SENATE DOCKET, NO. 1303   FILED ON: 1/19/2023

SENATE . . . . No. 30

The Commonwealth of Massachusetts

PRESENTED BY:

Barry R. Finegold

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:
Barry R. Finegold	*Second Essex and Middlesex*

SENATE DOCKET, NO. 1303   FILED ON: 1/19/2023

SENATE . . . . No. 30

By Mr. Finegold, a petition (accompanied by bill, Senate, No. 30) of Barry R. Finegold for legislation to protect 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:

SECTION 1. Section 1 of chapter 93H of the General Laws is hereby amended by inserting after the definition of “Agency” the following definition:-

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

(i) a digital or physical photograph;

(ii) an audio or video recording; or

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

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

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

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

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

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

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

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

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

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

"Personal information" shall mean either of the following:

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

(A) social security number;

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

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

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

(E) biometric information;

(F) date of birth;

(G) genetic information;

(H) health insurance information;

(I) medical information; or

(J) specific geolocation information; or

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

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

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

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

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

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

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

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

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

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

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

If the breach of security involves log-in credentials, pursuant to clause (ii) of the definition of "personal information" in section 1, for an online account and no other personal information, the person or agency may comply with this chapter by providing notice in electronic or other form; provided, however, that such notice shall direct the resident whose personal information has been breached to: (i) promptly change the resident’s password and security question or answer, as applicable; or (ii) take other steps appropriate to protect the affected online account with the person or agency and all other online accounts for which the resident whose personal information has been breached uses the same username or electronic mail address and password or security question or answer.

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