Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Washington

Wash. Rev. Code § 19.255.010 *et seq.*, § 42.56.590

S.B. 6043 (signed into law May 10, 2005, Chapter 368)

Effective July 24, 2005

H.B. 1149 (signed into law March 22, 2010) requiring reimbursement from payment processors, businesses, and vendors to financial institutions for the cost of replacing credit and debit cards after a breach

Effective July 1, 2010

H.B. 1078 (signed into law April 23, 2015)

Effective July 24, 2015

H.B. 1071 (signed into law May 7, 2019)

Effective March 1, 2020

Application. Any state or local agency or any person or business which conducts business in WA (collectively, Entity) that owns or licenses computerized data that includes PI.

Security Breach Definition. Unauthorized acquisition of 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 when the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system to any resident of WA whose PI was, or is reasonably believed to have been, acquired by an unauthorized person and the PI was not "secured" (i.e., encrypted in a manner that meets or exceeds the National Institute of Standards and Technology (NIST) standard or is otherwise modified so that the PI is rendered unreadable, unusable, or undecipherable by an unauthorized person).

- Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured PI must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured PI was acquired by an unauthorized person.

Attorney General Notification. Any Entity that is required to issue a notification to more than 500 WA residents as a result of a single breach shall, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. The Entity shall also provide to the Attorney General the following information:

- The number of WA consumers affected by the breach, or an estimate if the exact number is not known;

- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- A timeframe of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
- A summary of steps taken to contain the breach.

The notice to the attorney general must be updated if any of the information identified above is unknown at the time the notice is due.

Third-Party Data Notification. Any Entity that maintains computerized data that includes PI that the Entity does not own shall notify the owner or licensee of the PI of any breach immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure to affected consumers and to the Attorney General shall be made in the most expedient time possible and without unreasonable delay, no more than 30 calendar days after the breach was discovered, unless the delay is at the request of law enforcement or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

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, when either the name or the data elements are not encrypted:

- Social Security number;
- Driver's license number or state identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account.
- Full date of birth;
- Private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- Student, military, or passport identification number;
- Health insurance policy number or health insurance identification number;
- Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or
- Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;

(2) Username or email address in combination with a password or security questions and answers that would permit access to an online account; and

(3) Any of the data elements or any combination of the data elements described in (1) above, without the consumer's first name or first initial and last name if the data element or combination of data elements would enable a person to commit identity theft against a consumer.

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

For government agencies subject to RCW 42.56.590 only, the last four digits of a social security number is included in the definition of personal information.

Notice Required. Notice may be provided by 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 must be written in plain language and must include, at a minimum, the following information:

- The name and contact information of the reporting person or business subject to this section;
- A list of the types of PI that were or are reasonably believed to have been the subject of a breach;
- A timeframe of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed PI.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, 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; or

If the breach of the security of the system involves personal information including a username or password, notice may be provided electronically or by email. If the breach involves login credentials of an email account furnished by the Entity, notice may be provided using another method; not to that email address.

The notice must inform the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the Entity and all other online accounts for which the person uses the same username or email address and password or security question or answer.

Exception: Compliance with Other Laws.

- **Certain Financial Institutions.** A financial institution under the authority of the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, or the Federal Reserve system is deemed to have complied with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on the effective date of this section. The entity shall comply with the Attorney General notification requirements here in addition to providing notice to its primary federal regulator.
- **HIPAA-Covered Entities**. A covered entity under Health Insurance Portability and Accountability Act of 1996 (HIPAA) is deemed to have complied with respect to protected health information if it has complied with section 13402 of the federal Health Information Technology for Economic and Clinical Health Act, Public Law 111-5. Covered entities must notify the Attorney General in compliance with the timeliness of

notification requirements of the aforementioned section 13402, notwithstanding the timing of notification requirements here.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the Entity notifies subject persons in accordance with its policies in the event of a breach of security.

Other Key Provisions:

- **Delay for Law Enforcement.** Notification may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The required notification shall be made after the law enforcement agency determines that it will not compromise the investigation.
- **Attorney General Enforcement.** The Attorney General may bring action on behalf of the state or its residents. The violations are "unfair or deceptive act" and "unfair method of competition."
- **Private Right of Action.** Any consumer injured by a violation of this section may institute a civil action to recover damages.
- Waiver Not Permitted.

Reimbursement from Businesses to Financial Institutions. In the event of a breach where an Entity held unencrypted account information or was not Payment Card Industry Data Security Standard compliant, payment processors, businesses, and vendors can be liable to a financial institution for the cost of reissuing credit and debit cards in the event of a breach that results in the disclosure of the full, unencrypted account information contained on an identification device, or the full, unencrypted account number on a credit or debit card or identification device plus the cardholder's name, expiration date, or service code.