Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Florida

Fla. Stat. § 501.171

S.B. 1524 (signed into law June 20, 2014)

Effective July 1, 2014

S.B. 1526 (signed into law June 20, 2014)

Effective July 1, 2014

*S.B. 262 (signed into law June 6, 2023)

Effective July 1, 2024

Application. A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses PI (collectively, Entity).

- For notice requirements, Entity includes governmental entities.

An entity that has been contracted to maintain, store, or process PI on behalf of an Entity or governmental entity ("Third-Party Agent").

Security Breach Definition. The unauthorized access of data in electronic form containing PI.

- Good-faith access of PI by an employee or agent of the Entity is not a breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Notification to Individuals. An entity must give notice to each individual in Florida whose PI was, or the Entity reasonably believes to have been, accessed as a result of the breach.

Notice to affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the Entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose PI has been accessed. Such a determination must be documented in writing and maintained for at least 5 years

Attorney General Notification. Entity must provide notice to the Department of Legal Affairs (Department) of any breach of security affecting 500 or more individuals in FL. Written notice must include:

- A synopsis of the events surrounding the breach at the time notice is provided.
- The number of individuals in FL who were or potentially have been affected by the breach.
- Any services related to the breach being offered or scheduled to be offered, without charge, by the Entity to individuals, and instructions as to how to use such services.
- A copy of the notice required to affected individuals or an explanation of the other actions taken to give notice to affected individuals.

- The name, address, telephone number, and email address of the employee or agent of the Entity from whom additional information may be obtained about the breach.

Upon the Department's request, the Entity must provide the following information to the Department:

- A police report, incident report, or computer forensics report.
- A copy of the policies in place regarding breaches.
- Steps that have been taken to rectify the breach.

Notification to Consumer Reporting Agencies. If notice is required to more than 1,000 FL residents, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

Third-Party Data Notification. Any third-party agent shall disclose to the Entity for which the information is maintained any breach of the security of the system as soon as practicable, but no later than 10 days following the determination of the breach or reason to believe the breach occurred. Upon receiving notice from a third-party agent, the Entity for which the information is maintained shall provide notices to the Department and Affected Individuals. A third-party agent must provide the Entity with all information that the Entity needs to comply with notice requirements. A third-party agent may provide notice to the Department or Affected Individuals on behalf of the Entity; however, a third-party agent's failure to provide proper notice shall be deemed a violation against the Entity.

Timing of Notification.

- **To the Department:** Notice must be provided as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred.
- **To the Affected Individuals:** Notice must be made as expeditiously as practicable and without unreasonable delay, but no later than 30 days after the determination of a breach or reasons to believe a breach occurred, taking into account the time necessary to allow the Entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached. The Entity may receive 15 additional days to provide notice to Affected Individuals if good cause for delay is provided in writing to the Department within 30 days after determination.

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 for that individual:
    - Social Security number;
    - Driver's license or state identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
    - Financial account number or credit or debit card number in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
    - Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
    - Health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
    - **[as of July 1, 2024]** An individual's biometric information or genetic information; or
    - **[as of July 1, 2024]** Any information regarding an individual's geolocation.

- A username or email address, in combination with a password or security question and answer that would permit access to an online account.

PI does not include publicly available information that is made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

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

- Written notice sent to the mailing address of the individual in the records of the Entity; or
- Email notice sent to the individual's email address in the Entity's records.

Notice must contain, at a minimum:

- The date, estimated date, or estimated date range of the breach.
- A description of the PI that was accessed or reasonably believed to have been accessed as a part of the breach.
- Information that the individual can use to contact the Entity to inquire about the breach and the PI that the Entity maintained about the individual.

Substitute Notice to Affected Individuals Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, 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 both of the following:

- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and
- Notification in print and to broadcast media, including major media in urban and rural areas where the Affected Individuals reside.

Penalties. An Entity that violates the statute in the following manner is subject to the following administrative fines:

- A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the Department against an Entity or third-party agent.
- An Entity that fails to notify the Department or Affected Individuals shall be liable for a civil penalty not to exceed $500,000 (i) in the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion therefore for up to 180 days; or (ii) if the violation continues for more than 180 days, in an amount not to exceed $500,000. The civil penalties under this paragraph apply per breach, and not per individual affected by the breach.

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.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice to Individuals may be delayed for a specified period that the law enforcement agency determines is reasonably necessary in a written request if a law enforcement agency determines that the notice will impede a criminal investigation. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period specified in the

original request made to a specified date if further delay is necessary.

- **Public Records Exemption.** All information received by the Department pursuant to the notification requirements or pursuant to a law enforcement or Department investigation is confidential and exempt from the Public Records requirement under the State Constitution and statutes.
- **No Private Cause of Action.** There is no private cause of action.