Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Rhode Island

R.I. Gen. Laws § 11- 49.3-4 ***et seq.***

H.B. 5684 signed into law June 27, 2023

Effective June 27, 2023

Application. A municipal agency, state agency, individual, business or legal entity (collectively, Entity) that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes PI.

Security Breach Definition. Unauthorized access or acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.
- Note that the notification obligation applies to a breach of security of the system ***or*** any disclosure of PI.

Notification Obligation. Any Entity to which the statute applies shall provide notification of (i) any disclosure of PI ***or*** (ii) any breach of the security of the system, that poses a significant risk of identity theft to any resident of RI whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person or entity.

- Where affected employees are represented by a labor union through a collective bargaining agreement, a state or municipal agency employer shall also notify the collective bargaining agent of the breach.

Attorney General Notification. If more than 500 RI residents are to be notified, the Entity shall notify the Attorney General as to the timing, content, and distribution of the notices and the approximate number of affected individuals.

- State and municipal agencies must also report cybersecurity incidents to the RI state police within 24 hours.

Credit Reporting Agency Notification. In the event that more than 500 RI residents are to be notified, the Entity shall notify the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals.

Timing of Notification. The notification shall be made in the most expedient time possible but no later than 45 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements and shall be consistent with the legitimate needs of law enforcement.

For state and municipal Entities, notice must be given no later than 30 calendar days.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or are in hard copy paper format:

- Social Security number;
- Driver's license number, state identification card number, or tribal identification number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, password, or personal identification number that would permit access to an individual's financial account;
- Medical or health insurance information; or
- Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

"Encrypted" means the transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data shall not be considered encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data.

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

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

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

The notification to individuals must include the following information to the extent known:

- A general and brief description of the incident, including how the security breach occurred and the number of affected individuals;
- The type of information that was subject to the breach;
- The date of breach, estimated date of breach, or the date range within which the breach occurred;
- The date that the breach was discovered;
- A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact (i) credit reporting agencies; (ii) remediation service providers; and (iii) the Attorney General; and
- A clear and concise description of the consumer's ability to file or obtain a police report, how the consumer can request a security freeze and the necessary information to be provided when requesting the security freeze, and any fees that may be required to be paid to the consumer reporting agencies.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $25,000, or that the affected class of subject persons to be notified exceeds 50,000, 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 subject persons;
- Conspicuous posting of the notice on the Entity's website if the Entity maintains one; and
- Notification to major statewide media.

Credit Monitoring Services. State and municipal Entities must provide remediation services for five years for adults 18 years and older, and up to the age of 18 and not less than two years for those under 18.

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, provided such Entity notifies subject persons in accordance with such Entity's policies in the event of a breach of security.

Exception: Compliance with Other Laws.

- **Compliance with Primary Regulator.** Any Entity that maintains a security breach procedure pursuant to the rules, regulations, procedures, or guidelines established by the primary or functional regulator shall be deemed to be in compliance with the security breach notification requirements of this section, provided such Entity notifies subject persons in accordance with the policies or the rules, regulations, procedures, or guidelines established by the primary or functional regulator in the event of a breach of security of the system.
- **Interagency Guidance.** A financial institution, trust company, credit union, or its affiliates that is subject to and examined for and found in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter.
- **HIPAA-Covered Entities.** A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.

Penalties. Each reckless violation is a civil violation for which a penalty of not more than $100 per record may be adjudged against a defendant. Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than $200 per record may be adjudged against a defendant. Whenever the Attorney General has reason to believe that a violation has occurred and that proceedings would be in the public interest, the Attorney General may bring an action in the name of the state against the business or person in violation.

Other Key Provisions:

- **Delay for Law Enforcement.** The notification required by this section may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation. The law enforcement agency must notify the Entity of the request to delay notification without unreasonable delay. If notice is delayed due to such determination, then as soon as the law enforcement agency determines and informs the Entity that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable. The Entity shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided, however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.
- Waiver Not Permitted.