



MAURA HEALEY
ATTORNEY GENERAL

THE COMMONWEALTH OF MASSACHUSETTS OFFICE OF THE ATTORNEY GENERAL

ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

TEL: (617) 727-2200
www.mass.gov/ago

March 17, 2015

The Honorable Michael C. Burgess M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, & Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20215

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, & Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20215

Re: *The Data Security and Breach Notification Act of 2015*

Dear Chairman Burgess and Ranking Member Schakowsky:

We write to address the discussion draft bill entitled the Data Security and Breach Notification Act of 2015 (the "Bill"), dated March 12, 2015, which seeks to establish federal standards concerning data security and data breach notification obligations. We appreciate that the Committee recognizes the importance of strong data security protections and breach disclosure obligations to protect consumers and preserve consumer confidence in the market. Moreover, we are cognizant of the business community's concerns regarding compliance with myriad state security breach notification regimes.

Nonetheless, we write to express serious reservations with the Bill, which in our view represents an unnecessary retraction of existing protections for consumers at a time when such protections are imperative. Our concerns are informed by this Office's experience enforcing Massachusetts' data security breach notification law (Mass. Gen. Law ch. 93H, attached as Exhibit 1), data security regulations (Title 201 of the Code of Massachusetts Regulations ("CMR"), section 17.00 *et seq.*, attached as Exhibit 2), and data disposal law (Mass. Gen. Law ch. 93I, attached as Exhibit 3). Together, these laws and regulations – which are enforced by this Office through the Massachusetts Consumer Protection Act¹ – require entities that own or license "personal information"² of Massachusetts residents to develop, implement, and maintain

¹ Mass Gen. Law ch. 93A.

² In Massachusetts, "personal information" is defined by statute to mean a resident's first name and last name, or first initial and last name, in combination with any one or more of the following data elements: (a) social security

minimum security procedures and policies consistent with industry standards to safeguard such information (whether in paper or electronic form) from anticipated threats or hazards and from unauthorized access or use.³ Massachusetts law also obligates entities to provide prompt notice to affected residents and state agencies in the event of a breach of security or compromise of that information.⁴ These laws and regulations protect consumers from identity theft and fraud, and concomitantly, instill consumer confidence in the commercial collection and use of their personal information.

From January 1, 2008 through July 31, 2014, this Office received notice pursuant to Mass. Gen. Law ch. 93H, section 3 of over 8,665 security breaches, affecting nearly 5 million Massachusetts residents. To the extent any of those breaches resulted in enforcement actions by this Office (a very small percentage), the circumstances reflected gross failures to implement or maintain basic security practices, unreasonable delays in providing notice of the breach, or other egregious conduct that raised real risks of resulting consumer harm. As a result, this Office has an informed and comprehensive view into the nature, extent, and frequency of data breaches, the risks faced by consumers, and the security practices and procedures that can prevent or mitigate those risks.

Accordingly, this Office is uniquely positioned to highlight some of the potential problems with the Bill. Our principal concerns are as follows:

I. The Bill's proposed preemption of state law undercuts existing consumer protections and is overly broad.

Although the stated purpose of the Bill is to “protect consumers from identity theft, economic loss or economic harm, and financial fraud,” the Bill would preempt Massachusetts’ data security/breach law to the extent they relate to data in electronic form, and replace it with weaker protections. In addition, the Bill would preempt other state laws that protect “data in electronic form” from unauthorized access (including, among others, laws that criminalize the interception of wire communications (Mass Gen. Law c. 272, § 99(C)) or require the confidentiality of medical records and mental health records (Mass Gen. Law c. 111, § 70E(b), and c. 123, § 36)). It is also in conflict with, and would appear to potentially preempt, the enforcement authority given to the States under other federal laws relating to the security of electronic data (including, for example, the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 1320d–5(d))). Such sweeping preemption is harmful to consumers, and restricts innovative States from responding to and protecting their residents from emerging threats to the privacy and security of their data. The Bill should at least preserve the current level of protections enjoyed by consumers and the enforcement powers of the state Attorneys General to avoid a national downward harmonization of security and breach standards, and an associated drop in consumer confidence in the marketplace. The Bill will not only fail to

number; or (b) driver’s license number or state-issued identification card number; or (c) financial account number or credit or debit card number, with or without any required security code. See Mass Gen. Law ch. 93H, §1.

³ See Mass Gen. Law ch. 93I and 201 CMR 17.00 *et seq.*

⁴ See Mass Gen. Law ch. 93H.

maintain consumer confidence in the marketplace, but will scale back the protections consumers currently enjoy.

II. Minimum data security standards are important and necessary, but the proposed standards leave consumers' data vulnerable.

