Publications
June 01, 2014

# SECURITY BREACH NOTIFICATION CHART - Hawaii

**H.R.S. § 487N-1** ***et seq.***

S.B. 2290 (signed into law May 25, 2006, Act 135)

Effective January 1, 2007

S.B. 2402 (signed into law April 17, 2008, Act 19)

Effective April 17, 2008

---

**Application.** Any commercial or legal entity, or any government agency that collects PI for specific government purposes (collectively, Entity) that owns or licenses PI of residents of HI in any form (whether computerized, paper, or otherwise).

**Security Breach Definition.** Any unauthorized access to and acquisition of unencrypted or un-redacted records or data containing PI where illegal use of the PI has occurred, or is reasonably likely to occur, where such unauthorized access and acquisition creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing PI along with the confidential process or key constitutes a security breach.

- Good-faith acquisition of PI by an employee or agent of the Entity for a legitimate purpose is not a security breach, provided that the PI is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

**Notification Obligation.** An Entity shall provide notice to the affected person of a security breach following discovery or notification of the breach.

**Attorney General/Agency Notification.** If more than 1,000 persons are notified at one time under this section, the business shall notify the State of Hawaii's Office of Consumer Protection of the timing, content, and distribution of the notice.

**Notification to Consumer Reporting Agencies.** If more than 1,000 persons are notified at one time pursuant to this section, the Entity shall notify in writing, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.

**Notification Obligation for Government Agencies.** A government agency shall submit a written report to the legislature within 20 days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring. In the event that a law enforcement agency informs the government agency that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may

be delayed until 20 days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

**Third-Party Data Notification.** Any business located in HI or any business that conducts business in HI that maintains or possesses records or data containing PI of residents of HI that the business does not own or license, shall notify the owner or licensee of the PI of any security breach immediately following discovery of the breach.

**Timing of Notification.** Without unreasonable delay, consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system.

**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:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number, credit card number, debit card number, access code, or password that would permit access to an individual's financial account.

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 one of the following methods:

- Written notice to the last available address the Entity has on record;
- Telephonic notice, provided that contact is made directly with the affected persons; or
- Email notice, for those persons for whom an Entity has a valid email address and who have agreed to receive communications electronically 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 notice shall be clear and conspicuous and shall include a description of the following:

- The incident in general terms;
- Type of PI subject to the unauthorized access and acquisition;
- The general acts of the Entity to protect the PI from further unauthorized access;
- A telephone number that the person may call for further information and assistance, if one exists; and
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

**Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of persons to be notified exceeds 200,000, or if the Entity does not have sufficient contact information or consent to satisfy the required notice, for only those affected persons without sufficient contact information or consent, or if the Entity is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all 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.

**Exception: Compliance with Other Laws.**

- **Federal Interagency Guidance.** A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance.
- **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.** Any Entity that violates any provisions of the statute is subject to penalties of not more than $2,500 for each violation.

**Other Key Provisions:**

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the Entity documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice shall be provided without unreasonable delay after the law enforcement agency communicates to the Entity its determination that notice will no longer impede the investigation or jeopardize national security.
- Attorney General Enforcement.
- Waiver Not Permitted.