

SENATE No. 545

The Commonwealth of Massachusetts

PRESENTED BY:

Anthony W. Petruccelli

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:

Anthony W. Petruccelli

First Suffolk and Middlesex

William M. Straus

10th Bristol

SENATE No. 545

By Mr. Petruccelli, a petition (accompanied by bill, Senate, No. 545) of Anthony W. Petruccelli and William M. Straus for legislation relative to the security of personal financial information. Financial Services.

The Commonwealth of Massachusetts

**In the One Hundred and Eighty-Ninth General Court
(2015-2016)**

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:

1 SECTION 1: Section 1 of chapter 93H as appearing in the 2012 official Edition, is hereby
2 amended by striking out said section and inserting in place thereof the following section:—

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

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

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

10 “Breach of security”, the unauthorized acquisition or unauthorized use of unencrypted
11 data or, encrypted electronic data and the confidential process or key that is capable of

12 compromising the security, confidentiality, or integrity of personal information, maintained by a
13 person or agency that creates an identifiable risk of identity theft or fraud. A good faith but
14 unauthorized acquisition of personal information by a person or agency, or employee or agent
15 thereof, for the lawful purposes of such person or agency, is not a breach of security unless the
16 personal information is used in an unauthorized manner or subject to further unauthorized
17 disclosure.

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

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

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

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

29 “Financial institution”, any office of a trust company, commercial bank, industrial loan
30 company, savings bank, savings and loan association, cooperative bank or credit union chartered
31 by the commonwealth or by another state of the United States, the District of Columbia, the
32 commonwealth of Puerto Rico, a territory of possession of the United States, or a country other

33 than the United States, or a national banking association, federal savings and loan association,
34 federal savings bank or federal credit union.

35 “Magnetic stripe data”, the data contained in the magnetic stripe of an access device.

36 “Microprocessor chip data”, the data contained in the microprocessor chip of an access
37 device.

38 “Notice”, shall include:

39 (i) written notice;

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

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

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

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

50 (a) Social Security number;

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

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

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

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

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

62 "Substitute notice", shall consist of all of the following:

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

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

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

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

72 SECTION 2: Section 3 of said chapter 93H is hereby further amended by striking out the
73 third paragraph and inserting in place thereof the following paragraph:–

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

78 SECTION 3: Said chapter 93H is hereby further amended by striking out sections 5 and 6
79 and inserting in place thereof the following 6 sections:–

80 Section 5. No person or entity conducting business in Massachusetts that accepts an
81 access device in connection with a transaction shall retain, or otherwise permit its retention of,
82 the card security code data, the PIN verification code number, or the full contents of any track of
83 magnetic stripe data or microprocessor chip data, subsequent to the authorization of the
84 transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of
85 the transaction. A person or entity is in violation of this section if such data remains in its
86 possession, or the possession of its service provider, intentionally or unintentionally, subsequent
87 to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48
88 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 Section 5 herein, or a breach of the security of the system of that person's or
91 entity's service provider, that person or entity shall be liable, without a showing of fault, to the
92 financial institution that issued any access devices affected by the data breach for all resulting
93 damages, including, but not limited to, the costs of reasonable actions undertaken by the

94 financial institution as a result of the breach in order to protect the information of its cardholders
95 or to continue to provide services to cardholders, including but not limited to, any cost incurred
96 in connection with:

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

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

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

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

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

105 Section 7. Any person or entity conducting business in Massachusetts that accepts an
106 access device in connection with a transaction shall take reasonable action to secure, at all times,
107 the card security code data, the PIN verification code number, and the full contents of any track
108 of magnetic stripe data or microprocessor chip data. Whenever there is a breach of the security of
109 the system of a person or entity that has failed to take such reasonable action required by this
110 section, that person or entity shall be liable to any financial institution that issued any access
111 devices affected by the data breach for all resulting damages including, but not limited to, all
112 damages set forth in Section 6 herein.

113 Section 8. Any financial institution suffering damages set forth in Sections 6 and 7 may
114 recover such damages in an action at law instituted in any court of competent jurisdiction. Such

115 damages shall not include, and are to be offset by, any amounts recovered from a credit card
116 company by a financial institution, as a result of the relevant data breach. The remedies
117 hereunder are cumulative and do not restrict any other right or remedy otherwise available to the
118 financial institution.

119 Section 9. This chapter does not relieve a person or agency from the duty to comply with
120 requirements of any applicable general or special law or federal law regarding the protection and
121 privacy of personal information; provided however, a person who maintains procedures for
122 responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or
123 guidelines, is deemed to be in compliance with this chapter if the person notifies affected
124 Massachusetts residents in accordance with the maintained or required procedures when a breach
125 occurs; provided further that the person also notifies the attorney general and the director of the
126 office of consumer affairs and business regulation of the breach as soon as practicable and
127 without unreasonable delay following the breach. The notice to be provided to the attorney
128 general and the director of the office of consumer affairs and business regulation shall consist of,
129 but not be limited to, any steps the person or agency has taken or plans to take relating to the
130 breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided
131 further that if said person or agency does not comply with applicable federal laws, rules,
132 regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter.

133 Section 10. The attorney general may bring an action pursuant to section 4 of chapter
134 93A against a person or otherwise to remedy violations of this chapter and for other relief that
135 may be appropriate.

136