



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](http://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 Act<sup>1</sup> – require entities that own or license "personal information"<sup>2</sup> of Massachusetts residents to develop, implement, and maintain

---

<sup>1</sup> Mass Gen. Law ch. 93A.

<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup> 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.

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

<sup>4</sup> *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.<sup>5</sup> We are concerned the Bill will lower the bar already set by Massachusetts and other existing federal data security regulations,<sup>6</sup> 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

---

<sup>5</sup> 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)).

<sup>6</sup> *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,<sup>7</sup> 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.<sup>8</sup> In cases where “substitute notice” is

---

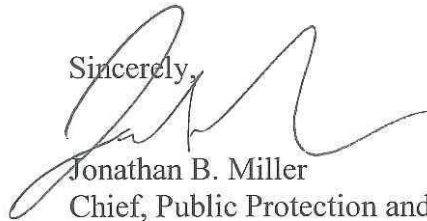
<sup>7</sup> The Bill imposes the consumer notice obligation on “a covered entity that uses, accesses, transmits, stores, disposes of, or collects” personal information (section 3(a)(1)), but not on the covered entity that “store[s], processe[s], or maintain[s]” personal information” for a covered entity. 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)).

<sup>8</sup> 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.<sup>9</sup>

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

---

<sup>9</sup> 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]”).

# EXHIBIT 1

Massachusetts General Laws Annotated  
Part I. Administration of the Government (Ch. 1-182)  
Title XV. Regulation of Trade (Ch. 93-110h)  
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 1

§ 1. Definitions

Effective: October 31, 2007

[Currentness](#)

(a) As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:--

“Agency”, any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.

“Breach of security”, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

“Data” any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

“Electronic”, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

“Encrypted” transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation.

“Notice” shall include:--

(i) written notice;

(ii) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in [§ 7001 \(c\) of Title 15 of the United States Code](#); and chapter 110G; or

(iii) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed \$250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

“Person”, a natural person, corporation, association, partnership or other legal entity.



“Personal information” a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

(a) Social Security number;

(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, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that “Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

“Substitute notice”, shall consist of all of the following:--

(i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents;

(ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and

(iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth.

(b) The department of consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of “encrypted”, as used in this chapter, to reflect applicable technological advancements.

#### **Credits**

Added by [St.2007, c. 82, § 16, eff. Oct. 31, 2007](#).

#### [Notes of Decisions \(1\)](#)

M.G.L.A. 93H § 1, MA ST 93H § 1

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

Massachusetts General Laws Annotated  
Part I. Administration of the Government (Ch. 1-182)  
Title XV. Regulation of Trade (Ch. 93-110h)  
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 2

§ 2. Regulations to safeguard personal information of commonwealth residents

Effective: October 31, 2007

[Currentness](#)

(a) The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.

(b) The supervisor of records, with the advice and consent of the information technology division to the extent of its jurisdiction to set information technology standards under [paragraph \(d\) of section 4A of chapter 7](#), shall establish rules or regulations designed to safeguard the personal information of residents of the commonwealth that is owned or licensed. Such rules or regulations shall be applicable to: (1) executive offices and any agencies, departments, boards, commissions and instrumentalities within an executive office; and (2) any authority created by the General Court, and the rules and regulations shall take into account the size, scope and type of services provided thereby, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

(c) The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor shall adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

**Credits**

Added by [St.2007, c. 82, § 16, eff. Oct. 31, 2007](#).



[Notes of Decisions \(1\)](#)

M.G.L.A. 93H § 2, MA ST 93H § 2

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Massachusetts General Laws Annotated

Part I. Administration of the Government (Ch. 1-182)

Title XV. Regulation of Trade (Ch. 93-110h)

Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 3

§ 3. Duty to report known security breach or unauthorized use of personal information

Effective: October 31, 2007

[Currentness](#)

(a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use. (b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(c) <sup>1</sup> If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or



use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.

**Credits**

Added by [St.2007, c. 82, § 16, eff. Oct. 31, 2007](#).

[Notes of Decisions \(1\)](#)

**Footnotes**

[1](#) So in original.

M.G.L.A. 93H § 3, MA ST 93H § 3

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

Massachusetts General Laws Annotated  
Part I. Administration of the Government (Ch. 1-182)  
Title XV. Regulation of Trade (Ch. 93-110h)  
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 4

§ 4. Delay in notice when notice would impede criminal investigation; cooperation with law enforcement

Effective: October 31, 2007

[Currentness](#)

Notwithstanding section 3, notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The person or agency shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.

**Credits**

Added by [St.2007, c. 82, § 16, eff. Oct. 31, 2007](#).

[Notes of Decisions \(1\)](#)

M.G.L.A. 93H § 4, MA ST 93H § 4

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.



Massachusetts General Laws Annotated

Part I. Administration of the Government (Ch. 1-182)

Title XV. Regulation of Trade (Ch. 93-110h)

Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 5

§ 5. Applicability of other state and federal laws

Effective: October 31, 2007

[Currentness](#)

This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information; provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach. The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided further that if said person or agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter.

**Credits**

Added by [St.2007, c. 82, § 16, eff. Oct. 31, 2007](#).

