julien.nagarajan@relx.com
www.risk.lexisnexis.com

Senate Bill 112 amends 14-3504(d)(2), 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 is simply not feasible operationally for a business that is obligated to wait for law enforcement to conclude its own investigation and provide information 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 and the vast majority of such laws do not establish any corresponding time frame for notification following the conclusion of a law enforcement investigation.

LexisNexis requests Senate Bill 112 revert to existing law by striking the proposed changes under 14-3504(d)(2).

We remain committed to working with Senator Lee on Senate Bill 112 and with Delegate Carey on the House companion measure as they continue to refine this legislation and engage key stakeholders. Thank you for your consideration of LexisNexis feedback on the proposed changes made by Senate Bill 112 to MPIPA under 14-3504(c)(2) and 14-3504(d)(2).

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

Respectfully submitted,

Julien Nagarajan
Manager, Government Affairs Mid-Atlantic & US Health Policy
RELX (parent company of LexisNexis Risk Solutions)
1150 18th Street, NW, Suite 600
Washington, DC, 20036
Mobile: (202) 403-7346
Email: julien.nagarajan@relx.com

CC Senator Susan Lee

SB112 - CGDP - Support w Amendment .pdf
Uploaded by: McDonough, Caitlin
Position: FWA

COALITION FOR GENETIC DATA PROTECTION

February 10, 2021

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

RE: SENATE BILL 112 – COMMERICAL LAW – PERSONAL INFORMATION PROTECTION ACT – REVISIONS - TESTIMONY IN SUPPORT WITH AMENDMENT

Dear Chair Davis:

The Coalition for Genetic Data Protection (CGDP) serves to provide a unified and proactive voice to advance policies that ensure the privacy and security of an individual's genetic data and enable responsible innovation. Consumer genetic testing can empower consumers to take a proactive role in their health, wellness, ethnicity, and origin in unprecedented ways – and millions of consumers have taken advantage of these opportunities. At the same time, genetic data provides unprecedented opportunities for the research community to better understand the role genetics play in our health and well-being as a human population. While we recognize the significant opportunities genetic testing and research present, we also support and advocate for reasonable and uniform privacy regulation that will ensure the responsible and ethical handling of every consumer's genetic data.

Senate Bill 112 (SB112), as introduced, makes several changes to the Maryland Personal Information Protection Act (MPIPA), including updating the definition of "personal information" to include genetic data. CGDP does not oppose the inclusion of genetic data in MPIPA, but it would propose a more modern definition of genetic data that better encompasses the current collection and use practices for this type of data and also takes into consideration existing federal regulation for genetic data collected for specific purposes. Below, please find a proposed definition for genetic data for the Committee's consideration:

(A) "Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample obtained from a natural person (an "individual"), and concerns information about an individual's inherited or acquired genetic characteristics, including: deoxyribonucleic acid (DNA), ribonucleic acid (RNA), genes, chromosomes, alleles and genome.

(B) "Genetic data" does not include deidentified data. For purposes of this subparagraph, "deidentified data" means data that cannot be used to link information to a particular individual, provided that the business that possesses the deidentified data does all of the following:

(i) Takes reasonable measures to ensure that the deidentified data cannot be linked with an individual.

(ii) Publicly commits to maintain and use the deidentified data only in deidentified form and not to attempt to reidentify the deidentified data, except that the business may attempt to reidentify the deidentified data solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subparagraph, provided that the business does not use or disclose any reidentified data in this process and destroys the reidentified data upon completion of that assessment.

(iii) Contractually obligates any recipients of the deidentified data to take reasonable measures to ensure that the deidentified data cannot be linked with an individual and to commit to maintaining and using the deidentified data only in deidentified form and not to reidentify.

