

THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL

ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

MAURA HEALEY
ATTORNEY GENERAL

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

April 15, 2015

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 Ranking Member Schakowsky:

Thank you for your questions regarding certain provisions of *The Data Security and Breach Notification Act of 2015* (H.R. ___) (March 20, 2015 Discussion Draft) (the "Bill"). We appreciate the opportunity to respond to them, and hope our responses are helpful to the Committee as it considers the Bill.

- 1. What are the potential implications of the Bill's preemption clause (section 6(a)) with regard to the States' and, specifically, Massachusetts' ability to "maintain, enforce, or impose or continue in effect" laws, regulations, or standards relating to the security of data in electronic form and/or notification following a breach of security?***

Section 6(a) of the Bill restricts the States from "adopt[ing], maintain[ing], enforc[ing], or impos[ing] or continu[ing] in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law relating to or with respect to the security of data in electronic form or notification following a breach of security." Read in a manner consistent with the stated purpose of the Bill – to "establish[] strong and uniform data security and breach notification standards for electronic data in interstate commerce" (Bill, § 1(b)) – Section 6(a) preempts the States from enforcing or enacting data security standards (such as Title 201 of the Code of Massachusetts Regulations, section 17.00 *et seq.* ("201 CMR 17.00") or breach notification laws (such as Mass. Gen. Law ch. 93H)).

The scope of Section 6(a), however, goes far beyond the stated purpose of the Bill. Because of the breadth of Section 6(a), it could be asserted in an attempt to preempt – or at best, complicate or discourage – States' efforts to enforce existing civil or criminal laws or even enact

new laws necessary to protect its citizens or address purely local concerns, to the extent such laws are even tangentially related to data security, privacy or breach notification.

For example, Section 6(a) could be asserted by entities engaged in unfair or deceptive trade practices to thwart a civil law enforcement action by a state Attorney General under state consumer protection law (*e.g.*, Mass. Gen. Law ch. 93A), where such practices arguably “relat[e] to . . . the security of data in electronic form.” Such practices could include, for example, solicitations in the form of false or misleading data breach notices that fraudulently induce consumers to pay for unnecessary or illusory fraud protection services or data security services, or to disclose even further personal information. With the increasing threat and ever-evolving nature of data security risks, state consumer protection laws provide vital flexibility and a vehicle by which the States can rapidly and effectively respond to protect their consumers. As drafted, Section 6(a) could present a legal hurdle complicating, unnecessarily delaying, and potentially blocking the States from enforcing their consumer protection laws to protect their consumers.

Additionally, insofar as Section 6(a) would restrict a State from “continu[ing] in effect any . . . duty, requirement, standard, or other provision having the force and effect of law relating to or with respect to the security of data in electronic form or notification following a breach of security,” it could complicate a state Attorney General’s ability to enforce consumer protections obtained through prior enforcement efforts or established by prior judicial precedent. For example, a state Attorney General may face challenges enforcing compliance with data security protections required by prior judgments (or by an “Assurance of Discontinuance” or “Assurance of Voluntary Compliance” accepted by an Attorney General in lieu of initiating a civil action). Additionally, the data security standards established by such judgments and Assurances would lose their normative force. Further, the phrase “duty, requirement, standard, or other provision having the force and effect of law” could be interpreted to abolish state judicial precedents under either specific state data security or breach laws or even state common law.¹ As a result, the Bill could leave both public and private parties with little choice but to “start over” and establish new case law altogether through protracted and expensive legal action, which is not in the best interest of consumers or businesses.

Moreover, in attempting to preempt the entire field “relating to or with respect to the security of data in electronic form or notification following a breach of security,” the reach of Section 6(a) could extend to laws that impose no data security or breach notice standard, but which arguably still “relat[e] to” data security or breach notification. For example, Section 6(a) could be asserted by a criminal defendant against charges of unauthorized access to a computer system² or the interception of wire communications.³ It could also reach and potentially preempt

¹ Although Section 6(b) (which is still under debate by the Subcommittee) purports to clarify that the preemption “section shall not exempt a covered entity from liability under common law,” it is inherently inconsistent with the language of Section 6(a), which prohibits a State from enforcing any “rule . . . duty, requirement, [or] standard . . . having the force and effect of law,” a phrase that appears to refer to and encompass common law. Bill, §6 (a), (b).