M.G.L.A. 93H § 5, MA ST 93H § 5

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Massachusetts General Laws Annotated  
Part I. Administration of the Government (Ch. 1-182)  
Title XV. Regulation of Trade (Ch. 93-110h)  
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 6

§ 6. Enforcement of chapter

Effective: October 31, 2007

[Currentness](#)

The attorney general may bring an action pursuant to [section 4 of chapter 93A](#) against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

**Credits**

Added by [St.2007, c. 82, § 16, eff. Oct. 31, 2007](#).

M.G.L.A. 93H § 6, MA ST 93H § 6

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

# EXHIBIT 2



Code of Massachusetts Regulations Currentness

Title 201: Office of Consumer Affairs and Business Regulation

Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth  
(Refs & Annos)

201 CMR 17.01

17.01: Purpose and Scope

(1) Purpose. 201 CMR 17.00 implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. 201 CMR 17.00 establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of 201 CMR 17.00 is to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope. 201 CMR 17.00 applies to all persons that own or license personal information about a resident of the Commonwealth.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.01, 201 MA ADC 17.01

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

**Code of Massachusetts Regulations Currentness****Title 201: Office of Consumer Affairs and Business Regulation****Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth  
(Refs & Annos)****201 CMR 17.02****17.02: Definitions**

The following words as used in 201 CMR 17.00 shall, unless the context requires otherwise, have the following meanings:

Breach of Security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or Licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal Information, a Massachusetts 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 that relate to such resident:

- (a) Social Security number;
- (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, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service Provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to 201 CMR 17.00.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.02, 201 MA ADC 17.02

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.



Code of Massachusetts Regulations Currentness

Title 201: Office of Consumer Affairs and Business Regulation

Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth  
(Refs & Annos)

201 CMR 17.03

17.03: Duty to Protect and Standards for Protecting Personal Information

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

- (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
- (b) the amount of resources available to such person;
- (c) the amount of stored data; and
- (d) the need for security and confidentiality of both consumer and employee information.

The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

- (a) Designating one or more employees to maintain the comprehensive information security program;
- (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
  - 1. ongoing employee (including temporary and contract employee) training;
  - 2. employee compliance with policies and procedures; and
  - 3. means for detecting and preventing security system failures.
- (c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
- (d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with 201 CMR 17.00 and any applicable federal regulations; and

2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 201 CMR 17.03(2)(f)2. even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.03, 201 MA ADC 17.03

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Code of Massachusetts Regulations Currentness

Title 201: Office of Consumer Affairs and Business Regulation

Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth  
(Refs & Annos)

201 CMR 17.04

17.04: Computer System Security Requirements

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

(1) Secure user authentication protocols including:

- (a) control of user IDs and other identifiers;
- (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- (d) restricting access to active users and active user accounts only; and
- (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that:

- (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
- (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices;



(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.04, 201 MA ADC 17.04

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Code of Massachusetts Regulations Currentness

Title 201: Office of Consumer Affairs and Business Regulation

Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth  
(Refs & Annos)

201 CMR 17.05

17.05: Compliance Deadline

(1) Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.05, 201 MA ADC 17.05

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

# EXHIBIT 3



Massachusetts General Laws Annotated

Part I. Administration of the Government (Ch. 1-182)

Title XV. Regulation of Trade (Ch. 93-110h)

Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)

M.G.L.A. 93I § 1

§ 1. Definitions

Effective: February 3, 2008

[Currentness](#)

As used in this chapter the following words shall, unless the context clearly requires otherwise, have the following meanings:--

“Agency”, any county, city, town, or constitutional office or any agency thereof, including but not limited to, any department, division, bureau, board, commission or committee thereof, or any authority created by the general court to serve a public purpose, having either statewide or local jurisdiction.

“Data subject”, an individual to whom personal information refers.

“Person”, a natural person, corporation, association, partnership or other legal entity.

“Personal information”, a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident:--

(a) Social Security number;

(b) driver's license number or Massachusetts identification card number;

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; or

(d) a biometric indicator.

**Credits**

Added by [St.2007, c. 82, § 17, eff. Feb. 3, 2008](#).

M.G.L.A. 93I § 1, MA ST 93I § 1

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

Massachusetts General Laws Annotated

Part I. Administration of the Government (Ch. 1-182)

Title XV. Regulation of Trade (Ch. 93-110h)

Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)

M.G.L.A. 93I § 2

§ 2. Standards for disposal of records containing personal information; disposal by third party; enforcement

Effective: February 3, 2008

[Currentness](#)

When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than \$100 per data subject affected, provided said fine shall not exceed \$50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.

**Credits**

Added by [St.2007, c. 82, § 17, eff. Feb. 3, 2008](#).

M.G.L.A. 93I § 2, MA ST 93I § 2

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

Massachusetts General Laws Annotated

Part I. Administration of the Government (Ch. 1-182)

Title XV. Regulation of Trade (Ch. 93-110h)

Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)

M.G.L.A. 93I § 3

§ 3. Enforcement

Effective: February 3, 2008

[Currentness](#)

The attorney general may bring an action pursuant to [section 4 of chapter 93A](#) against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

**Credits**

Added by [St.2007, c. 82, § 17, eff. Feb. 3, 2008](#).

M.G.L.A. 93I § 3, MA ST 93I § 3

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.