SENATE DOCKET, NO. 2333 FILED ON: 1/17/2025

SENATE . . . . . No. 39

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 protecting sensitive personal information from breaches and other cybersecurity incidents.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
Barry R. Finegold	*Second Essex and Middlesex*

SENATE DOCKET, NO. 2333 FILED ON: 1/17/2025

SENATE . . . . . No. 39

By Mr. Finegold, a petition (accompanied by bill, Senate, No. 39) of Barry R. Finegold for legislation to protect sensitive personal information from breaches and other cybersecurity incidents by creating a Massachusetts Cyber Incident Response Team. Advanced Information Technology, the Internet and Cybersecurity.

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE SENATE, NO. *2539* OF 2023-2024.]

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act protecting sensitive personal information from breaches and other cybersecurity incidents.

Whereas, The deferred operation of this act would tend to defeat its purpose, which is to further regulate cybersecurity and breaches of personal information, therefore it is hereby declared to be an emergency law, necessary for the immediate preservation of the public safety.

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. Chapter 7D of the General Laws is hereby amended by adding the following new sections:-

Section 12. Definitions

As used in this section, and sections 13 and 14, the following words shall have the following meanings, unless the context clearly requires otherwise:

"Critical infrastructure", the assets, systems and networks, either physical or virtual, within the commonwealth that are so vital to the commonwealth or the United States that the incapacitation or destruction of such a system or asset would have a debilitating impact on physical security, economic security, public health or safety or any combination thereof; provided, however, that "critical infrastructure" shall include, but not be limited to, election systems, transportation infrastructure, water, gas and electric utilities and shall include any critical infrastructure sectors as identified by: (1) Presidential Policy Directive-21 or a successor directive; or (2) the Cybersecurity and Infrastructure Security Agency.

"Cybersecurity incident", an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems or information resident thereon; provided, however, that a cybersecurity incident may include a vulnerability in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source.

"Cybersecurity threat", any circumstance or event with the potential to adversely impact organizational operations, including mission, functions, image or reputation, organizational assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, denial of service or any combination thereof; provided, however, that the term "cybersecurity threat" shall also include the potential for a threat source to successfully exploit a particular information system vulnerability..

"Governmental entity", any department of state, county or local government including the executive, legislative or judicial, and all councils thereof and thereunder, any division, board, bureau, commission, institution, tribunal or other instrumentality within such department or any independent state, county or local authority, district, commission, instrumentality or agency.

"Response team", the Massachusetts Cyber Incident Response Team established pursuant to section 13.

Section 13. Massachusetts Cyber Incident Response Team.

(a) There shall be established a Massachusetts Cyber Incident Response Team, which shall serve as a standing subcommittee of the office, the mission of which is to enhance the commonwealth's ability to prepare for, respond to, mitigate against and recover from significant cybersecurity incidents.

(b) The response team shall consist of: the secretary of technology services and security or their designee, who shall serve as chair; a representative of the commonwealth security operations center as designated by the director of security operations; the secretary of public safety and security or their designee; a representative of the state police cyber crime unit; a representative of the commonwealth fusion center; the adjutant general of the Massachusetts National Guard or their designee; the director of the Massachusetts emergency management agency or their designee; the comptroller or their designee; and any other state or local officials as assigned by the chair. The chair shall designate a member of the response team to act as a liaison with federal agencies.

(c) The response team shall review cybersecurity threat information, including intrusion methods, common techniques and known vulnerabilities, to make informed recommendations

and establish appropriate policies to manage the risk of cybersecurity incidents for all governmental entities; provided, however, that such recommendations, policies and directives shall be informed by information and best practices obtained through the established information sharing network of local, state, federal and industry partners in which response team members regularly participate.

