House of Representatives

General Assembly

File No. 133

February Session, 2026

Substitute House Bill No. 5210

House of Representatives, March 24, 2026

The Committee on Banking reported through REP. DOUCETTE of the 13th Dist., Chairperson of the Committee on the part of the House, that the substitute bill ought to pass.

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

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Section 36a-44a of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) As used in this section:

(1) "Data security incident" means any unauthorized access to or unauthorized acquisition, destruction or corruption of electronic files, media, databases or computerized data containing (A) personal information of an individual, or (B) supervisory, financial, operational or business information of any (i) licensee under this title, (ii) Connecticut bank, or (iii) Connecticut credit union;

(2) "Financial institution" has the same meaning as provided in Section 509 of the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809, and the regulations promulgated thereunder, as said

act and such regulations may be amended from time to time; and

(3) "Personal information" has the same meaning as provided in section 36a-701b.

(b) Each financial institution that is a bank, a Connecticut credit union, a federal credit union, an out-of-state bank that maintains a branch in this state, an out-of-state trust company or out-of-state credit union that maintains an office in this state **[**,**]** or a licensee under this title, **[**or any**]** and each person subject to the jurisdiction of the commissioner under title 36b, shall (1) adopt, in writing, a program setting forth standards for developing, implementing and maintaining reasonable data security safeguards to protect the security, confidentiality and integrity of customer information, and (2) comply with all provisions of Subtitle A of Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6801 et seq., and the regulations promulgated thereunder that apply to such financial institution **[**, except to**]** or person, including, but not limited to, the applicable provisions of 12 CFR Part 364, Appendix B, 12 CFR Part 748, Appendix A and 16 CFR Part 314, as said act and such regulations may be amended from time to time. To the extent that this **[**section**]** subsection is inconsistent with the provisions of sections 36a-41 to 36a-44, inclusive, **[**in which case**]** the provisions that afford the customer greater protection shall control. **[**For purposes of this section, "financial institution" has the meaning given to that term in Section 509 of the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809, and the regulations promulgated thereunder.**]**

(c) Each licensee under this title, Connecticut bank and Connecticut credit union shall file a notification with the Department of Banking, in a form and manner prescribed by the Banking Commissioner, not later than three business days after such licensee, Connecticut bank or Connecticut credit union knows, or has reason to know, of the occurrence of any data security incident that may (1) materially impact its ability to operate in a safe and sound manner or comply with applicable laws and regulations, (2) cause significant disruption in

customer services, or (3) involve any unauthorized access to the personal information of any individual.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2026*	36a-44a

BA *Joint Favorable Subst.*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact: None

Municipal Impact: None

Explanation

The bill, which requires certain financial institutions to adopt data security safeguards and to notify the Department of Banking of certain data security incidents, results in no fiscal impact to the state as the department has sufficient resources to receive the notifications.

OLR Bill Analysis

sHB 5210

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

SUMMARY

This bill requires the following entities and individuals to adopt written programs with standards on developing, implementing, and maintaining reasonable data security safeguards to protect the security, confidentiality, and integrity of customer information: banks, Connecticut credit unions, federal credit unions, out-of-state banks with a branch in Connecticut, out-of-state trust companies or credit unions with an office in Connecticut, licensees under Connecticut banking law, and those who are subject to the Department of Banking's (DOB) jurisdiction under Connecticut securities law. Under the bill, to the extent that this requirement conflicts with existing state law on financial records disclosure, the provisions giving customers the greater protection control.

The bill also requires DOB licensees and Connecticut banks and credit unions to notify the department within three business days after they know, or have reason to know, of certain data security incidents. The reporting requirement is triggered by any incident that may (1) materially impact the ability to operate safely and soundly or comply with applicable laws and regulations, (2) significantly disrupt customer services, or (3) involve unauthorized access to an individual's personal information (see BACKGROUND).

Under existing law, the same entities and individuals that the bill requires to adopt a written program on protecting customer information must comply with the financial privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999 and associated regulations

(see BACKGROUND). The bill specifies that this includes required compliance with the applicable provisions of three associated federal regulations on standards for developing, implementing, and maintaining safeguards to protect customer information.

Lastly, the bill makes technical and conforming changes.

EFFECTIVE DATE: October 1, 2026

DATA SECURITY INCIDENT

Under the bill, a "data security incident" is unauthorized access to or unauthorized acquisition, destruction, or corruption of certain electronic files, media, databases, or computerized data. The files, media, databases, or data involved must have either (1) an individual's personal information or (2) a DOB-licensee's or Connecticut bank's or credit union's supervisory, financial, operational, or business information.

BACKGROUND

Gramm-Leach-Bliley Financial Modernization Act of 1999

Subtitle A of Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999 limits the circumstances under which a financial institution can disclose a consumer's nonpublic personal information to nonaffiliated third parties. It also requires financial institutions to disclose to their customers the institution's financial privacy policies and practices with respect to affiliated and nonaffiliated parties (15 U.S.C. § 6801 et seq.).

Personal Information

By law, "personal information" is a person's first name or initial and last name, combined with at least one of the following:

1. driver's license or state identification card number;

2. government-issued identification number that is commonly used to verify identity, such as a Social Security, taxpayer identification, passport, or military identification number;

3. credit or debit card number;

4. financial account number, with other information that would give account access;

5. information about the person's medical history, mental or physical condition, or medical treatment or diagnosis;

6. health insurance policy number or subscriber identification number, or any unique identifier a health insurer uses to identify the person;

7. biometric data generated by electronic measurements of the person's unique physical characteristics used to authenticate or determine identity (for example, fingerprint, voice print, or eye image); or

8. precise geolocation data.

It also includes a person's username or email address, combined with a password or security question and answer that would allow access to an online account (breach of login credentials) (CGS § 36a-701b).

COMMITTEE ACTION

Banking Committee

Joint Favorable Substitute
Yea 13 Nay 0 (03/10/2026)