Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Connecticut

Conn. Gen. Stat. § 36a-701b

S.B. 650 (signed into law June 8, 2005, Public Act 05-148)

Effective January 1, 2006

H.B. 6001 (signed into law June 15, 2012, Public Act 12-1)

Effective October 1, 2012

S.B. 949 (signed into law June 11, 2015)

Effective Oct. 1, 2015

S.B. 472 (signed into law June 4, 2018)

Effective October 1, 2018

H.B. 5310 (signed into law June 16, 2021)

Effective October 1, 2021

S.B. 1058 (Signed into law June 26, 2023)

Effective October 1, 2023

Application. Any person (Entity) that owns, licenses, or maintains computerized data that includes PI of Connecticut residents.

Security Breach Definition. Unauthorized access to or acquisition of electronic files, media, databases, or computerized data containing PI when access to the PI has not been secured by encryption or by any other method or technology that renders the PI unreadable or unusable.

Notification Obligation. An Entity to which the statute applies shall disclose any breach of security following the discovery of the breach to any CT resident whose PI was breached or is reasonably believed to have been breached.

- Notification is not required if, after an appropriate investigation the Entity reasonably determines that the breach will not likely result in harm to the individuals whose PI has been acquired or accessed.

Notification Obligation to Attorney General. Any Entity that is required under the statute to notify CT residents of any breach of security shall provide notice of the breach of security to the Attorney General not later than the time notice is provided to the residents.

Third-Party Data Notification. If an Entity maintains PI that the Entity does not own, the Entity shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery if the PI was, or is reasonably believed to have been, breached.

Timing of Notification. The disclosure shall be made without unreasonable delay, but not later than 60 days after the discovery of such breach, unless a shorter time is required under federal law, consistent with any measures necessary to determine the nature and scope of the breach, to identify individuals affected, or to restore the reasonable integrity of the data system.

- If additional residents whose information has been breached or reasonably believed to be breached is identified more than 60 days after discovery, the Entity shall notify as expediently as possible.

Personal Information Definition.

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number;
- Driver's license number or state identification card number;
- Credit card number, or debit card number; or
- Financial account number, in combination with any required security code, access code, or password that would permit access to such financial account.
- Taxpayer identification number;
- Identity protection personal identification number issued by the IRS;
- Passport number, military identification number or other identification number issued by the government that is commonly used to verify identity;
- Medical information regarding individual medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
- Health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual;
- Biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image
- Precise geolocation data.

OR

(2) username or email address in combination with a password or security question and answer that would permit access to an online account (name not required).

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Notice Required. Notice may be provided by one of the following methods:

Generally:

- Written notice;
- Telephonic notice; or
- Electronic notice; provided it is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Online account credentials: Notice may be provided in electronic or other form directing the resident to promptly change any password or security question or to take other appropriate steps to protect the affected

online account and all other online accounts for which the resident uses the same username or email address and password or security question and answer.

Email account credentials: An Entity that furnishes an email account shall not provide notice to the email account that was breached if the Entity cannot reasonably verify the affected person's receipt of that notification. In such event, notice should be provided by another method described in this section or clear and conspicuous notice delivered to the resident when they are online and connected to the account from an IP address or online location from which the person knows the resident customarily accesses the account.

Credit Monitoring Services: The Entity who owns or licenses the affected PI shall offer to each resident whose Social Security number or taxpayer identification number was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than 24 months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

Substitute Notice Available. If the Entity demonstrates in the notice to the AG that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000 persons, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has email addresses for the affected persons;
- Conspicuous posting of the notice on the website of the Entity, if the Entity maintains one; and
- Notification to major statewide media, including newspapers, radio and television.

Exception: Own Notification Policy. Any Entity that maintains its own security breach procedures as part of an information security policy for the treatment of PI and otherwise complies with the timing requirements of the statute shall be deemed to be in compliance with the security breach notification requirements of the statute, provided such Entity notifies subject persons in accordance with its policies in the event of a breach of security.

Exception: Compliance with Other Laws.

- **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance.
- **HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH).** Compliance with HIPAA and HITECH is deemed compliance with the statute, provided that the Entity provides notice to the state Attorney General no later than when notice is provided to residents and offers identity theft protection to those whose Social Security Number or taxpayer identification number was breached.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed for a reasonable period of time if a law enforcement agency determines that the notice will impede a criminal investigation and such law enforcement agency has made a request that notification be delayed. Notice required by the statute must be made after the law enforcement agency determines that notification will no longer impede the investigation and so notifies the Entity of such determination.
- **Attorney General Enforcement.** The Attorney General may seek direct damages and injunctive relief. Any civil penalties collected for failure to comply may be deposited into the privacy protection guaranty and enforcement account.
- **Public Disclosure Exception.** All documents, materials, and information provided in response to an investigative demand issued pursuant to section 42-110d(c) shall be exempt from public disclosure under

section 1-210(a) provided the Attorney General may make such documents, materials or information available to third parties in furtherance of such investigation.