General Law Committee
JOINT FAVORABLE REPORT

Bill No.: SB-137
Title: AN ACT CONCERNING DATA PRIVACY BREACHES.
Vote Date: 3/10/2020
Vote Action: Joint Favorable Substitute
PH Date: 2/25/2020
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:

The General Committee

REASONS FOR BILL:

To expand the data privacy breach notification statute to protect consumers.

RESPONSE FROM ADMINISTRATION/AGENCY:

Attorney General William Tong State of Connecticut: Attorney General William Tong expressed support for Senate Bill 137 as it updates Connecticut's breach notification statute. It also strengthens consumer protections by broadening the definition of "personal information," shortening the time period to notify consumers and the Office of the Attorney General of a security breach from 90 to 30 days, and by improving notification procedures for security breaches involving the compromise of online account credentials. Connecticut's current definition of "personal information" covers some of the most sensitive personal identifiers, including Social Security numbers and financial account information. To ensure that our data breach notification statute is effective in protecting Connecticut residents against identity theft, the definition of "personal information" must be broadened to include additional categories of sensitive information. It must also be versatile enough to respond to new types of technology capable of exposing individuals to identity theft.

NATURE AND SOURCES OF SUPPORT:

The Credit Union League of Connecticut expressed support for SB 137 because it will a piece of legislation that holds businesses with access to consumer data accountable to the same data security and notification standards as credit unions and other financial institutions. SB 137 will be placing responsibility and accountability for costs resulting from data breaches on the businesses that cause them makes common sense.

ACLU Connecticut expressed support for SB 137 which amends existing state law regarding data breaches to include additional categories of information, including taxpayer numbers, passport numbers, military ID numbers, medical information, and biometric information, when in conjunction with name; as well as usernames and email addresses in conjunction with a password or security question. We appreciate this Committee's efforts to accomplish this via Senate Bill 137. This bill, however, should clarify that the data breach requirements are imposed equally on state and local governments and agencies as they are on other people who maintain digital personal information.

NATURE AND SOURCES OF OPPOSITION:

Kathleen Silard President & CEO Stamford Health expressed opposition to SB 137. In regards to the medical information, Hospitals and other healthcare providers are currently subject to breach notifications relating to the improper disclosure of personal health information under the federal Health Insurance Portability and Accountability Act (HIPAA). These comprehensive regulations require healthcare providers such as hospitals to provide breach notification to affected individuals, the U.S. Health and Human Services Secretary and in some cases to the media. Stamford Health is in compliance with these federal requirements and remains committed to protecting our patients' privacy. It is unclear how an additional, state requirement for a provider to notify individuals would assist the individuals and doing so may create confusion. For these reasons, we urge you to not extend the current breach notification requirements to healthcare providers.

Connecticut Hospital Association opposes SB 137 as written. SB 137 seeks to clarify data breach reporting requirements that were expanded during the 2019 legislative session and inserted into the budget bill, which became Public Act 19-177. The 2019 changes, which are repeated in SB 137 in a more comprehensive format than in the 2019 version add categories of data to the banking title's chapter 669 that would trigger a reporting obligation and consumer notifications. HIPAA covered both healthcare providers and health insurers, and their business associates should be exempt from the reporting requirements of section 36a-701b because HIPAA and HITECH already include significant security and breach compliance requirements. State law should not apply this state banking law to healthcare entities that already must follow long-standing HIPAA reporting obligations designed specifically for the healthcare industry and healthcare consumers.

Reported by: Jeff Lucas **Date: 3/20/20**