

HOUSE No. 213

By Mr. Costello of Newburyport, petition of Michael A. Costello relative to enhancing the confidentiality and protection of certain consumer information. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

In the Year Two Thousand and Seven.

AN ACT RELATIVE TO ENHANCING THE CONFIDENTIALITY AND PROTECTION OF CERTAIN CONSUMER 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 The General Laws are hereby amended by inserting after
2 chapter 66A the following chapter:—

3 **Chapter 66B.**

4 **Personal Data Protection.**

5 Section 1. As used in this chapter, the following words shall
6 have the following meanings unless the context clearly requires
7 otherwise:

8 (1) “Breach of the security of the system” means the unautho-
9 rized acquisition of unencrypted computerized data that compro-
10 mises the security, confidentiality, or integrity of personal
11 information maintained by an individual or a commercial entity.
12 Good faith acquisition of personal information by an employee or
13 agent of an individual or a commercial entity for the purposes of
14 the individual or the commercial entity is not a breach of the secu-
15 rity of the system, provided that the personal information is not
16 used or subject to further unauthorized disclosure;

17 (2) “Commercial entity” includes corporations, business trusts,
18 estates, trusts, partnerships, limited partnerships, limited liability
19 partnerships, limited liability companies, associations, organiza-

20 tions, joint ventures, governments, governmental subdivisions,
21 agencies, or instrumentalities, or any other legal entity, whether
22 for profit or not-for-profit;

23 (3) “Notice” means:

24 a. Written notice;

25 b. Telephonic notice;

26 c. Electronic notice, if the notice provided is consistent with the
27 provisions regarding electronic records and signatures set forth in
28 § 7001 of Title 15 of the United States Code; or

29 d. Substitute notice, if the individual or the commercial entity
30 required to provide notice demonstrates that the cost of providing
31 notice will exceed \$250,000, or that the affected class of Massa-
32 chusetts residents to be notified exceeds 500,000 residents, or that
33 the individual or the commercial entity does not have sufficient
34 contact information to provide notice. Substitute notice consists of
35 all of the following:

36 1. E-mail notice if the individual or the commercial entity has
37 e-mail addresses for the members of the affected class of Massa-
38 chusetts residents; and

39 2. Conspicuous posting of the notice on the web site page of the
40 individual or the commercial entity if the individual or the com-
41 mercial entity maintains one; and

42 3. Notice to major statewide media.

43 (4) “Personal information” means a Massachusetts resident’s
44 first name or first initial and last name in combination with any 1
45 or more of the following data elements that relate to the resident,
46 when either the name or the data elements are not encrypted:

47 a. Social Security number;

48 b. Driver’s license number or Massachusetts Identification Card
49 number; or

50 c. Account number, or credit or debit card number, in combina-
26 tion with any required security code, access code, or password
27 that would permit access to a resident’s financial account.

28 The term “personal information” does not include publicly
29 available information that is lawfully made available to the
30 general public from federal, state, or local government records;

31 Section 2.

32 Disclosure of breach of security of computerized personal
33 information by an individual or a commercial entity.

34 (a) An individual or a commercial entity that conducts business
35 in Massachusetts and that owns or licenses computerized data that
36 includes personal information about a resident of Massachusetts
37 shall, when it becomes aware of a breach of the security of the
38 system, conduct in good faith a reasonable and prompt investiga-
39 tion to determine the likelihood that personal information has
40 been or will be misused. If the investigation determines that the
41 misuse of information about a Massachusetts resident has
42 occurred or is reasonably likely to occur, the individual or the
43 commercial entity shall give notice as soon as possible to the
44 affected Massachusetts resident. Notice must be made in the most
45 effective and expedient time possible and without unreasonable
46 delay, consistent with the legitimate needs of law enforcement and
47 consistent with any measures necessary to determine the scope of
48 the breach and to restore the reasonable integrity of the computer-
49 ized data system.

50 (b) An individual or a commercial entity that maintains com-
51 puterized data that includes personal information that the indi-
52 vidual or the commercial entity does not own or license shall give
53 notice to and cooperate with the owner or licensee of the informa-
54 tion of any breach of the security of the system immediately
55 following discovery of a breach, if misuse of personal information
56 about a Massachusetts resident occurred or is reasonably likely to
57 occur. Cooperation includes sharing with the owner or licensee
58 information relevant to the breach.

59 (c) Notice required by this chapter may be delayed if a law
60 enforcement agency determines that the notice will impede a
61 criminal investigation. Notice required by this chapter must be
62 made in good faith, without unreasonable delay and as soon as
63 possible after the law enforcement agency determines that notifi-
64 cation will no longer impede the investigation.

65 Section 3.

66 (a) Under this chapter, an individual or a commercial entity that
67 maintains its own notice procedures as part of an information
68 security policy for the treatment of personal information, and
69 whose procedures are otherwise consistent with the timing
70 requirements of this chapter is deemed to be in compliance with
71 the notice requirements of this chapter if the individual or the
72 commercial entity notifies affected Massachusetts residents in

73 accordance with its policies in the event of a breach of security of
74 the system.

75 (b) Under this chapter, an individual or a commercial entity that
76 is regulated by state or federal law and that maintains procedures
77 for a breach of the security of the system pursuant to the laws,
78 rules, regulations, guidances, or guidelines established by its pri-
79 mary or functional state or federal regulator is deemed to be in
80 compliance with this chapter if the individual or the commercial
81 entity notifies affected Massachusetts residents in accordance with
82 the maintained procedures when a breach occurs. This chapter
83 shall not apply to any financial institution, trust company or credit
84 union that is required by the federal gram-Leach-Bliley Act of
85 1999, 15 U.S.C. s. 6801-6809 or any other state or federal statute,
86 regulation or other regulatory action to notify consumers of a
87 breach of security and is subject to examination by its functional
88 governmental regulatory agency for compliance with applicable
89 federal law.

90 Section 4.

91 Notwithstanding any other provision of law or contract and in
92 addition to any other liability of a commercial entity to a bank as
93 defined in section 1 of Chapter 167, whenever a commercial entity
94 is required to provide notice to a consumer pursuant to section 3
95 of this act or to a bank pursuant to section 3 of this act, the com-
96 mercial entity shall be liable to such bank for the costs of reason-
97 able actions undertaken by the bank on behalf of customers of the
98 bank as a direct result of an actual breach of data security in order
99 to protect sensitive financial personal information of such cus-
100 tomer or to continue to provide financial services to any such cus-
101 tomer, including any cost incurred as a result of a potential or
102 actual breach of data security in connection with:

103 a) the cancellation or reissuance of any credit card issued by
104 any bank as defined in Chapter 167, or access device as defined in
105 section 1 of chapter 167B;

106 b) the closure of any deposit, transaction, share draft or other
107 account and any action to stop payments or block transactions
108 with respect to any such account;

109 c) the opening or reopening of any deposit, transaction, share
110 draft, or other account for any customer of the bank;

111 d) any refund or credit made to any customer of the bank as a
112 result of unauthorized transactions.

113 Section 5.

114 The Office of Consumer Affairs and Business Regulation is
115 hereby authorized and directed to prescribe regulations necessary
116 to implement this section within 6 months from the effective date
117 of this act. Such regulations shall include a method of enforcing
118 and collecting the costs owed to banks pursuant to this section.