We agree that establishing minimum data security standards is important and necessary. Massachusetts has had robust minimum data security regulations in place since 2010 in the form of data security regulations (201 CMR 17.00 *et seq.*) and data disposal law (Mass Gen. Law ch. 93I). The flexible standards established by Massachusetts represent the leading information security framework in the nation, and are the standards to which all commercial entities aspire.⁵ We are concerned the Bill will lower the bar already set by Massachusetts and other existing federal data security regulations,⁶ and will weaken consumers' confidence in the security of their personal information in commerce. Specifically, the Bill fails to articulate the minimum data security standards that would constitute the required "reasonable security measures and practices." As a result, the Bill would result in the retroactive establishment of data security standards through protracted litigation and piecemeal judicial interpretation. To ensure that the data security obligations are sufficiently robust, defined, and responsive to changing threats and technologies, the Bill should establish minimum data security standards, modeled after those in place in Massachusetts and under existing federal law.

III. The Bill fails to require notice that will ensure meaningful enforcement.

While the Bill's requirement of notice of a breach to the Federal Trade Commission is an important first step for enforcement of the Bill's requirements, it is not by itself enough. Recent breaches reported in the media underscore the necessary role played by the state Attorneys General in enforcing data breach and data security requirements. The absence of a requirement to provide notice to state Attorneys General of data breaches – even for those breaches that impact a significant number of their residents – frustrates their ability to protect their residents. Further, the threshold for providing notice to the FTC may be set too high. In Massachusetts, the vast majority (approximately 97%) of the 2,314 data breaches reported in 2013 involved fewer than 10,000 persons; each of these breaches affected, on average, 74 persons. Assuming these statistics are consistent nationally, the Bill would create an enforcement "blind spot" for both

⁵ Similar to existing federal standards applicable to financial institutions (*see* 16 C.F.R. Part 314) and entities covered under HIPAA (*see e.g.* 45 CFR Subpart C of Part 164), Massachusetts requires entities to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information (201 CMR 17.03(2)(b)); develop, implement and maintain a "written comprehensive information security program" containing physical, administrative and technical safeguards necessary to protect personal information from those risks (201 CMR 17.03); take reasonable steps to oversee third parties handling personal information (201 CMR 17.03(2)(f)); and securely dispose of personal information (Mass Gen. Law ch. 93I). Cognizant of the particular risks associated with electronic data, Massachusetts also requires entities, among other things, to establish and maintain a technically-feasible computer security system (201 CMR 17.04); and to encrypt personal information sent over public networks or wirelessly, or stored on laptops and portable devices (201 CMR 17.04(3), (5)).

⁶ *See, e.g.*, 16 C.F.R. Part 314 (Standards for Safeguarding Customer Information); 45 CFR Subpart C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information); 16 CFR Part 682 (Proper Disposal of Consumer Information); and 201 CMR 17.00 *et seq.* (Standards for the Protection of Personal Information of Residents of the Commonwealth).

state and federal regulators, who would not receive notice of the vast majority of data breaches that occur. To ensure effective enforcement of the Bill, the Bill should require prompt notice of breaches to the FTC and also to the state Attorneys General in cases where their State's residents are impacted.

IV. The Bill infringes on the States' consumer protection enforcement authority.

While the Bill gives the state Attorneys General the option of bringing a civil action as *parens patriae* in U.S. district court, it requires the State to first notify the FTC, and to abstain from that action if the FTC initiates the action first. Such requirements infringe on the enforcement prerogatives of the state Attorneys General by injecting unnecessary delay and costs, and unnecessarily complicating their efforts to enforce their respective consumer protection laws. Numerous federal laws illustrate that dual federal/state enforcement coordination of consumer protection laws is both possible and effective, including for example: the Federal Trade Commission Act (15 U.S.C. § 45(a)(1) and its numerous State counterparts (*see, e.g.* Mass Gen. Law ch. 93A), the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), the Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) and the Health Information Technology for Clinical and Economic Health (HITECH) Act (42 U.S.C. § 17930 *et seq.*). To ensure meaningful protections for consumers, the Bill should likewise establish a dual federal/state enforcement framework that respects – not constricts – the enforcement prerogative of the States.

V. The penalties proposed by the Bill are insufficient, and leave consumers without a remedy.

The Bill limits the state Attorneys General to civil penalties of up to \$11,000 for each day per violation of the Bill's information security requirements, and up to \$11,000 per violation of the Bill's breach notice requirements, capped at a total liability of \$2.5 million, and based on "penalty factors" that do not expressly take into account consumer harm or the need to deter future violations. Given the massive scope of recently-reported breaches affecting some of the largest companies in the country, a civil penalty cap of \$2.5 million may be an insufficient deterrent, and could be treated as a cost of doing business. Moreover, the Bill does not authorize the state Attorneys General to recover consumer restitution, and further does not provide for a private cause of action. Thus, a consumer who suffers loss due to a data breach effectively has no remedy under this Bill. The Bill should instead retain the existing discretion of state Attorneys General and the FTC to seek both civil penalties and consumer restitution at levels sufficient to penalize and deter the conduct at issue and make consumers whole, and further provide a private right of action.

