THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

MAURA HEALEY
ATTORNEY GENERAL

(617) 727-2200
(617) 727-4765 TTY
www.mass.gov/ago

May 14, 2015

The Honorable Jeb Hensarling
Chairman
The Committee on Financial Services
U.S. House of Representatives
Washington, DC 20215

The Honorable Maxine Waters
Ranking Member
The Committee on Financial Services
U.S. House of Representatives
Washington, DC 20215

Re: *Federal Legislation Relating to Data Security and Breach Notification Standards*

Dear Chairman Hensarling and Ranking Member Waters:

We write concerning the Committee's upcoming hearing, entitled "Protecting Consumers: Financial Data Security in the Age of Computer Hackers." We are encouraged and appreciate that the Committee recognizes the critical importance of this issue. In this era of increasing data breach risks, strong data security protections and breach disclosure requirements are essential to protect consumers and to preserve confidence in the market.

We understand that one issue before this Committee is whether federal data security and breach notification standards are warranted. We are cognizant of the business community's concerns regarding compliance with multiple state security breach notification regimes. As it considers this issue, we urge the Committee to carefully balance the calls for a national standard with the necessary protections consumers currently rely upon under state law, to avoid invalidating those critical protections and leaving consumers in a vulnerable position.

In particular, we write to share with the Committee the insights and perspective this Office has gained through its enforcement of Massachusetts' data security breach notification law,[1] data security regulations,[2] and data disposal law.[3] Together, these laws (enforced by this Office through the Massachusetts Consumer Protection Act)[4] require covered entities to develop, implement, and maintain minimum data security procedures and policies, consistent with

[1] Mass. Gen. Laws ch. 93H, attached as Exhibit 1.

[2] Title 201 of the Code of Massachusetts Regulations ("CMR"), section 17.00 *et seq.*, attached as Exhibit 2.

[3] Mass. Gen. Laws ch. 93I, attached as Exhibit 3.

[4] Mass Gen. Laws ch. 93A.

industry standards, to safeguard Massachusetts consumers' "personal information"[5] (whether in paper or electronic form) from anticipated threats or hazards and from unauthorized access or use.[6] Massachusetts data breach notice law also obligates entities to provide notice as soon as reasonably practicable, and without unreasonable delay, to affected residents and state agencies in the event of a breach of security or compromise of that information.[7]

From September 1, 2007 through December 31, 2014, this Office received notice of over 9,800 data breaches, reporting over 5 million impacted Massachusetts residents. Over 2,400 breaches were reported in 2014 alone (a 33% increase over 2012 and a 527% increase over 2008). 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. More commonly, this Office engages in regular outreach with the business community to improve data security practices and facilitate compliance with those laws. As a result of this work, this Office has an informed and comprehensive view into the nature, extent, and frequency of data breaches, the challenges businesses encounter, the risks faced by consumers and, most importantly, the security practices and procedures that can prevent or mitigate those risks.

Our experience reflects that data breaches are an ever-present and increasing threat for companies and consumers alike, that strong data security and data breach notification standards are essential, and that the States need to retain the ability to protect their consumers from these rapidly-evolving risks. In particular, we believe that any effective data security and breach notification framework should include the following features.

- **Federal Law Should Establish a "Floor," not a "Ceiling," of Consumer Protections.**

We appreciate the calls for a uniform, federal standard for data security and breach notice. But any such federal standard should not dilute or preempt protections already in place in many States, including Massachusetts. In order to raise the level of protection nationally, to enable the States to innovate to best protect the needs of their residents, and to avoid enacting a stagnant security and breach standard that fails to keep up with changing technologies, a federal standard should set a "floor" of protections that state law can exceed. To the extent Congress intends to preempt state law in this field, it should set standards that are at least as strong – or stronger – than the protections consumers currently rely upon in their states. Finally, the scope of any federal preemption should be narrowly and carefully drawn to avoid: preempting state laws in areas other than data security or breach notification, infringing on the States' consumer protection laws or enforcement authority, or preventing the States from continuing to innovate to protect their consumers from the rapidly evolving data security and privacy risks.

