

Bill: HB4144 of 2007-2008 session

Date: 07/12/2007 10:30am

COMMONWEALTH OF MASSACHUSETTS, 2007
AUTHOR: CONFERENCE COMMITTEE
HB4144

An Act Relative to the Protection of Personal Information

SECTION 1. Chapter 66 of the General Laws is hereby amended by inserting after section 8A the following section:-

Section 8B. Records or documents required to be destroyed or disposed of in this chapter shall be destroyed or disposed of in the manner set forth in chapter 93I.

SECTION 2. Section 2 of said chapter 66A, as appearing in the 2006 Official Edition, is hereby amended by inserting after the word "fire", in line 32, the following words:-
, identity theft.

SECTION 3. Section 50 of chapter 93 of the General Laws, as so appearing, is hereby amended by inserting after the definition of "Firm offer of credit" the following definition:-

"Identity theft report", a report that alleges a violation of section 37E of chapter 266, 18 United States Code, section 1028, or a similar statute in any other jurisdiction, or a copy of a report filed by a consumer with an appropriate federal, state or local law enforcement agency, and the filing of which subjects the person filing the report to criminal penalties pursuant to section 6713 of chapter 266 or section 13A of chapter 269.

SECTION 4. Said section 50 of said chapter 93, as so appearing, is hereby further amended by inserting after the definition of "Investigative consumer report" the following definition:-

"Lift", to suspend a security freeze for the purpose of releasing a consumer's credit information to a specific party or for a specified period of time, as authorized by the consumer.

SECTION 5. Said section 50 of said chapter 93 of the General Laws, as so appearing, is hereby further amended by inserting after the definition of "Medical information" the following definition:-

"Password" or "Personal identification number", a unique and random number or a unique and random combination of numbers, letters or symbols, which shall not contain a consumer's social security number or any sequence of 3 or more numbers of a consumer's social security number, or other personal identifying information.

SECTION 6. Said section 50 of said chapter 93 of the General Laws, as so appearing, is hereby further amended by inserting after the definition of "Prescreening" the following 3 definitions:-

"Proper identification", information sufficient to identify a person, which shall include, but not be limited to, name, address, social security number and date of birth. Such information shall not include information concerning the consumer's employment and personal or family history unless the consumer is unable to reasonably identify himself with the information described in the preceding sentence.

"Remove", to permanently terminate a security freeze.

"Security freeze", a notice placed on a person's consumer report by a consumer reporting agency, at the request of the consumer and subject to certain exceptions, which prohibits the consumer reporting agency from releasing the report or any information derived therefrom without the express authorization of the consumer.

SECTION 7. Section 55 of said chapter 93, as so appearing, is hereby amended by striking out, in line 1, the words "the provisions of section fifty-one" and inserting in place thereof the following words:- sections 51 and 62A.

SECTION 8. The second subparagraph of subsection (b) of section 56 of said chapter 93, as so appearing, is hereby amended by striking out the first sentence and inserting in place thereof the following 2 sentences:- You have a right to dispute inaccurate information by contacting the consumer reporting agency directly, either in writing or by telephone. The consumer reporting agency shall provide, upon request and without unreasonable delay, a live representative of the consumer reporting agency to assist in dispute resolution whenever possible and practicable, or to the extent consistent with federal law.

SECTION 9. The last paragraph of said subsection (b) of said section 56 of said chapter 93, as so appearing, is hereby amended by striking out the last sentence and inserting in place thereof the following sentence:- You may be entitled to collect compensation, in certain circumstances, if you are damaged by a person's negligent or intentional failure to comply with the credit reporting act.

SECTION 10. Said subsection (b), of said section 56 of said chapter 93, as so appearing, is hereby further amended by adding the following 4 subparagraphs:-

You have a right to request a "security freeze" on your consumer report. The security freeze will prohibit a consumer reporting agency from releasing any information in your consumer report without your express authorization. A security freeze shall be requested by sending a request either by certified mail, overnight mail or regular stamped mail to a consumer reporting agency, or as authorized by regulation. The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. You should be aware that using a security freeze may delay, interfere with, or prevent the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transactions, or other services, including an extension of credit at point of sale.

