General Law Committee
JOINT FAVORABLE REPORT

Bill No: SB-117 / Bill Status / Public Hearing Testimony
Title: AN ACT CONCERNING BREACHES OF SECURITY INVOLVING ELECTRONIC PERSONAL INFORMATION.
Vote Date: 3/16/2026
Vote Action: Joint Favorable Substitute
PH Date: 2/18/2026
File No.:

Disclaimer: *The following JOINT FAVORABLE Report is prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and does not represent the intent of the General Assembly or either chamber thereof for any purpose.*

SPONSORS OF BILL

General Law Committee per request of Attorney General Tong

REASONS FOR BILL

The General Law Committee raised this bill at the request of the Office of the Attorney General. Its intent is to streamline investigations of massive data breaches in Connecticut. As the bill's main proponent, Attorney General Tong submitted detailed written testimony outlining the bill's provisions and their associated rationale.

SUBSTITUTE LANGUAGE

The substitute language (LCO 3237) responds to public hearing testimony and other stakeholder feedback by making a series of changes to the underlying bill. It addresses concerns regarding the impact of the legislation on small businesses by changing the penalty structure, including adding a requirement that the court consider whether the business is a small business, micro business, or nonprofit. The substitute language incorporates other edits to definitions and required timelines, along with other small changes.

RESPONSE FROM ADMINISTRATION/AGENCY

Attorney General William Tong—As the main proponent of the bill, Attorney General Tong's written testimony explains that the bill intends to update statutory requirements regarding massive data breaches. He writes that incidents involving such breaches have increased over time, and his office is responsible for investigating each one. Attorney General Tong testifies that companies have often withheld forensic reports after data breach events, or they have avoided creating them in the first place in an effort to avoid liability.

This proposal intends to address the most serious data breaches: "massive data breaches," which are defined as those involving the personal information of 100,000 residents or more. If

a massive data breach occurs, the legislation would require a company to prepare a third-party forensic report and to provide it to the Privacy Section on a confidential basis. Attorney General Tong argues that these requirements intend to ensure that his office can efficiently investigate massive data breaches without unnecessary expense to Connecticut residents.

Office of the Consumer Counsel (OCC)--Claire E. Coleman, Consumer Counsel—OCC supports the bill and commends the committee for strengthening consumer data protection as technology advances. OCC recommends expanding the definition of "personal information" to include confidential utility account information, ensuring that customers are notified if such data is exposed. OCC cites an incident in 2025 involving Avangrid, in which 60,000 customers were impacted. Many were not clearly informed that their data had been compromised. OCC argues that expanding the definition would improve transparency and consumer protection.

Requested amendments:

- Strengthen protections for utility consumers by expanding the definition of “personal information” to include confidential utility account information (language included in written testimony).

Department of Emergency Services and Public Protection (DESPP), Ronnell A. Higgins, Commissioner–DESPP submitted written testimony in support of SB 117. They characterize the legislation’s requirements regarding investigation and reporting of massive data breaches as “reasonable and necessary.” DESPP cites increases in crimes related to data breaches as evidence that the legislation is needed. They appreciate the bill’s efforts to increase their access to actionable information regarding criminal activity. Overall, DESPP supports SB 117 because it advances shared public safety goals.

NATURE AND SOURCES OF SUPPORT

Zachary van Luling, Town Councilor, Rocky Hill (co-signed by Miriam Lifshitz-Theroux, Deputy Mayor, Rocky Hill)—These two people testified in support of the bill in their individual capacities. They argue that the bill's requirement to submit forensic reports in the wake of "massive data breaches" is key to oversight, enforcement, and corrective action. They testify that the reporting requirements allow state government to act quickly to protect residents, and they express appreciation for the bill's enforceability and its confidentiality provisions. They urge the committee to support SB 117.

NATURE AND SOURCES OF OPPOSITION

Connecticut Bankers Association (CBA)—Tom Mongellow, President and CEO—CBA testified in opposition to the bill as drafted, arguing that its requirements are inconsistent with federal regulations regarding cybersecurity and data breaches at financial institutions. CBA's written testimony details various rules and regulations impacting how banks and other financial institutions must handle these incidents. Although they oppose the bill, CBA requests if the bill does advance, that it be amended to include an exemption for financial institutions.

Requested amendment: If the bill advances, they ask for an exemption for financial institutions (full details in written testimony).

Connecticut Business and Industry Association (CBIA)—Chris Davis, Vice President of Public Policy—CBIA testified in opposition to SB 117, arguing that it would place new legal, financial, and operational burdens on Connecticut businesses without improving consumer protections. They testify that many small businesses have email lists, point-of-sale entries, and other datasets that, if hacked, would be subject to the bill's requirements. CBIA argues that the reporting requirement could unintentionally put residents' data at further risk. They characterize the fine structure as excessive and ask the committee to decline to move the bill forward.