CGDP

(C) "Genetic data" does not include any data that is collected, used, maintained, and disclosed exclusively for scientific research, clinical trial, or other biomedical research conducted in compliance with applicable federal and state laws and regulations for the protection of human subjects in research, including, but not limited to, the Common Rule pursuant to Part 46 (commencing with Section 46.101) of Title 45 of the Code of Federal Regulations, United States Food and Drug Administration regulations pursuant to Parts 50 and 56 of Title 21 of the Code of Federal Regulations, the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g), or the Protection of Human Subjects in Medical Experimentation Act, Chapter 1.3 (commencing with Section 24170) of Division 20 of the Health and Safety Code.

(D) "Genetic data" does not include any physical biological sample.

CGDP believes amending SB112 to include this comprehensive definition of genetic data, in place of the drafted definition of "genetic data" is more consistent with other aspects of the legislation, including provisions dealing with deidentified data and overlapping federal regulation. The proposed definition is also in keeping with the types of services that are now associated with the collection and use of genetic data, as opposed to it solely being used for health testing purposes. CGDP looks forward to working with the bill sponsor, the members of the Committee, and the Attorney General's Office to develop and implement reasonable policy for the use and protection of genetic data in Maryland.

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

cc:

IIAM 2021 Testimony on SB 112 Maryland Personal In

Uploaded by: Lininger, Brett

Position: UNF

Written Testimony from the
Independent Insurance Agents of Maryland
Senate Bill 112

Maryland Personal Information Act - Revisions

Position: Oppose

Dear Chairman Kelley and members of the Senate Finance Committee,

Thank you for the opportunity to provide this testimony in opposition to SB 112. The Independent Insurance Agents of Maryland (IIAM) is the State's oldest trade association of independent insurance agents. It represents 200 independent agencies, which employ over 2000 people in the state. IIAM represents independent insurance agents and brokers who present consumers with a choice of policy options from a variety of different insurance companies. These small, medium, and large businesses offer a variety of insurance products – including property, casualty, life, health, employee benefit plans, and retirement products.

The majority of our members are very small businesses with limited resources. We currently take every precaution to protect the personal information of all our clients. The provisions set forth in SB 112 will make this process more onerous and costly for these businesses. We urge your unfavorable vote on this legislation.

IIA Maryland's Legislative Representation

Legislative Committee Chair
Jay Duke
Waring-Ahearn Insurance Agency, Inc.
P.O. Box 666
Leonardtown, MD. 20650
Telephone: 301-475-5541
Fax: 301-475-3441
Email: Jay@waring-ahearn.com

Legislative Advisor
Brett S. Lininger, Esq.
Old Line Government Affairs
100 West Pennsylvania Avenue, Suite 101G
Baltimore, MD 21204
410-321-8200
Email: blininger@nemphosbraue.com

Denise Carnes, CPCU
Insurance Services Group, Inc.
309 International Circle, Suite 100
Hunt Valley, MD 21030
Telephone: 410-296-5700
Fax: 410-296-7546
Email: dcarnes@isgusa.com

Sandy Chaney, CIC, CRM
The Insurance Exchange, Inc.
9713 Key West Ave., Ste 401
Rockville, MD. 20850
Telephone: 301-545-1595
Email: chaney.s@tie-inc.com

Pamela Dodge, CIC, CISR, CPIA
RMS, LLC
2330 West Joppa Road, #365
Lutherville, MD. 21093
Telephone: 410-526-6690
Email: pamela@hellerkowitz.com

Michael McCartin, CPCU
Joseph W. McCartin Insurance
P.O. Box 899
College Park, MD. 20740
Telephone: 301-937-0400
Fax: 301-937-5120
Email: Mike@McCartin.com

Stacey Nicholson, CIC, CPCU, LUTCF
CNR Insurance, Inc.
166 West Street
Annapolis, MD. 21409
Telephone: 410-897-9890
Email: stacey@cnrinsurance.com

Shannon O'Hare, ACSR
Maury Donnelly & Parr, Inc.
22 Commerce Street
Baltimore, MD. 21202
Telephone: 410-685-4625
Email: sohare@mdpins.com

