

HOUSE No. 76

The Commonwealth of Massachusetts

PRESENTED BY:

Tram T. Nguyen

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 protecting sensitive information from security breaches.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
<i>Tram T. Nguyen</i>	<i>18th Essex</i>	<i>1/18/2023</i>

HOUSE No. 76

By Representative Nguyen of Andover, a petition (accompanied by bill, House, No. 76) of Tram T. Nguyen relative to protecting sensitive information from security breaches. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

**In the One Hundred and Ninety-Third General Court
(2023-2024)**

An Act relative to protecting sensitive information from security breaches.

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 of the General Laws is hereby amended by
2 inserting after the definition of “Agency” the following definition:-

3 “Biometric information”, a retina or iris scan, fingerprint, voiceprint, map or scan of hand
4 or face geometry, vein pattern, gait pattern, or other data generated from the specific technical
5 processing of an individual’s unique biological or physiological patterns or characteristics used
6 to authenticate or identify a specific individual; provided, however, that “biometric information”
7 shall not include:

8 (i) a digital or physical photograph;

9 (ii) an audio or video recording; or

10 (iii) data generated from a digital or physical photograph, or an audio or video recording,
11 unless such data is generated to identify a specific individual.

12 SECTION 2. Said section 1 of said chapter 93H is hereby further amended by striking out
13 the definition of “Breach of security” and inserting in place thereof the following definition:-

14 “Breach of security”, the unauthorized acquisition or use of unencrypted electronic data,
15 or encrypted electronic data when the encryption key or security credential has been acquired;
16 provided, however, that such unauthorized acquisition or use compromises the security,
17 confidentiality, or integrity of personal information maintained by a person or agency; and
18 provided further, that a good faith but unauthorized acquisition of personal information by an
19 employee or agent of a person or agency for the lawful purposes of such person or agency is not
20 a breach of security unless the personal information is used in an unauthorized manner or subject
21 to further unauthorized disclosure.

22 SECTION 3. Said section 1 of said chapter 93H is hereby further amended by inserting
23 after the definition of “Encrypted” the following definitions:-

24 “Genetic information”, information, regardless of format, that:

25 (i) results from the analysis of a biological sample of an individual, or from another
26 source enabling equivalent information to be obtained; and

27 (ii) concerns an individual’s genetic material, including, but not limited to,
28 deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes,
29 alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs),
30 uninterpreted data that results from analysis of the biological sample or other source, and any
31 information extrapolated, derived, or inferred therefrom.

32 "Health insurance information", an individual's health insurance policy number,
33 subscriber identification number, or any identifier used by a health insurer to identify the
34 individual.

35 "Medical information", information regarding an individual's medical history, mental or
36 physical condition, or medical treatment or diagnosis by a healthcare professional.

37 SECTION 4. Said section 1 of said chapter 93H is hereby further amended by striking out
38 the definition of "Personal information" and inserting in place thereof the following definition:-

39 "Personal information" shall mean either of the following:

40 (i) a resident's first name and last name or first initial and last name in combination with
41 any 1 or more of the following data elements that relate to such resident:

42 (A) social security number;

43 (B) taxpayer identification number or identity protection personal identification number
44 issued by the Internal Revenue Service;

45 (C) driver's license number, passport number, military identification number, state-issued
46 identification card number, or other unique identification number issued by the government that
47 is commonly used to verify the identity of a specific individual;

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

51 (E) biometric information;

52 (F) date of birth;

53 (G) genetic information;

54 (H) health insurance information;

55 (I) medical information; or

56 (J) specific geolocation information; or

57 (ii) a username or electronic mail address, in combination with a password or security
58 question and answer that would permit access to an online account.

59 SECTION 5. Said section 1 of said chapter 93H is hereby further amended by inserting
60 after the definition of “Personal information” the following definition:-

61 “Specific geolocation information”, information derived from technology including, but
62 not limited to, global positioning system level latitude and longitude coordinates or other
63 mechanisms that directly identify the specific location of an individual within a geographic area
64 that is equal to or less than the area of a circle with a radius of 1,850 feet; provided, however,
65 that “geolocation information” shall exclude the content of communications or any information
66 generated by or connected to advanced utility metering infrastructure systems or equipment for
67 use by a utility.