When you place a security freeze on your consumer report within 5 business days of receiving your request for a security freeze, the consumer reporting agency shall provide you with a personal identification number or password to use if you choose to remove the freeze on your consumer report or to authorize the release of your consumer report to a specific party or for a specified period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide the following:

- (1) the personal identification number or password provided by the consumer reporting agency;
- (2) proper identification to verify your identity; and
- (3) the third party or parties who are to receive the consumer report or the specified period of time for which the report shall be available to authorized users of the consumer report.

A consumer reporting agency that receives a request from a consumer to lift a freeze on a consumer report shall comply with the request not later than 3 business days after receiving the request.

A security freeze shall not apply to a person or entity, or to its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information relative to your consumer report for the purposes of reviewing or collecting the account, if you have previously given consent to the use of your consumer report "Reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements."

SECTION 11. Said chapter 93, as so appearing, is hereby further amended by inserting after section 62 the following section:-

Section 62A. If a consumer requests a security freeze, the consumer reporting agency shall disclose to the consumer the process of placing, removing and lifting a security freeze. A consumer reporting agency shall require proper identification of the person making a request to place, lift or remove a security freeze.

A consumer may request that a security freeze be placed on his consumer report by sending a request to a consumer reporting agency by certified mail, overnight mail or regular stamped mail to an address designated by the consumer reporting agency to receive such requests, or by a method otherwise permitted by regulation. If a security freeze is in place, the information from a consumer report shall not be released to a third party without prior express authorization from the consumer. This section

shall not prohibit a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer report.

A consumer reporting agency shall place a security freeze on a consumer report not later than 3 business days after receiving a request from the consumer. The consumer reporting agency shall send a written confirmation of the security freeze to the consumer within 5 business days after receiving the request and shall provide the consumer with a unique personal identification number or a unique password, or both, to be used by the consumer for the purpose of providing authorization for the removal or lifting of the security freeze.

If the consumer wishes to lift a security freeze that is in place, he shall contact the consumer reporting agency, request that the freeze be lifted, and provide proper identification, the personal identification number or password, or both, provided by the consumer reporting agency, and the third party who is to receive the consumer report or the specified period of time for which the report shall be available to authorized users of the consumer report.

A consumer reporting agency that receives a request from a consumer to lift a security freeze on a consumer report pursuant to this chapter shall comply with the request as soon as practicable and without unreasonable delay, but under no circumstances not later than 3 business days after receiving the request.

A security freeze shall remain in place until the consumer requests that the security freeze be lifted or removed in accordance with this section; provided, however, that a consumer reporting agency may remove a security freeze if the consumer report was frozen due to a material misrepresentation of fact. If a consumer reporting agency intends to remove a freeze on a consumer report due to a material misrepresentation of fact by the consumer, the consumer reporting agency shall notify the consumer in writing 5 business days prior to removing the freeze on the consumer report.

While a security freeze is in place, a consumer reporting agency shall not change any of the following official information in a consumer report without sending a written confirmation of the change to the consumer within 30 days of the change being posted to the consumer report: name, date of birth, social security number, and address. Written confirmation shall not be required for technical modifications of information contained in a consumer report, including name and street abbreviations, complete spellings, or transposition of numbers or letters. In the case of an address change, the written confirmation shall be sent to both the new address and to the former address.

If a third party requests access to a consumer report on which a security freeze is in effect, and this request is submitted in connection with an application for credit or any other use, and the consumer does not allow his or her consumer report to be accessed for that specific party or for that specified period of time, the third party shall treat the application as incomplete.

A consumer reporting agency shall remove a security freeze within 3 business days of receiving a request for removal from a consumer who provides both proper identification and the personal identification number or password provided by the consumer reporting agency pursuant to this section.