Rick Raley, AAI, CIC
Combs, Drury, Reeves Insurance Agency
41625 Park Avenue
Leonardtown, MD. 20650
Telephone: 301-475-5674
Fax: 301-475-5665
Email: rick.raley@cdrassociated.net

G. Bradford Reeves, AAI, AFIS
Combs, Drury, Reeves Insurance Agency
41625 Park Avenue
Leonardtown, MD. 20650
Telephone: 301-475-5674
Fax: 301-475-5665
Email: brad.reeves@cdrassociated.net

Christopher Weller
Monterey Insurance Group
3235 Solomons Island Rd
Huntingtown, MD. 20639
Telephone: 410-535-0416
Email: chris.weller@monteresyinsurancegroup.com

SB 112_MAMIC_UNF.pdf
Uploaded by: Popham, Bryson
Position: UNF

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)

February 10, 2021

The Honorable Delores G. Kelley
The Honorable Susan Lee
3 East, Miller Senate Office Building
Annapolis, MD 21401

RE: Senate Bill 112 - Commercial Law - Personal Information Protection Act - Revisions

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

I am writing on behalf of the Maryland Association of Mutual Insurance Companies (MAMIC) to register our opposition to SB 112 - Commercial Law - Personal Information Protection Act – Revisions.

MAMIC is comprised of 12 mutual insurance companies that are headquartered in Maryland and neighboring states. Approximately one-half of MAMIC members are domiciled in Maryland and are key contributors and employers in their local communities. Together, MAMIC members offer a wide variety of insurance products and services and provide coverage for thousands of Maryland citizens. Although some mutual insurance companies may be large organizations, MAMIC members tend to be small and medium-sized businesses.

SB 112, at page 4, lines 21 through 25, eliminates the time period in current law under which a business conducts its required investigation of a breach of the security system. The removal of a reasonable opportunity to conduct an investigation may well make it impossible to conduct that investigation.

The bill also, at page 6, lines 21-23, introduces a new publication requirement of a breach using the term "MAJOR PRINT OR BROADCAST MEDIA IN GEOGRAPHIC AREAS WHERE THE INDIVIDUALS AFFECTED BY THE BREACH LIKELY RESIDE." MAMIC respectfully submits that compliance with this new standard would be difficult, if not impossible.

Finally, MAMIC notes that SB 112, at page 7, line 16, requires the notice to describe a breach, "INCLUDING WHEN AND HOW IT OCCURRED." This new requirement not only raises the question of adequate compliance with the statutory language, it also introduces the likelihood that a MAMIC member, in attempting to comply, may have to reveal confidential information regarding its security systems. In other words, the notice itself could further jeopardize the security of the entity.

For these and other reasons, MAMIC respectfully requests an unfavorable report on SB 112.

Very truly yours,

Bryson F. Popham

cc: Members of the Senate Finance Committee

SB 112_Opposed_MAMIC.pdf
Uploaded by: Popham, Bryson
Position: UNF

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)

January 18, 2021

The Honorable Delores G. Kelley
The Honorable Susan Lee
3 East, Miller Senate Office Building
Annapolis, MD 21401

RE: Senate Bill 112 - Commercial Law - Personal Information Protection Act - Revisions

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

I am writing on behalf of the Maryland Association of Mutual Insurance Companies (MAMIC) to register our opposition to SB 112 - Commercial Law - Personal Information Protection Act – Revisions.

MAMIC is comprised of 12 mutual insurance companies that are headquartered in Maryland and neighboring states. Approximately one-half of MAMIC members are domiciled in Maryland and are key contributors and employers in their local communities. Together, MAMIC members offer a wide variety of insurance products and services and provide coverage for thousands of Maryland citizens. Although some mutual insurance companies may be large organizations, MAMIC members tend to be small and medium-sized businesses.