(d) The response team shall develop and maintain an updated cybersecurity incident response plan for the commonwealth and submit such plan annually for review, not later than November 1, to the governor and the joint committee on advanced information technology, the internet and cybersecurity. The response team shall conduct tabletop exercises to test the plan at least twice per year and shall conduct individual tabletop exercise testing with a subset of governmental entities, as selected by the response team, at least quarterly. Said plan, which shall not be a public record pursuant to chapter 66 or clause twenty-sixth of section 7 of chapter 4, shall include, but not be limited to:

(i) ongoing and anticipated cybersecurity incidents or cybersecurity threats;

(ii) a risk analysis identifying the vulnerabilities of critical infrastructure and detailing risk-informed recommendations to address such vulnerabilities;

(iii) recommendations regarding the deployment of governmental entity resources and security professionals in rapidly responding to such cybersecurity incidents or cybersecurity threats;

(iv) recommendations regarding best practices to minimize the impact of significant cybersecurity threats to governmental entities; and

(v) guidelines for governmental entities regarding communication with an individual or entity that is demanding a payment of ransom related to a cybersecurity incident

(e) In the event of a cybersecurity incident that threatens or results in a material impairment of the infrastructure or services of a governmental entity or critical infrastructure, the secretary of technology services and security shall, with the approval of the governor, serve as the director of the response team; provided, however, that the secretary of technology services and security may direct the response team to collaborate with other governmental entities, including federal entities, that are not members of the response team as appropriate to respond to a cybersecurity incident. The provisions of sections 18 through 25, inclusive, of chapter 30A shall not apply to meetings, communications, deliberations or other activities of the response team conducted in response to a cybersecurity incident under this subsection.

(f) Governmental entities shall comply with all protocols and procedures established by the response team and all related policies, standards and administrative directives issued by the office pursuant to subsection (b) of section 3. The chief information officer or equivalent responsible officer for any governmental entity shall, as soon as practicable, report any known cybersecurity incident to the commonwealth security operations center, in a form to be prescribed by the office. The commonwealth security operations center shall notify the response team of all reported security threats or incidents as soon as practicable, but not later than 24 hours after receiving a report.

(g) The commonwealth fusion center and the commonwealth security operations center shall routinely exchange information with the response team and the federal cybersecurity and infrastructure security agency related to cybersecurity threats and cybersecurity incidents that

have been reported to or discovered by their respective state agencies or reported to the response team.

(h) The office and the response team shall consult with the Massachusetts Cyber Center and assist said center with efforts to foster cybersecurity resiliency through communications, collaboration and outreach to governmental entities, educational institutions and industry partners.

(i) The secretary of technology services and security shall promulgate regulations or directives to carry out the purposes of this section.

Section 14. Critical Infrastructure Cyber Incident Reporting Requirements

(a) As used in this section, the following words shall have the following meanings unless the context clearly requires otherwise:

“Covered entity”, any entity that owns or operates critical infrastructure.

“Secretary”, the secretary of the executive office of public safety and security.

(b) A covered entity shall provide notice, as soon as practicable and without unreasonable delay, when such covered entity knows or has reason to know of a cybersecurity incident to the commonwealth fusion center in a form to be prescribed by the secretary in consultation with the response team; provided, however, that such notice shall include, but not be limited to:

(i) a timeline of events as best known by the covered entity and the type of cybersecurity incident known or suspected;

(ii) how the cybersecurity incident was initially detected or discovered;

(iii) a list of the specific assets that have been affected or are suspected to be affected;

(iv) copies of any electronic communications that are suspected of being malicious, if applicable;

(v) copies of any malware, threat actor tool or malicious links suspected of causing the cybersecurity incident, if applicable;

(vi) any digital logs such as firewall, active directory or event logs, if available;

(vii) forensic images of random access memory or virtualized random access memory from affected systems, if available;

(viii) contact information for the covered entity and any third-party entity engaging in cybersecurity incident response that is involved; and

(ix) any other information related to the cybersecurity incident as required by the secretary.

Any notice provided by a covered entity under this subsection shall not be a public record pursuant to chapter 66 or clause twenty-sixth of section 7 of chapter 4.

