

PART I. ADMINISTRATION OF THE GOVERNMENT

TITLE XV. REGULATION OF TRADE

CHAPTER 93H. SECURITY BREACHES

[Chapter 93H added by 2007, 82, Sec. 16 effective October 31, 2007.]

Chapter 93H: Section 1. Definitions

[Text of section added by 2007, 82, Sec. 16 effective October 31, 2007.]

Section 1. (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.

CHAPTER 93H. SECURITY BREACHES

[Chapter 93H added by 2007, 82, Sec. 16 effective October 31, 2007.]

Chapter 93H: Section 2. Regulations to safeguard personal information of commonwealth residents

[Text of section added by 2007, 82, Sec. 16 effective October 31, 2007.]

Section 2. (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.

CHAPTER 93H. SECURITY BREACHES

[Chapter 93H added by 2007, 82, Sec. 16 effective October 31, 2007.]

Chapter 93H: Section 3. Duty to report known security breach or unauthorized use of personal information

[Text of section added by 2007, 82, Sec. 16 effective October 31, 2007.]

Section 3. (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) 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.

CHAPTER 93H. SECURITY BREACHES

[Chapter 93H added by 2007, 82, Sec. 16 effective October 31, 2007.]

Chapter 93H: Section 4. Delay in notice when notice would impede criminal investigation; cooperation with law enforcement

[Text of section added by 2007, 82, Sec. 16 effective October 31, 2007.]

Section 4. 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.

[Chapter 93H added by 2007, 82, Sec. 16 effective October 31, 2007.]

Chapter 93H: Section 5. Applicability of other state and federal laws

[Text of section added by 2007, 82, Sec. 16 effective October 31, 2007.]

Section 5. 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.

[Chapter 93H added by 2007, 82, Sec. 16 effective October 31, 2007.]

Chapter 93H: Section 6. Enforcement of chapter

[Text of section added by 2007, 82, Sec. 16 effective October 31, 2007.]

Section 6. 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.