This section shall not apply to the use of a consumer report by any of the following:

- 1) a person or agent thereof, or an assignee of a financial obligation owing by the consumer to such person or agent thereof, or a prospective assignee of a financial obligation owing by the consumer to that person or agent thereof in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had, prior to assignment, an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract or negotiable instrument. For purposes of this paragraph, "reviewing the account" shall include activities related to account maintenance, monitoring, credit line increases and account upgrades and enhancements; or access to said account by a subsidiary, affiliate, agent, assignee or prospective assignee of a person, or agent thereof, to whom access has been granted for purposes of facilitating the extension of credit or other permissible use;
- 2) any federal, state or local agency, law enforcement agency, or trial court acting pursuant to a court order, warrant or subpoena;
- 3) the Massachusetts child support agency under Title IV-D of the Social Security Act, 42 U.S.C. et seq;
- 4) the executive office of health and human services or its agents or assigns acting to investigate Medicaid fraud;

5) the department of revenue or its agents or assigns acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of its other statutory responsibilities;

6) a person using credit information for the purposes of prescreening as provided for by the federal Fair Credit Reporting Act;

7) any person administering a credit file monitoring subscription service to which the consumer has subscribed;

8) any person acting solely for the purpose of providing a consumer with a copy of his consumer report upon the consumer's request; or

9) to the extent otherwise allowed by statute, any property and casualty insurer licensed by the commonwealth for use in rating or underwriting insurance policies.

Nothing in this chapter shall prevent a consumer reporting agency from charging a reasonable fee, not to exceed \$5, to a consumer who elects to freeze, lift or remove a freeze to a consumer report, except that a consumer reporting agency shall not charge a fee to a victim of identity theft or his spouse, provided that the victim has submitted a valid police report relating to the identity theft to the consumer reporting agency.

The following persons shall not be required to place a security freeze on a consumer report:

1) a check services or fraud prevention services company, which issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers or similar methods of payments;

2) a deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or similar negative information regarding a consumer, to inquiring banks or other financial institutions for use only in reviewing a consumer request for a demand deposit account at the inquiring bank; or

3) a consumer reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the database of another consumer reporting agency or multiple consumer reporting agencies, and does not maintain a permanent database of credit information from which new consumer reports are produced, except that such financial institution or consumer reporting agency shall be subject to any security freeze placed on a consumer report by another consumer reporting agency from which it obtains information.

Notwithstanding any general or special law to the contrary, the director of consumer affairs and business regulation, in consultation with the secretary of housing and economic development, shall promulgate rules and regulations for the purpose of expediting the methods of requesting, lifting and removing security freezes through technological advancements, consistent with this section and designed to benefit consumers.

SECTION 12. Section 58 of said chapter 93, as so appearing, is hereby amended by inserting after the word "writing", in line 17, the following words:- , but shall provide consumers with the option of speaking with a live representative at any time during the dispute resolution process, whenever possible and practicable or to the extent consistent with federal law.

SECTION 13 Said section 58 of said chapter 93, as so appearing, is hereby further amended by adding the following paragraph:-

(j) At any time during the dispute process described in this section, the consumer shall have the right to request to speak to a live representative from the consumer reporting agency in an attempt to resolve the dispute. The consumer reporting agency shall maintain a toll-free telephone number available to consumers for such purpose and shall notify consumers of its availability whenever possible and practicable or to the extent consistent with federal law".

SECTION 14. Section 63 of said chapter 93, as so appearing, is hereby amended by striking out, in line 4, the words "fifty to sixty-two" and inserting in place thereof the following figures:- 50 to 62A.

SECTION 15. Section 64 of said chapter 93, as so appearing, is hereby amended by striking out, in line 4, the words "fifty to sixty-two", and inserting in place thereof the following figures:- 50 to 62A.

SECTION 16. The General Laws are hereby further amended by inserting after chapter 93G the following 2 chapters:-

CHAPTER 93H SECURITY BREACHES

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 of the General Laws; 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. drivers 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; however.

"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; and

(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 state.

(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.

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 division of public records 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.

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.

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.

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.

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.

CHAPTER 93I. DISPOSITION AND DESTRUCTION OF RECORDS.

Section 1. 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.

Section 2. 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.

Section 3. 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.

SECTION 17. Section 37E of chapter 266 of the General Laws, as appearing in the 2006 Official Edition, is hereby amended by adding the following subsection:-

(f) A law enforcement officer shall accept a police incident report from a victim and shall provide a copy to such victim, if requested, within 24 hours. Such police incident reports may be filed in any county where a victim resides, or in any county where the owner or license holder of personal information stores or maintains said personal information, the owner or license holder's principal place of business or any county in which the breach of security occurred, in whole or in part.

SECTION 18. Chapter 93I of the General Laws, inserted by section 16 of this act, shall take effect as of February 3, 2008.