SB 112, at page 4, lines 21 through 25, eliminates the time period in current law under which a business conducts its required investigation of a breach of the security system. The removal of a reasonable opportunity to conduct an investigation may well make it impossible to conduct that investigation.

The bill also, at page 6, lines 21-23, introduces a new publication requirement of a breach using the term "MAJOR PRINT OR BROADCAST MEDIA IN GEOGRAPHIC AREAS WHERE THE INDIVIDUALS AFFECTED BY THE BREACH LIKELY RESIDE." MAMIC respectfully submits that compliance with this new standard would be difficult, if not impossible.

Finally, MAMIC notes that SB 112, at page 7, line 16, requires the notice to describe a breach, "INCLUDING WHEN AND HOW IT OCCURRED." This new requirement not only raises the question of adequate compliance with the statutory language, it also introduces the likelihood that a MAMIC member, in attempting to comply, may have to reveal confidential information regarding its security systems. In other words, the notice itself could further jeopardize the security of the entity.

For these and other reasons, MAMIC respectfully requests an unfavorable report on SB 112.

Very truly yours,

Bryson F. Popham

cc: Members of the Senate Finance Committee

SB 112_T.ROWE PRICE_info.pdf
Uploaded by: Smith, Sarah Joan
Position: INFO

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)

February 10, 2021

The Honorable Delores G. Kelley
The Honorable Susan Lee
3 East, Miller Senate Office Building
Annapolis, MD 21401

RE: Senate Bill 112 - Commercial Law - Personal Information Protection Act – Revisions – Letter of Information

Dear Chair Kelley and Members of the Senate Finance Committee,

I am writing this letter of information on behalf of my client, T. Rowe Price Group, Inc. We have met with Committee Counsel and wish to share our comments on certain provisions of Senate Bill 112 with the Committee.

Our chief concerns with this legislation are as follows:

- On page 6, in lines 7-15, the current thresholds to have the option to give substitute notice of a breach have been removed. Under these requirements in current law, to give substitute notice a business either demonstrates that the cost of the notice would exceed $100,000 or that the class of individuals to be notified exceed 175,000, or there is insufficient contact information to give actual notice.

  While we believe the above existing statutory model has worked, the new language at lines 13-15 on page 6 would add substitute-like notice provisions (e.g., website, media, email) even when actual notice to impacted individuals has been given by letter, email (for those who have already consented to electronic notices), or phone. This will create confusion for those already notified by letter, for example, and worry for those who have not been impacted at all but see a website or media notice.

  If the General Assembly determines that a change to the current model is necessary, it could simply remove the $100,000/175,000 individual standard in lines 8-10 on page 6, and retain substitute notice for situations where there is insufficient contact information for actual notice.

- On page 5, at line 25, shortening the notice period from 30 to 7 days in impracticable. As an example, if a law enforcement agency makes a determination a day or two in advance of a holiday, such as Christmas or New Years, issuing a notification in a 7 day period would be extremely difficult. It is highly likely that information from law enforcement relating to the closing of the investigation will impact the contents of the letter to impacted individuals and to the Maryland Attorney General. We recommend retaining the 30-day period or making a modest adjustment to it.

- On page 6, at line 22, there is new language requiring extensive notification through the media in areas where the individuals affected are likely to reside. There should be a limitation in this language to the State of Maryland.

- On page 5, at line 2, the notice period has been shortened from 45 days to 10 days. Again, this is impracticable for compliance purposes. Although the period should be longer, a possible compromise could be where the business sends two notifications: one notification directly to impacted individuals under Subsection (b) of

Section 14-3504, and one notification to the owner or licensee of the personal information under paragraph (1) of Section 14-3504(c) at the same time. Again, the preference would be to retain the current 45 day notice period.

On behalf of T. Rowe Price we respectfully offer these comments and suggestions for the consideration of the Committee as it deliberates Senate Bill 112.

Very truly yours,

Bryson F. Popham

cc: Members of the Senate Finance Committee
Patrick Carlson