² *See* Mass. Gen. Law ch. 266, § 120F (“Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both. The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.”).

laws meant to protect medical records and mental health records from unauthorized access (*see, e.g.*, Mass Gen. Law ch. 111, § 70E(b), and ch. 123, § 36). Indeed, Section 6(a) could even be read to divest enforcement authority specifically given to the States under other federal laws relating to data security, including, for example, the “Security Standards for the Protection of Electronic Protected Health Information” (45 C.F.R. Subpart C of Part 164), which are enforceable by the States under the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 1320d–5(d)).

Finally, by prohibiting a State from “adopt[ing] ... any law ... [or] regulation ... relating to or with respect to the security of data in electronic form,” Section 6(a) would have a chilling effect on innovation and adaptation by state legislatures and policy-makers in responding to data security and privacy threats. New laws or regulations to prevent or penalize identity theft or that address security concerns that arise from future technologies, for example, could arguably be subject to a preemption challenge under Section 6(a) because they “relate to the security of data in electronic form.” Legislative agility and regulatory rule-making is especially important in the field of data security, where new technologies and changing notions of privacy and security may raise data security risks impossible to foresee or which cannot be addressed by this Bill. Section 6(a) essentially “freezes” data security and breach notification standards in time without regard to future, unforeseen risks.

2. How is the breadth of the preemption language in Sections 6(a) and 6(b) of the discussion draft harmful to consumers?

Articulated, minimum data security standards are imperative to safeguard the privacy and security of consumers’ personal information. It is equally important that such standards be flexible and responsive to changing risks and technologies. The Bill, however, divests the States of their authority to establish or enforce any existing data security laws or regulations (*e.g.* 201 CMR 17.00), and imposes in their place the requirement that a covered entity “implement and maintain reasonable security measures and practices.” Bill, § 2. As we have previously stated, in the absence of specifically defined regulatory guidance (*e.g.*, from the Federal Trade Commission (“FTC”)), this amorphous standard is too vague to achieve the Bill’s stated goal of “protect[ing] consumers from identity theft, economic loss or economic harm, and financial fraud.” Bill, § 1(b).

Data breaches are an ever-present and increasing threat for companies of all sizes and from all industries. Massachusetts’ experience enforcing its data security regulations (201 CMR 17.00) shows that while some breaches reported to this Office in 2014 appear to have resulted from intentional, criminal acts, many resulted from the improper disposal of consumers’ information, lost files, disclosure through inadvertence, carelessness, or the failure to follow basic and well-accepted data security practices and procedures. Our enforcement experience suggests even those data breaches resulting from intentional criminal attacks could have been

³ *See* Mass. Gen. Law ch. 272, § 99(C) (“any person who— willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment”).

avoided or mitigated if the entity had complied with its own data security policies or employed basic security practices such as software updates or firewalls. In an era of rising data breach risks,⁴ the need for strong and enforceable minimum data security standards is imperative.

Unfortunately, the data security standard set forth in Section 2 of the Bill is weaker than the state laws (including Massachusetts') the Bill would preempt, and as measured against other federal regimes.⁵ Specifically, because the Bill fails to define or enumerate any of the required "reasonable security measures and practices," or provide any regulatory agency with rule-making authority to do so, it would force covered entities to guess what constitutes such "reasonable security measures and practices," risking a downward harmonization towards the least expensive (and likely least effective) measures and practices. The resulting litigation to establish data security standards by judicial interpretation will not keep pace with evolving technology and security threats, and will expose consumers' sensitive personal information to unnecessary risk.

Finally, because Section 6 does not provide for recovery of consumer restitution, and because Section 4(c) prohibits a private right of action by a consumer, a consumer would not be able to seek compensation for the financial consequences of a data breach. This prohibition, together with the inability of a state Attorney General to recover restitution for injured consumers under the Bill, will result in victimized consumers effectively being left without remedy. Such an outcome is directly contrary to the stated purpose of the Bill to "protect consumers from identity theft, economic loss or economic harm, and financial fraud." Bill, § 1(b).

