Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Utah

Utah Code §§ 13-44-101, *et seq.*

S.B. 69 (signed into law March 20, 2006, Session Law Chapter 343)

Effective January 1, 2007

S.B. 208 (signed into law March 30, 2009)

Effective May 12, 2009

S.B. 193 (signed into law March 26, 2019)

Effective May 14, 2019

S.B. 127 (signed into law March 23, 2023)

Effective May 3, 2023

S.B. 98 (signed into law March 19, 2024)

Effective May 1, 2024

Application. Any Entity who owns or licenses computerized data that includes PI concerning a UT resident.

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

- Does not include the acquisition of PI by an employee or agent of the Entity possessing unencrypted computerized data unless the PI is used for an unlawful purpose or disclosed in an unauthorized manner.

Notification Obligation. If investigation reveals that the misuse of PI for identity theft or fraud has occurred, or is reasonably likely to occur, the person shall provide notification to each affected UT resident.

- Notification is not required if after a good-faith, reasonable, and prompt investigation the Entity determines that it is unlikely that PI has been or will be misused for identity theft or fraud.

Attorney General Notification. If an Entity must notify 500 or more UT residents, it must also notify the Office of the Attorney General, and the Utah Cyber Center. Notice shall include:

- the date the breach of system security occurred;
- the date the breach of system security was discovered;
- the total number of people affected by the breach of system security, including the total number of Utah residents affected;
- the type of personal information involved in the breach of system security; and

- a short description of the breach of system security that occurred.

Notification to Consumer Reporting Agencies. If an Entity must notify 1,000 or more UT residents, the Entity must also notify each nationwide consumer reporting agency.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall notify and cooperate with the owner or licensee of the PI of any breach of system security immediately following the Entity's discovery of the breach if misuse of the PI occurs or is reasonably likely to occur.

Timing of Notification. Notification shall be provided in the most expedient time possible without unreasonable delay, after determining the scope of the breach of system security and after restoring the reasonable integrity of the system.

Personal Information Definition. A person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person, when either the name or data element is unencrypted or not protected by another method that renders the data unreadable or unusable:

- Social Security number;
- Driver's license number or state identification card number; or
- 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 the person's account.

PI does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.

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

- In writing by first-class mail to the most recent address the Entity has for the resident;
- By telephone, including through the use of automatic dialing technology not prohibited by other law; or
- Electronically, if the Entity's primary method of communication with the resident is by electronic means, or if provided consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Substitute Notice. If notification in the manner described above is not feasible, by publishing notice of the breach of system security in a newspaper of general circulation. Such notice must comply with Utah Code § 45-1-101.

Exceptions:

- **Own Notification Policy.** If an Entity maintains its own notification procedures as part of an information security policy for the treatment of PI the Entity is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the Entity notifies each affected UT resident in accordance with the Entity's information security policy in the event of a breach.
- **Compliance with Other Laws**. An Entity who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the Entity notifies each affected UT resident in accordance with the other applicable law in the event of a breach.
- **Financial Institutions**. This chapter does not apply to a financial institution or affiliate of a financial institution, as defined in 15 U.S.C. § 6809.

Penalties. Violators are subject to a civil fine of no more than $2,500 for a violation or series of violations concerning a specific consumer and no more than $100,000 in the aggregate for related violations concerning more than one consumer. The latter limitation does not apply if the violations concern more than 10,000 Utah residents and more than 10,000 residents of other states, or if the Entity agrees to settle for a greater amount.

Other Key Provisions:

- **Delay for Law Enforcement.** An Entity may delay providing notification at the request of a law enforcement agency that determines that notification may impede a criminal investigation. Notification shall be provided in good faith, without unreasonable delay, and in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.
- Attorney General Enforcement.
- Waiver Not Permitted.
- Records are confidential if reported to the Attorney General or Utah Cyber Center per requirements.