(c) Upon receipt of said notice, the representative of the commonwealth fusion center to the response team or their designee shall:

(i) create and maintain a record of the cybersecurity incident, including all information provided by the covered entity in the notice under subsection (b); and

(ii) provide a copy of said record to the response team, which shall be included in the response team’s annual cyber incident response plan required pursuant to subsection (d) of

section 13; provided, however, that such copy shall not include any information identifiable to the covered entity that is not expressly necessary for the preparation of the response team's report unless the covered entity has provided affirmative consent to share such information.

(d) Upon receipt of the notice required by subsection (b), the commonwealth fusion center may:

(i) coordinate with the response team to identify or communicate recommended response measures as appropriate;

(ii) assist the covered entity with implementing recommended response measures as appropriate, alone or in conjunction with: (A) any agency or entity represented in the response team; (B) any local law enforcement agency; (C) private individuals and other entities at the discretion of the secretary; or (D) the Massachusetts Cyber Center; and

(iii) provide, at the discretion of the secretary, information about other entities that are capable of providing mitigation and remediation support following a cybersecurity incident or in response to a cybersecurity threat.

(e) Nothing in this section shall be construed to:

(i) fulfill any regulatory data breach reporting requirements pursuant to chapter 93H; or

(ii) absolve any duty under applicable federal law to report a cybersecurity threat or cybersecurity incident to the federal cybersecurity and infrastructure security agency.

(f) This section shall not apply to a covered entity that reports the cybersecurity incident to the federal cybersecurity and infrastructure security agency pursuant to the federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 and its implementing regulations.

(g) The secretary, in consultation with the secretary of technology services and security, shall promulgate regulations for the purposes of carrying out this section.

SECTION 2. Section 1 of chapter 93H of the General Laws, as appearing in the 2022 Official Edition, 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 3. Said section 1 of said chapter 93H, as so appearing, 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 4. Said section 1 of said chapter 93H, as so appearing, is hereby further amended by inserting after the definition of “Encrypted” the following 3 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, ribonucleic acids, genes, chromosomes, alleles, genomes, alterations or modifications to deoxyribonucleic acids or ribonucleic acids, single nucleotide polymorphisms, uninterpreted data that results from analysis of the biological sample or other source or 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 5. Said section 1 of said chapter 93H, as so appearing, is hereby further amended by striking out the definition of “Personal information” and inserting in place thereof the following definition:-

“Personal information” shall mean:

(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 6. Said section 1 of said chapter 93H, as so appearing, 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 not greater than the area of a circle with a radius of 1,850 feet; provided, however, that "specific 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 7. Section 2 of said chapter 93H, as so appearing, is hereby amended by adding the following new 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 8. Section 3 of said chapter 93H, as so appearing, is hereby amended by striking out subsection (b) and inserting in place thereof the following subsection:-

(b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency: (i) knows or has reason to know of a breach of security; or (ii) knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose and such use or acquisition presents a reasonably foreseeable risk of financial, physical, reputational or other cognizable harm to the resident, the attorney general, the Federal Bureau of Investigation and the director of consumer affairs and business regulation, in accordance with this chapter. The notice to be provided to the attorney general, Federal Bureau of Investigation and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to: (i) the nature of the breach of security or unauthorized acquisition or use; (ii) the number of residents of the commonwealth affected by such incident at the time of notification; (iii) the name and address of the person or agency that experienced the breach of security; (iv) the name and title of the person or agency reporting the breach of security and their relationship to the person or agency that experienced the breach of security; (v) the type of person or agency reporting the breach of security; (vi) the person responsible for the breach of security, if known; (vii) the type of personal information compromised, including, but not limited to, any of the categories of personal information set forth in the definition of "personal information" in section 1; (viii) whether the person or agency maintains a written information security program; and (ix) any steps the person or agency has taken or plans to take relating to the incident, including updating such written information security program. 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.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies so identified.

The notice to be provided to the resident shall include, but 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 number, address and website for the federal trade commission; provided, however, that 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.