HOUSE . . . . . No. 4807

The Commonwealth of Massachusetts

HOUSE OF REPRESENTATIVES, December 8, 2025.

The committee on Consumer Protection and Professional Licensure, to whom were referred the petition (accompanied by bill, House, No. 358) of Michael S. Day relative to the security of personal financial information; and the petition (accompanied by bill, House, No. 461) of Lindsay N. Sabadosa, Steven Owens and others relative to consumer health data, reports recommending that the accompanying bill (House, No. 4807) ought to be pass.

For the committee,

TACKEY CHAN.

FILED ON: 11/25/2025

HOUSE . . . . . No. 4807

The Commonwealth of Massachusetts

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

An Act relative to updating the security of personal information.

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, as appearing in the 2024 Official Edition, is hereby amended by striking out the definition of “Agency”, and inserting in place thereof the following 3 definitions:-

“Access device”, a card or other device that contains a magnetic stripe, microprocessor chip or other means for storage of personal information.

"Agency", any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.

“Biometric indicator”, any unique biological attribute or measurement data that can be used to authenticate the identity of a resident, including, but not limited to fingerprint, iris or retina patterns, voice print, facial characteristics or hand geometry; provided, however, it shall not include a physical or digital photograph or a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or

operations under the federal health insurance portability and accountability act of 1996 and its implementing regulations.

SECTION 2. Said section 1 of said chapter 93H of the General Laws, as so appearing, is hereby further amended by inserting after the definition of “Encrypted”, the following 2 definitions:-

“Information security program”, the administrative, technical or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of or otherwise handle personal information.

“Neural data”, information generated by measuring the activity of a resident’s central or peripheral nervous system, and that is not inferred from nonneural data.

SECTION 3. Said section 1 of said chapter 93H of the General Laws, as so appearing, is hereby further amended by striking out the definitions of “Personal information” and “Substitute notice”, and inserting in place thereof the following definitions:-

"Personal information", 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) driver's license number, state-issued identification card number, or federal-issued identification number;

(c) health insurance policy number or health insurance identification number;

(d) any information about a resident's medical or medication history, bodily functions, vital signs, measurements, or symptoms, or mental or physical condition, or about a health care professional's medical diagnosis or treatment of the resident;

(e) precise location information;

(f) a user-name or electronic mail address in combination with a password or security question and answer that would permit access to a resident's account;

(g) neural data;

(h) a biometric indicator; or

(i) 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; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Precise location information", data derived from technology, including, but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a resident with precision and accuracy within a radius of 1,750 feet; provided, however, precise location information shall not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

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

"Substitute notice", shall consist of all of the following:—

(i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents except if the breached personal information includes a user-name or electronic mail address in combination with a password or security question and answer that would permit access to an account, in which case a person shall instead provide clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or from an online location which the person knows the resident customarily uses to access the online account;

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

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

SECTION 4. Section 2 of said chapter 93H of the General Laws, as so appearing, is hereby amended by striking out subsection (a), and inserting in place thereof the following subsection:-

(a) The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated

threats or hazards to the security or integrity of such information; oversee third-party service providers by taking reasonable steps to select and retain by written contract third-party service providers that are capable of maintaining appropriate safeguards for personal information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.

SECTION 5. Section 3 of said chapter 93H of the General Laws, as so appearing, is hereby amended by striking out the third paragraph of subsection (b), and inserting in place thereof the following paragraph:-

The notice to be provided to the resident shall include, but shall not be limited to: (i) the resident's right to obtain a police report; (ii) a time frame of exposure, if known, including the date of the breach of security and the date of the discovery of said breach; (iii) how a resident may request a security freeze and the necessary information to be provided when requesting the security freeze; (iv) that there shall be no charge for a security freeze; and (v) mitigation services to be provided pursuant to this chapter; provided, however, that said notice shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use. 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.

SECTION 6. Said section 3 of said chapter 93H of the General Laws, as so appearing, is hereby further amended by striking out subsection (f), and inserting in place thereof the following 2 subsections:-

(f) Notice to affected residents under this section is not required if the exposure of the personal information was an inadvertent disclosure by persons authorized to access such personal information, and the person reasonably determines such exposure will not likely result in misuse of such personal information, financial harm to the affected residents or emotional harm in the case of unknown disclosure. Such a determination must be documented in writing and maintained for at least 5 years. If the incident affects over 500 residents of the commonwealth, the person shall provide the written determination to the office of the attorney general within 10 days after the determination.

(g) The department of consumer affairs and business regulation may promulgate regulations interpreting and applying this section.