3. How are the enforcement powers conferred to the state Attorneys General under Section 4(b) of the Discussion Draft insufficient to maintain even current levels of state enforcement?

Although Section 4(b) of the Bill grants enforcement authority to the States, various other provisions of the proposed Bill undercut the States' ability to effectively exercise it. Most significantly, the Bill does not require notice of a security breach to any regulator – state or federal – in the event fewer than 10,000 consumers are affected and, then, only requires notice to

⁴ Since September 1, 2007, through December 31, 2014, this Office has received notice of over 9,800 breaches, reporting over 5 million impacted Massachusetts residents, with 2,409 breaches reported in 2014 alone (a 33% increase over 2012, and over a 527% increase over 2008).

⁵ Similar to existing federal standards applicable to financial institutions (see 16 C.F.R. Part 314 ((Standards for Safeguarding Customer Information)) and entities covered under HIPAA (see e.g. 45 CFR Subpart C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information)), 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)).

the FTC. Bill, § 3(a)(3). Currently under the Massachusetts Data Breach Notification Act (Mass. Gen. Law ch. 93H), this Office must receive notice of any data breach impacting one or more Massachusetts residents. These notices provide this Office with essential insight into emerging data security threats and enable this Office to ensure that consumers are promptly and appropriately notified.⁶ Under the Bill, this Office would receive no notices – even when a breach impacts a significant number of Massachusetts residents, or only Massachusetts residents. Even if the FTC were to share with the States the notices it receives under the Bill, a threshold of 10,000 consumers is too high to enable the States to effectively protect its residents.⁷ As a result, the Bill would create a significant enforcement “blind spot” to smaller-scale breaches, even where the breaches resulted from unreasonable data security practices and where consumers remain subject to unnecessary and avoidable risks.

Other provisions of Section 4(b) would unnecessarily complicate and burden the States’ efforts to enforce the requirements of the Bill. A State would have to bring an enforcement action in federal court, provide prior notice to the FTC, and abstain in the event the FTC initiated an action first. Such limits subject each State to unnecessary expense and potential delay while consumers’ personal information potentially remains at risk. Additionally, Section 4(b) restricts the remedies a State may pursue, capping civil penalties at \$2,500,000 per event⁸ without regard to the extent of consumer harm, and preventing the State from seeking restitution on behalf of injured consumers. These significant obstacles, coupled with Section 4(c)’s explicit prohibition of any private right of action, will not only impede state enforcement but also leave consumers without any meaningful remedy or protection in the event their personal information is compromised by a breach of security.

* * *

We appreciate this opportunity to convey to the Subcommittee our serious concerns regarding the effectiveness of the Bill to meet its intended purpose to protect consumers from data security breaches. As you can see, where the Bill may have intended to set a common floor of national consumer protections, it also sets a ceiling in States where laws currently provide greater consumer protections than the Bill would provide. Please do not hesitate to contact us for additional detail or clarity, or with questions you may have. We are happy to provide you with

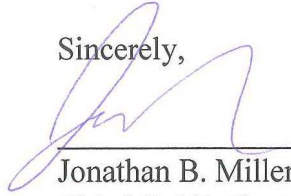
⁶ While this Office investigates only a small fraction of the data breaches about which it receives notice, those notices also allow this Office to effectively monitor to ensure that consumers’ personal information is appropriately protected from breach.

⁷ In Massachusetts, fewer than 3% of the breaches reported in 2013 met that threshold. Each of those breaches impacted, on average, 74 Massachusetts residents.

⁸ As this Office previously stated, this cap may be an insufficient deterrent, and could be treated as cost of doing business. In light of even limited history, this figure is too low and would constitute Congress’ encouraging businesses to underinvest in consumer protections. Prior data security settlements have involved much higher monetary penalties, including the \$9.75 million monetary payment by the TJX Companies to settle a 41-state multistate investigation regarding a 2007 data breach that put the personal information of over 45 million consumers at risk. *See In re: The TJX Companies, Inc.*, Case No. 09-2602 (Mass. Sup. Ct. June 28, 2009).

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