

SENATE No.

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:

Barry R. Finegold

DISTRICT/ADDRESS:

Second Essex and Middlesex

SENATE No.

[Pin Slip]

[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:

1 SECTION 1. Chapter 7D of the General Laws is hereby amended by adding the
2 following new sections:-

3 Section 12. Definitions

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

6 “Critical infrastructure”, the assets, systems and networks, either physical or virtual,
7 within the commonwealth that are so vital to the commonwealth or the United States that the

8 incapacitation or destruction of such a system or asset would have a debilitating impact on
9 physical security, economic security, public health or safety or any combination thereof;
10 provided, however, that “critical infrastructure” shall include, but not be limited to, election
11 systems, transportation infrastructure, water, gas and electric utilities and shall include any
12 critical infrastructure sectors as identified by: (1) Presidential Policy Directive-21 or a successor
13 directive; or (2) the Cybersecurity and Infrastructure Security Agency.

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

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

27 “Governmental entity”, any department of state, county or local government including
28 the executive, legislative or judicial, and all councils thereof and thereunder, any division, board,

29 bureau, commission, institution, tribunal or other instrumentality within such department or any
30 independent state, county or local authority, district, commission, instrumentality or agency.

31 “Response team”, the Massachusetts Cyber Incident Response Team established pursuant
32 to section 13.

33 Section 13. Massachusetts Cyber Incident Response Team.

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

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

47 (c) The response team shall review cybersecurity threat information, including intrusion
48 methods, common techniques and known vulnerabilities, to make informed recommendations
49 and establish appropriate policies to manage the risk of cybersecurity incidents for all
50 governmental entities; provided, however, that such recommendations, policies and directives

51 shall be informed by information and best practices obtained through the established information
52 sharing network of local, state, federal and industry partners in which response team members
53 regularly participate.

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

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

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

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

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

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

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

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

89 (g) The commonwealth fusion center and the commonwealth security operations center
90 shall routinely exchange information with the response team and the federal cybersecurity and
91 infrastructure security agency related to cybersecurity threats and cybersecurity incidents that
92 have been reported to or discovered by their respective state agencies or reported to the response
93 team.

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

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

100 Section 14. Critical Infrastructure Cyber Incident Reporting Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

130 (ii) provide a copy of said record to the response team, which shall be included in the
131 response team's annual cyber incident response plan required pursuant to subsection (d) of
132 section 13; provided, however, that such copy shall not include any information identifiable to

133 the covered entity that is not expressly necessary for the preparation of the response team's
134 report unless the covered entity has provided affirmative consent to share such information.

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

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

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

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

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

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

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

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

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

155 SECTION 2. Section 1 of chapter 93H of the General Laws, as appearing in the 2022
156 Official Edition, is hereby amended by inserting after the definition of “Agency” the following
157 definition:-

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

163 (i) a digital or physical photograph;

164 (ii) an audio or video recording; or

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

167 SECTION 3. Said section 1 of said chapter 93H, as so appearing, is hereby further
168 amended by striking out the definition of “Breach of security” and inserting in place thereof the
169 following definition:-

170 “Breach of security”, the unauthorized acquisition or use of unencrypted electronic data,
171 or encrypted electronic data when the encryption key or security credential has been acquired;
172 provided, however, that such unauthorized acquisition or use compromises the security,
173 confidentiality or integrity of personal information maintained by a person or agency; and

174 provided further, that a good faith but unauthorized acquisition of personal information by an
175 employee or agent of a person or agency for the lawful purposes of such person or agency is not
176 a breach of security unless the personal information is used in an unauthorized manner or subject
177 to further unauthorized disclosure.

178 SECTION 4. Said section 1 of said chapter 93H, as so appearing, is hereby further
179 amended by inserting after the definition of “Encrypted” the following 3 definitions:-

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

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

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

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

191 “Medical information”, information regarding an individual’s medical history, mental or
192 physical condition or medical treatment or diagnosis by a healthcare professional.

193 SECTION 5. Said section 1 of said chapter 93H, as so appearing, is hereby further
194 amended by striking out the definition of “Personal information” and inserting in place thereof
195 the following definition:-

196 “Personal information” shall mean:

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

199 (A) social security number;

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

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

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

208 (E) biometric information;

209 (F) date of birth;

210 (G) genetic information;

211 (H) health insurance information;

212 (I) medical information; or

213 (J) specific geolocation information; or

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

216 SECTION 6. Said section 1 of said chapter 93H, as so appearing, is hereby further
217 amended by inserting after the definition of “Personal information” the following definition:-

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

225 SECTION 7. Section 2 of said chapter 93H, as so appearing, is hereby amended by
226 adding the following new subsection:-

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

230 SECTION 8. Section 3 of said chapter 93H, as so appearing, is hereby amended by
231 striking out subsection (b) and inserting in place thereof the following subsection:-

232 (b) A person or agency that owns or licenses data that includes personal information
233 about a resident of the commonwealth shall provide notice, as soon as practicable and without
234 unreasonable delay, when such person or agency: (i) knows or has reason to know of a breach of
235 security; or (ii) knows or has reason to know that the personal information of such resident was
236 acquired or used by an unauthorized person or used for an unauthorized purpose and such use or
237 acquisition presents a reasonably foreseeable risk of financial, physical, reputational or other
238 cognizable harm to the resident, the attorney general, the Federal Bureau of Investigation and
239 the director of consumer affairs and business regulation, in accordance with this chapter. The
240 notice to be provided to the attorney general, Federal Bureau of Investigation and said director,
241 and consumer reporting agencies or state agencies if any, shall include, but not be limited to: (i)
242 the nature of the breach of security or unauthorized acquisition or use; (ii) the number of
243 residents of the commonwealth affected by such incident at the time of notification; (iii) the
244 name and address of the person or agency that experienced the breach of security; (iv) the name
245 and title of the person or agency reporting the breach of security and their relationship to the
246 person or agency that experienced the breach of security; (v) the type of person or agency
247 reporting the breach of security; (vi) the person responsible for the breach of security, if known;
248 (vii) the type of personal information compromised, including, but not limited to, any of the
249 categories of personal information set forth in the definition of “personal information” in section
250 1; (viii) whether the person or agency maintains a written information security program; and (ix)
251 any steps the person or agency has taken or plans to take relating to the incident, including
252 updating such written information security program. A person who experienced a breach of
253 security shall file a report with the attorney general and the director of consumer affairs and
254 business regulation certifying their credit monitoring services comply with section 3A; provided,

255 however, that such a report shall not be required if the personal information compromised by the
256 breach of security is medical information or specific geolocation information.

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

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

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

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

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

- 298 protocol address or online location from which the person or agency knows the resident
- 299 customarily accesses the account.