---

[5] 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 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. Laws ch. 93H, §1.

[6] *See* Mass Gen. Laws ch. 93I and 201 CMR 17.00 *et seq.*

[7] *See* Mass Gen. Laws ch. 93H.

- **Federal Law Should Preserve and Respect the States' Enforcement Authority.**

Recent breaches reported in the media underscore the necessary role played by the state Attorneys General in enforcing data breach and data security requirements for the protection of consumers. Indeed, in enforcing Massachusetts data security and breach notification law over the past several years, this Office has developed specialized expertise in the highly technical and rapidly evolving field of data security, and an informed perspective on the causes and effects of data breaches and the data security practices that can best avoid or mitigate them. The offices of many other state Attorneys General have developed a similar expertise and perspective. To harness this collective expertise, and to ensure that state Attorneys General can continue their role of protecting their consumers, any federal standard should preserve the States' existing enforcement authority, and in particular, with respect to the following areas.

First, prompt notice of breaches to the relevant state Attorneys General in cases where their State's residents are impacted is imperative. If threshold numbers of affected consumers are set for state regulator notice, they should not be so high that it frustrates a State's ability to enforce the law with respect to the vast majority of breaches that impact its residents. For example, in Massachusetts, approximately 97% of the 2,314 data breaches reported in 2013 involved fewer than 10,000 persons; in fact, each of these breaches affected, on average, 74 persons. Thus, thresholds requiring notice to state regulators that exceed 100 residents of that State would thus frustrate this Office's ability to protect Massachusetts residents.

Second, a dual federal/state enforcement framework that respects – not constricts – the enforcement prerogatives of the States should be utilized. Provisions that give exclusive enforcement authority to federal agencies, restrict state Attorneys General to suits in federal courts or create new enforcement mechanisms or procedures risk injecting unnecessary delay, costs and complications for the States. Numerous federal laws illustrate that parallel or dual federal/state enforcement coordination of consumer protection laws is both possible and effective.[8]

Third, to protect their consumers, state Attorneys General must be able to seek adequate civil remedies, including where appropriate preliminary and permanent injunctive relief to compel compliance, civil penalties to deter misconduct, attorneys' fees/costs, and restitution for ascertainable losses suffered by consumers (remedies currently obtainable by this Office under the Massachusetts Consumer Protection Act). If "caps" on civil penalties are set, they should be meaningful enough to deter future misconduct, so as to not be treated as a cost of doing business. Moreover, because consumers are the ultimate victims of data breaches, they should retain the ability to bring private rights of action to seek recovery of damages or harm they may suffer.

[8] *See, e.g.*, the Federal Trade Commission Act (15 U.S.C. § 45(a)(1) and its numerous State counterparts (*see, e.g.* Mass Gen. Laws ch. 93A), the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), and the Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) and Health Information Technology for Clinical and Economic Health (HITECH) Act (42 U.S.C. § 17930 *et seq*.).

- **Federal Law Should Enhance – Or At Least Preserve – Existing State and Federal Standards.**

State consumer protection and data security/breach notice laws provide important protections for consumers. As the Committee considers a national standard, it should build on these existing protections under federal and state law to ensure consumers are not exposed to increased risks as a result of a new national standard. In this vein, we urge the Committee to consider the following.

  - **Data Security Standards Under Massachusetts and Federal Law Should Be Preserved.**

Massachusetts' data security regulations (201 CMR 17.00 *et seq.*) and its data disposal law (Mass Gen. Laws ch. 93I) represent one of the leading information security frameworks in the nation. Rather than employ a "one-size-fits-all" approach or an undefined, generalized standard of "reasonableness," Massachusetts utilizes a risk-based, process-oriented approach to data security, similar to well-established federal standards governing financial institutions and certain health-related entities.[9] Covered entities must develop, implement, and maintain a written security program outlining administrative, technological, and physical safeguards appropriate for the entity's size, scope of business, amount of resources available to it, the nature and quantity of data collected or stored, and the need for security of the personal information it handles. Within this flexible framework, the regulations outline various categories of security measures and practices that constitute a "reasonable" information security program.