68 SECTION 6. Section 2 of said chapter 93H is hereby amended by inserting the following
69 subsection:-

70 (d) The rules and regulations adopted pursuant to this section shall be updated from time
71 to time to reflect any changes to the definitions of “breach of security” or “personal information”
72 in section 1.

73 SECTION 7. Section 3 of said chapter 93H is hereby amended by inserting after the
74 words “unauthorized purpose” in subsection (b) the following words:- and such use or
75 acquisition presents a reasonably foreseeable risk of financial, physical, reputational or other
76 cognizable harm to the resident.

77 SECTION 8. Said section 3 of said chapter 93H is hereby further amended by striking out
78 clause (vii) of subsection (b) and inserting in place thereof the following clause:- (vii) the type of
79 personal information compromised, including, but not limited to, any of the categories of
80 personal information set forth in subclauses (A) through (J) of clause (i) or in clause (ii) of the
81 definition of “personal information” in section 1.

82 SECTION 9. Said section 3 of said chapter 93H is hereby further amended by striking out
83 the last sentence of the first paragraph of subsection (b) and inserting in place thereof the
84 following sentence:- A person who experienced a breach of security shall file a report with the
85 attorney general and the director of consumer affairs and business regulation certifying their
86 credit monitoring services comply with section 3A; provided, however, that such a report shall
87 not be required if the personal information compromised by the breach of security is medical
88 information or specific geolocation information.

89 SECTION 10. Said section 3 of said chapter 93H is hereby further amended by striking
90 out the third paragraph of subsection (b) and inserting in place thereof the following paragraphs:-

91 The notice to be provided to the resident shall include, but shall not be limited to: (i) the
92 date, estimated date, or estimated date range of the breach of security; (ii) the type of personal
93 information compromised, including, but not limited to, any of the categories of personal
94 information set forth in subclauses (A) through (J) of clause (i) or in clause (ii) of the definition
95 of “personal information” in section 1; (iii) a general description of the breach of security; (iv)
96 information that the resident can use to contact the person or agency reporting the breach of
97 security; (v) the resident’s right to obtain a police report; (vi) how a resident may request a
98 security freeze and the necessary information to be provided when requesting the security freeze;
99 (vii) a statement that there shall be no charge for a security freeze; (viii) mitigation services to be
100 provided pursuant to this chapter; and (ix) the toll-free numbers, address, and website for the
101 federal trade commission. The notice shall not need to include information pursuant to clauses
102 (vi) and (vii) if the personal information compromised by the breach of security is medical
103 information or specific geolocation information.

104 The person or agency that experienced the breach of security shall provide a sample copy
105 of the notice it sent to consumers to the attorney general and the office of consumer affairs and
106 business regulation. A notice provided pursuant to this section shall not be delayed on grounds
107 that the total number of residents affected is not yet ascertained. In such case, and where
108 otherwise necessary to update or correct the information required, a person or agency shall
109 provide additional notice as soon as practicable and without unreasonable delay upon learning
110 such additional information.

111 If the breach of security involves log-in credentials, pursuant to clause (ii) of the
112 definition of “personal information” in section 1, for an online account and no other personal
113 information, the person or agency may comply with this chapter by providing notice in electronic

114 or other form; provided, however, that such notice shall direct the resident whose personal
115 information has been breached to: (i) promptly change the resident’s password and security
116 question or answer, as applicable; or (ii) take other steps appropriate to protect the affected
117 online account with the person or agency and all other online accounts for which the resident
118 whose personal information has been breached uses the same username or electronic mail
119 address and password or security question or answer.

120 If the breach of security involves the log-in credentials, pursuant to clause (ii) of the
121 definition of “personal information” in section 1, of an electronic mail account furnished by a
122 person or agency, the person or agency shall not comply with this chapter by providing notice of
123 the breach of security to such electronic mail address but shall instead provide notice by another
124 acceptable method of notice pursuant to this chapter or by clear and conspicuous notice delivered
125 to the resident online when the resident is connected to the online account from an internet
126 protocol address or online location from which the person or agency knows the resident
127 customarily accesses the account.