

Banking Committee JOINT FAVORABLE REPORT

Bill No: HB-5210 / [Bill Status](#) / [Public Hearing Testimony](#)

AN ACT ESTABLISHING VARIOUS DATA SECURITY REQUIREMENTS
Title: APPLICABLE TO CERTAIN FINANCIAL INSTITUTIONS.

Vote Date: 3/10/2026

Vote Action: Joint Favorable Substitute

PH Date: 2/24/2026

File No.: 3000

***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:

Banking Committee

REASONS FOR BILL:

To create new data security requirements for financial institutions in the state. This is intended to increase response times from financial institutions who are affected by security compromises and ensure customers affected by data breaches are informed quickly in the event of such.

SUBSTITUTE LANGUAGE:

Clarified definitions.

RESPONSE FROM ADMINISTRATION/AGENCY:

N/A

NATURE AND SOURCES OF SUPPORT:

N/A

NATURE AND SOURCES OF OPPOSITION:

David Reed, General Counsel, Receivables Management Association International opposes HB5210. HB5210 fails to define "data security incident" and recommends "data security" incident be replaced with "breach of security, as defined in section 36a-701b(a)(1)." RMAI also notes how HB5210 conflicts with Connecticut data breach statute. This will cause HB5210 to be too burdensome, duplicative, and conflicting as well as the three-business day-

limit being too strict to conduct forensic analysis. RMAI recommends replacing subsection (c) lines 26-33 and amending Conn. Gen. Stat. § 36a-701b(b)(2)(A) to include "(2) If notice of a breach of security is required by subdivision (1) of this subsection: (A) The person who owns, licenses or maintains computerized data that includes personal information, shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General, and to the Department of Banking if such person is a licensee under Title 36a."

COMMENTS:

Tom Mongellow, President and CEO, Connecticut Bankers Association (CBA) submits concerns regarding HB5210 as it will require banks in Connecticut to adopt a written information security program for the protection of consumer security, confidentiality, and integrity. The bill also requires Connecticut-chartered banks, and federally chartered banks headquartered in the state, to file a written report with the Department of Banking within three business days of learning or having reason to know of a data security incident that involves a consumer's personal information. Although the CBA appreciates the Department of Banking support for security systems, they suggest refining provisions to be closer to federal rules on data security incidents.

Reported by: Giovanni DeSantis

Date: March 11th, 2026