

Bill Number: H. 93

Title: An Act relative to protecting sensitive information from security breaches

Lead Sponsor: Representative Tram Nguyen

Hearing Date: April 9, 2025

Report Date: June 8, 2025

MGL Chapter: Amends Section 1 of Chapter 93H (Security Breaches)

Current Law:

- **M.G.L. Chapter 93H** outlines the requirements for notification for data breaches.
- **M.G.L. Chapter 93H § 1** defines “personal information,” among other terms.
- **M.G.L. Chapter 93H § 2** establishes regulatory authority to implement the chapter in various agencies.
- **M.G.L. Chapter 93H § 3** requires data holders and processors to report known security breaches of their systems.

Executive Summary: Expands and clarifies definitions in Massachusetts’ data breach notification statute, including more comprehensive descriptions of personal information such as biometric, genetic, and health-related data. The bill modifies the requirements for reporting security breaches, mandating that organizations notify residents and relevant authorities when unauthorized access to personal information occurs, with specific guidelines about the content and timing of such notifications. It introduces new categories of sensitive information like specific geolocation data and health insurance information, and specifies that a breach must present a reasonably foreseeable risk of harm to the resident.

Legislative History: Filed as H.76 (2023 - 2024) Referred to AITIC; accompanied to S. 2539

Defines “Personal information” as:

(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.
Includes “Specific geolocation information” as a category of sensitive information that can be breached.