

HOUSE No. 223

The Commonwealth of Massachusetts

PRESENTED BY:

Michael S. Day

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:
<i>Michael S. Day</i>	<i>31st Middlesex</i>
<i>David Allen Robertson</i>	<i>19th Middlesex</i>
<i>Carolyn C. Dykema</i>	<i>8th Middlesex</i>
<i>Jeffrey N. Roy</i>	<i>10th Norfolk</i>
<i>Stephan Hay</i>	<i>3rd Worcester</i>

HOUSE No. 223

By Mr. Day of Stoneham, a petition (accompanied by bill, House, No. 223) of Michael S. Day and others relative to the security of personal financial information. Consumer Protection and Professional Licensure.

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE HOUSE, NO. 2813 OF 2017-2018.]

The Commonwealth of Massachusetts

**In the One Hundred and Ninety-First General Court
(2019-2020)**

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 2016 Official Edition, is
2 hereby amended by striking out said section and inserting in place thereof the following section:-

3 Section 1. (a) As used in this chapter, the following words shall, unless the context
4 clearly 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 “Data”, any material upon which written, drawn, spoken, visual, or electromagnetic
19 information or images are recorded or preserved, regardless of physical form or characteristics.

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

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

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

33 “Notice”, shall include:

34 (i) written notice;

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

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

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

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

45 (a) Social Security number;

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

47 (c) financial account number, or credit or debit card number, with or without any required
48 security code, access code, personal identification number or password, that would permit access
49 to a resident’s financial account; or

50 (d) biometric indicator of the consumer used to gain access to financial accounts of the
51 consumer; provided, however, that “Personal information” shall not include information that is
52 lawfully obtained from publicly available information, or from federal, state or local government
53 records lawfully made available to the general public.

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

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

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

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

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

63 (b) The department of consumer affairs and business regulation may adopt regulations,
64 from time to time, to revise the definition of “encrypted”, as used in this chapter, to reflect
65 applicable technological advancements.

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

68 Section 2. (a) The department of consumer affairs and business regulation shall adopt
69 regulations relative to any person that owns or licenses personal information about a resident of
70 the commonwealth. Such regulations shall require a person subject to this chapter to develop,

71 implement, and maintain a comprehensive information security program that contains
72 administrative, technical, and physical safeguards that are reasonably designed to (1) ensure the
73 security and confidentiality of personal information of residents of the commonwealth, (2)
74 protect against any anticipated threats or hazards to the security or integrity of such information;
75 and (3) protect against unauthorized acquisition of such information that could result in
76 substantial harm to the individuals to whom such information relates.

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

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

91 SECTION 3: Section 3 of said chapter 93H is hereby further amended by striking out the
92 third paragraph and inserting in place thereof the following paragraph:- The notice to be

93 provided to the resident shall include, but not be limited to, the consumer's right to obtain a
94 police report, how a consumer requests a security freeze and the necessary information to be
95 provided when requesting the security freeze, and any fees required to be paid to any of the
96 consumer reporting agencies.