We believe that consumers will be best protected by a federal data security standard that is at least as comprehensive and strong as the Massachusetts data security regulations. Indeed, our review of thousands of breach notifications underscores the need for strong and enforceable data security standards. While some breaches result from intentional, criminal acts, many result from the failure to employ basic security practices, such as through the improper disposal of consumers' information, lost files, disclosure through inadvertence, carelessness, or the failure to follow basic and well-accepted data security practices. Often even those breaches resulting from intentional criminal attacks could reasonably have been 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.

[9] 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. Laws 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)).

A strong, generally-applicable standard would bolster the overall security of consumer data in commerce (and with it, consumer confidence), reduce the costs and burdens of responding to a data breach, and eliminate any potential competitive disadvantages created by differing, sector-specific standards. Further, the data security standard should not be so minimal so as to create a competitive disadvantage to those businesses that choose to invest in more robust, and more costly, data security measures in recognition of the inadequate protections resulting from such a minimal standard. To ensure that the law is responsive to changing technologies and risks, the Committee should consider giving rule-making authority to the Federal Trade Commission to define as appropriate those security measures and practices that are considered "reasonable."

- **Definitions of Protected Consumer Information Should Be Broad and Flexible, Not Narrow and Static.**

In today's data-driven economy, consumers share a variety of highly personal data points with numerous commercial entities. This information includes not just authenticating information that can lead directly to identity theft or fraud (such as biometric data, social security numbers, and drivers' license numbers), but various other types of information that can be used to access financial accounts, perpetrate medical or tax identity theft or fraud, or cause emotional distress or physical harm against a consumer. This may include, for example, financial account numbers, online account log-in credentials (and/or the secret question and answers necessary to access those credentials), geolocation information, details about a consumer's mental and physical health, personal habits, hobbies, shopping activity, political views, or religious beliefs. Such information can be used to identify a given consumer, obtain highly personal details about them, predict their future actions, and thus more convincingly impersonate them, or cause harm against them.

To encompass the various categories of information that can be used to impersonate or cause harm to a consumer and the changing nature of identity theft, the Commission should take this opportunity to adopt a broad and flexible statutory definition of protected "personal information," and not be limited to existing federal or state statutory definitions. The Committee should further consider giving the Federal Trade Commission ("FTC") rule-making authority to amend the definition of protected personal information as necessary to ensure it remains responsive to changing information practices and technologies.

- **Consumers Must Be Promptly Notified of a Breach.**

If preventing identity theft is the goal of a federal data breach notice standard, requiring timely notice of the breach to the consumer should be the first priority. Timely notice to the consumer may reduce the risk of resulting economic and noneconomic damages by enabling the consumer to take preemptive protective measures (such as by monitoring their credit reports and financial account records, placing security freezes or fraud alerts on their credit, and being on alert for identity theft or fraud). Conversely, delayed notice could increase the risk of both economic and non-economic harm by unduly shortening or eliminating the window of opportunity for such prophylactic steps.

Additionally, standards that require consumer notice only after the breached entity determines that there is a risk of financial harm to the consumer (so-called "financial harm triggers") are problematic in at least three respects. First, connecting any specific breach to financial harm can be a difficult and time consuming process, and may not be possible depending on the circumstances of a particular breach. Second, allowing the company to conduct a risk assessment deprives the consumer of the ability to make their own determination of their own risk, and may prevent them from taking steps to mitigate that risk. Third, financial harm triggers fail to take into account non-financial harms that can occur, such as medical identity theft, professional or personal embarrassment, or loss of access to online accounts or services. A federal standard should instead require breach notification as soon as reasonably practicable and without unreasonable delay when an entity knows, or has reason to know, that protected personal information of a consumer has been acquired without authorization, or used for unauthorized purposes.

***

We applaud the Committee for tackling this difficult but critical issue, and appreciate the opportunity to share our expertise. We are happy to provide you with any information you may need and to share with you our experience gained from working with businesses, reviewing security breach notifications, and enforcing our laws. Please do not hesitate to contact us with questions you may have about the points raised above, or about this issue in general.

Sincerely,

/s/ Jonathan B. Miller
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