HOUSE DOCKET, NO. 3350 FILED ON: 1/20/2017

HOUSE . . . . . No. 2813

The Commonwealth of Massachusetts

PRESENTED BY:

James M. Cantwell

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act relative to the security of personal financial information.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
James M. Cantwell	*4th Plymouth*
Thomas J. Calter	*12th Plymouth*
Josh S. Cutler	*6th Plymouth*
Michael S. Day	*31st Middlesex*

HOUSE DOCKET, NO. 3350 FILED ON: 1/20/2017

HOUSE . . . . . No. 2813

By Mr. Cantwell of Marshfield, a petition (accompanied by bill, House, No. 2813) of James M. Cantwell and others relative to the security of personal financial information. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

In the One Hundred and Ninetieth General Court
(2017-2018)

An Act relative to the security of personal financial information.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1: Section 1 of chapter 93H as appearing in the 2016 Official Edition, is hereby amended by striking out said section and inserting in place thereof the following section:-

Section 1. (a) As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:

"Access device", a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information which includes, but is not limited to, a credit card, debit card, or stored value card.

“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 an identifiable risk of identity theft or fraud. 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.

"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.

"Financial institution", any office of a trust company, commercial bank, industrial loan company, savings bank, savings and loan association, cooperative bank or credit union chartered by the commonwealth or by another state of the United States, the District of Columbia, the commonwealth of Puerto Rico, a territory of possession of the United States, or a country other than the United States, or a national banking association, federal savings and loan association, federal savings bank or federal credit union.

"Information security program", the administrative, technical, or physical safeguards that a covered entity uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

"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;

(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) biometric indicator of the consumer used to gain access to financial accounts of the consumer; 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.

"Service provider", a person or entity that stores, processes, or transmits access device data on behalf of another person or entity.

“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.

SECTION 2. Section 2 of said chapter 93H is hereby further amended by striking out the first paragraph and inserting in place thereof the following paragraphs:-

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 require a person subject to this chapter to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are reasonably designed to (1) ensure the security and confidentiality of personal information of residents of the commonwealth, (2) protect against any anticipated threats or hazards to the security or integrity of such information;

and (3) protect against unauthorized acquisition of such information that could result in substantial harm to the individuals to whom such information relates.

The regulations shall require a person subject to this chapter to (1) designate an employee or employees to coordinate the information security program, (2) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of sensitive financial account information and sensitive personal information and assess the sufficiency of any safeguards in place to control these risks, including consideration of risks in each relevant area of the covered entity's operations, (3) design and implement information safeguards to control the risks identified in its risk assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures, and (4) oversee third-party service providers by taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate safeguards for personal information and requiring third-party service providers by contract to implement and maintain such safeguards.

A person shall be deemed to be in compliance with this chapter if it is subject to 15 U.S.C. 6801, 42 U.S.C. 1320d–2, or 42 U.S.C. 17932 and 17937 and the regulations promulgated under these sections.

SECTION 3: Section 3 of said chapter 93H is hereby further amended by striking out the third paragraph and inserting in place thereof the following paragraph:- 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.