SENATE DOCKET, NO. 12 FILED ON: 1/9/2017

SENATE . . . . . No. 149

The Commonwealth of Massachusetts

PRESENTED BY:

Michael J. Rodrigues

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:
Michael J. Rodrigues	*First Bristol and Plymouth*

SENATE DOCKET, NO. 12 FILED ON: 1/9/2017

SENATE . . . . . No. 149

By Mr. Rodrigues, a petition (accompanied by bill, Senate, No. 149) of Michael J. Rodrigues for legislation relative to the security of personal financial information. Consumer Protection and Professional Licensure.

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE SENATE, NO. *184* OF 2015-2016.]

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 2012 official Edition, is hereby amended by striking out said section and inserting in place thereof the following 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.

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

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

19 "Card security code", the three-digit or four-digit value printed on an access device or
20 contained in the microprocessor chip or magnetic stripe of an access device which is used to
21 validate access device information during the authorization process.

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

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

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

30 "Financial institution", any office of a trust company, commercial bank, industrial loan
31 company, savings bank, savings and loan association, cooperative bank or credit union chartered
32 by the commonwealth or by another state of the United States, the District of Columbia, the
33 commonwealthof Puerto Rico, an territory of possession of the United States, or a country other
34 than the United States, or a national banking association, federal savings and loan association,
35 federal savings bank or federal credit union which has its main office located in the
36 commonwealth or in any other jurisdiction named hearing or a regulated lender.

37 “Magnetic stripe data", the data contained in the magnetic stripe of an access device.

38 “Microprocessor chip data", the data contained in the microprocessor chip of an access
39 device.

40 “Notice”, shall include:—

41 (i) written notice;

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

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

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

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

52 (a) Social Security number;

53 (b) driver’s license number or state-issued identification card number; or

54 (c) financial account number, or credit or debit card number, with or without any required
55 security code, access code, personal identification number or password, that would permit access
56 to a resident’s financial account; provided, however, that “Personal information” shall not
57 include information that is lawfully obtained from publicly available information, or from
58 federal, state or local government records lawfully made available to the general public.

59 "PIN", a personal identification code that identifies the cardholder.

60 "PIN verification code number", the data used to verify cardholder identity when a PIN is
61 used in a transaction.

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

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

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

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

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

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

74 SECTION 2. Section 3 of said chapter 93H is hereby further amended by striking out the
75 third paragraph and inserting in place thereof the following paragraph:-

76 The notice to be provided to the resident shall include, but not be limited to, the
77 consumer's right to obtain a police report, how a consumer requests a security freeze and the
78 necessary information to be provided when requesting the security freeze, and any fees required
79 to be paid to any of the consumer reporting agencies.

80 SECTION 3. Sections 5 and 6 of chapter 93H are hereby repealed and replaced with the
81 following sections:-

82 Section 5:-No person or entity conducting business in Massachusetts that accepts an
83 access device in connection with a transaction shall retain the card security code data, the PIN
84 verification code number, or the full contents of any track of magnetic stripe data, subsequent to
85 the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48
86 hours after authorization of the transaction. A person or entity is in violation of this section if its
87 service provider retains such data subsequent to the authorization of the transaction or in the case
88 of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

89 Section 6:- Whenever there is a breach of the security of the system of a person or entity
90 that has violated this section, or that person's or entity's service provider, that person or entity
91 shall reimburse the financial institution that issued any access devices affected by the breach for
92 the costs of reasonable actions undertaken by the financial institution as a result of the breach in
93 order to protect the information of its cardholders or to continue to provide services to
94 cardholders, including but not limited to, any cost incurred in connection with:

95 (1) the cancellation or reissuance of any access device affected by the breach;

96 (2) the closure of any deposit, transaction, share draft, or other accounts affected by the
97 breach and any action to stop payments or block transactions with respect to the accounts;

98 (3) the opening or reopening of any deposit, transaction, share draft, or other accounts
99 affected by the breach;

100 (4) any refund or credit made to a cardholder to cover the cost of any unauthorized
101 transaction relating to the breach; and

102 (5) the notification of cardholders affected by the breach.

103 The financial institution is also entitled to recover costs for damages paid by the financial
104 institution to cardholders injured by a breach of the security of the system of a person or entity
105 that has violated this section. Costs do not include any amounts recovered from a credit card
106 company by a financial institution. The remedies under this subdivision are cumulative and do
107 not restrict any other right or remedy otherwise available to the financial institution.

108 Section 7:- This chapter does not relieve a person or agency from the duty to comply with
109 requirements of any applicable general or special law or federal law regarding the protection and

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

122 Section 8: The attorney general may bring an action pursuant to section 4 of chapter 93A
123 against a person or otherwise to remedy violations of this chapter and for other relief that may be
124 appropriate.