Connecticut River Valley Chamber of Commerce (CRV Chamber)—Jessica Olander, President—CRV Chamber's testimony echoes the concerns raised in CBIA's testimony.

State Privacy and Security Coalition (SPSC), William Martinez, Counsel—SPSC testified in opposition to SB 117, offering four main points of contention:

- **Duplication/circularity of requirements:** Martinez expresses concern that companies may likely need to perform an internal investigation to determine if the numerical threshold for a "massive data breach" has been met. If they have already begun an internal investigation, he argues that the subsequent requirement to engage a third party investigator is duplicative.
- **90-day timeline:** Martinez testifies that requiring a report to be completed within 90 days can be unrealistic, especially if an investigation requires coordination with law enforcement.
- **Costs and penalties:** Martinez expresses concern that companies are facing large, unexpected costs in the aftermath of a massive data breach. He believes that the cost of a required investigation, along with any penalties, could further strain an organization's resources.
- **Overlap and/or conflict with federal requirements:** Martinez testifies that many industries are already subject to specific regulatory requirements pertaining to cybersecurity; adding additional requirements could unintentionally weaken protections for residents.

Requested amendment: If the bill advances, remove subsection (i)'s mandatory forensic reporting requirements and associated penalties.

Monique Ferraro testified in strong opposition to SB 117, arguing that the Attorney General does not need to know the details of a forensic investigation of a data breach interest. She states that this information cannot be used to create a security plan that would better protect Connecticut residents. Ferraro characterizes the proposal as "a thinly veiled attempt to subvert attorney/client privilege." She cautions that in collecting information about security incidents, the Office of the Attorney General could then become an attractive target for malicious actors.

TechNet—Chris Gilrein, Executive Director, Northeast—TechNet testified in opposition to SB 117, expressing particular concern about the bill's numerical threshold for a "massive data breach." TechNet also argues that the bill's 90-day timeline is too strict and does not account for potential delays related to law enforcement investigations. They argue that an organization's resources would be put to better use finding the cause of a breach or restoring services to users.

Insurance Association of Connecticut—Brooke Foley, General Counsel—The Insurance Association of Connecticut opposes SB 117, submitting an argument similar to the one made by CBA. They state that insurers are already subject to extensive federal rules and regulations and should therefore be exempt from the bill's requirements.
Requested amendment: If the bill advances, they are requesting an exemption for the insurance industry.

GENERAL COMMENTS

American Property Casualty Insurance Association (APCIA)—Kristina Baldwin, Vice President—APCIA filed its testimony as general commentary, but it expressed substantially similar concerns to those raised by the Insurance Association of Connecticut. APCIA makes a similar request to exempt the insurance industry if the bill does move forward.
Requested amendment: If the bill advances, they request an exemption for insurers.

Connecticut Association of Health Plans (CTAHP)–Susan Halpin—CTAHP makes an argument that is similar to the ones made by the Insurance Association of Connecticut and APCIA. Their testimony goes into further detail regarding the cybersecurity requirements to which HIPPA-covered entities are already subject. Consequently, CTAHP requests a similar exemption for HIPAA-covered entities.
Requested amendment: Include an exemption for HIPAA-covered entities. (Full language included in written testimony.)

Connecticut Hospital Association (CHA)—CHA provided commentary on SB 117, with a focus on providing a series of technical amendments with the intent of improving the bill.
Requested amendments:

- **Avoid unintentional implication of wrongdoing** by adding clarifying language to the bill. (Full language included in written testimony.)
- State that when an organization reports a "massive data breach," **they are permitted to work with the third-party investigator** and otherwise review the event. (Full language included in written testimony.)
- **Clarify whether a law enforcement hold is applicable (or not)** when reporting a “massive breach of security.”
- **Perform a cost-benefit study** of applying these reporting requirements to HIPAA-covered entities.

New England Connectivity and Telecommunications Association (NECTA)—Anna Lucey, Executive Vice President, External Affairs—NECTA comments that the bill's proposed requirements are novel and may be duplicative. They request that the committee amend the bill's language to allow for consideration of the “specific technical nature of the incident” before its investigative framework applies.

LeadingAge Connecticut and Rhode Island—Mag Morelli, President—Leading Age notes that they appreciate the bill's intent to improve security practices, but they characterize the bill's requirements as "overly burdensome," particularly for HIPAA-covered entities.

Reported by: Betsy Francolino **Date: March 23, 2026**