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)