VI. The Bill's data breach notice obligations lack many key safeguards.

Requiring prompt notice to consumers affected by a breach and to state regulators serves important ends, including alerting consumers to the fact that their personal information may be at risk, educating the market as to existing or emerging security threats, and providing incentives for improving security practices to prevent breaches. The data breach notice standards proposed by the Bill fall short for a number of reasons.

First, the Bill allows entities to delay notice without regard to the risks faced by consumers. By requiring notice only when the entity both “discovers” a “breach of security” and “determines” that a “reasonable risk of” identity theft, economic loss or harm, or financial fraud has resulted or will result, the Bill creates a disincentive for an entity to monitor their systems for potential compromises or vulnerabilities, an outcome directly at odds with the Bill’s stated purposes. Once “discovered,” the Bill would further grant a covered entity an unspecified (and unlimited) period of time to “tak[e] the necessary measures” to “determine the scope of the breach of security and restore the reasonable integrity, security, and confidentiality” of its data system. This creates opportunities for delay that would undermine the force of the proposed thirty (30) day notification deadline, and which may subject consumers to unnecessary risk. If preventing identity theft is the goal, notice should be issued in time for consumers to protect themselves, even if the breached entity has not completed its investigation or is still in the process of restoring its systems.

Second, the Bill fails to require notice in cases where identity theft is a real risk, such as when personal information is accessed or acquired with authorization (*e.g.* by an authorized employee) but used for unauthorized purposes. Additionally, the Bill does not provide for notice in cases where encrypted personal information – and information allowing for the decryption of that information – are both compromised in the breach.

Third, because notice obligation under the Bill turns on the manner in which a covered entity deals with the personal information, rather than its legal relationship to it,⁷ notice could be delayed or avoided as a result of disputes between covered entities as to which is the “third-party entity” and which is the covered entity responsible for notice. It may also result in consumer confusion insofar as consumers may receive notice from an entity with which they have not had direct dealings. To avoid such results, the Bill should follow Massachusetts’ lead and impose the consumer notification duty on the entity that “owns or licenses” the breached personal information. In turn, entities that “maintain or store” the breached personal information should be obligated to promptly notify the owner or licensor. *See* Mass Gen. Law ch. 93H, §§ 3(a), (b).

Finally, the content and form of the required consumer notice lacks several key safeguards. The Bill does not require the notice to contain information as to how a consumer may protect him or herself and instead, directs the consumer to the FTC for more information. The Bill should require the consumer notice to contain the information necessary for the consumer to protect him/herself from identity theft.⁸ In cases where “substitute notice” is

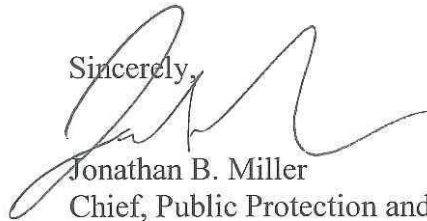
⁷ The Bill imposes the consumer notice obligation on “a covered entity that uses, accesses, transmits, stores, disposes of, or collects” personal information (section 3(a)(1)), but not on the covered entity that “store[s], processe[s], or maintain[s]” personal information” for a covered entity. This “third-party entity” would “ha[ve] no other notification obligations” than to notify the covered entity for whom it stores, processes, or maintains the personal information (section 3(b)(1)(A)).

⁸ Such information should include, for example, information concerning the availability of security freezes, the importance of filing and obtaining a police report (information required under Mass Gen. Law ch. 93H, § 3), the availability of fraud alerts, the importance of monitoring one’s credit reports, and other information about the breach that would allow the consumer to fairly assess their risk and protect themselves.

authorized, the entity should be required to make a media posting sufficient to constitute legal notice of the breach.⁹

We appreciate this opportunity to convey our serious concerns regarding the Bill to the Subcommittee. Please do not hesitate to contact us for any additional detail, clarity or with questions you may have. We are happy to provide you with any information you may need or to share with you our experience gained from working with businesses, reviewing security breach notifications, and enforcing our laws.

Sincerely,



Jonathan B. Miller
Chief, Public Protection and Advocacy Bureau

Sara Cable
Assistant Attorney General
Consumer Protection Division

Office of Attorney General Maura Healey
Commonwealth of Massachusetts
One Ashburton Place
Boston, MA 02108
(617) 727-2200

⁹ See, e.g. Mass Gen. Law ch. 93H, § 1 (requiring as one component of substitute notice “publication in or broadcast through media or medium that provides notice throughout the commonwealth [of Massachusetts]”).