Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Arizona

Ariz. Rev. Stat. § 18-551 *et seq.*

S.B. 1338 (signed into law April 26, 2006, Chapter 232)

Effective December 31, 2006

H.B. 2154 (signed into law April 11, 2018, Chapter 177)

Effective August 3, 2018

H.B. 2146 (signed into law March 29, 2022, Chapter 81)

Effective June 27, 2022

Application. Any person or entity (collectively, Entity) that conducts business in AZ and that owns, maintains, or licenses unencrypted and un-redacted computerized PI.

Security Breach Definition. An unauthorized acquisition of and access that materially compromises the security or confidentiality of unencrypted and un-redacted computerized PI maintained by an Entity as part of a database of PI regarding multiple individuals.

- 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 system if the PI is not used for a purpose unrelated to the Entity or subject to further unauthorized disclosure.

Notification Obligation. Any Entity that owns or licenses the PI shall notify the individuals affected within 45 days after its determination that there has been a security breach.

- An Entity is not required to disclose a breach of the system if the Entity, an independent third-party forensic auditor, or a law enforcement agency, after a reasonable investigation, determines that a breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.

Attorney General Notification. If an Entity is required to notify more than 1,000 AZ residents, the Entity shall notify the Attorney General and the Director of the Arizona Department of Homeland Security, in writing, in a form prescribed by rule or order of the Attorney General, or by providing a copy of the individual notification.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 AZ residents, the Entity shall also notify the three largest nationwide consumer reporting agencies.

Third-Party Data Notification. If an Entity maintains unencrypted and un-redacted computerized PI that the Entity does not own or license, the Entity shall notify, as soon as possible, the owner or licensee of the information, and cooperate with the owner or the licensee of the information. Cooperation shall include sharing information relevant to the breach The Entity that maintains the data under an agreement with the owner or

licensee is not required to provide notice to the individual unless the agreement stipulates otherwise.

Timing of Notification. The disclosure shall be made within 45 days after the Entity's determination that there has been a security breach.

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:

- Social Security number;
- Number on a driver's license issued pursuant to § 28-3166 or number on a nonoperating identification license issued pursuant to § 28-3165;
- Financial account number or credit number or debit card number in combination with any required security code, access code, or password that would permit access to the individual's financial account.
- A private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- An individual's health insurance identification number;
- Information about an individual's medical or mental health treatment or diagnosis by a health care professional;
- Passport number;
- Individual's taxpayer identification number or an identity protection personal identification number issued by the IRS; and
- Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account.

2. An individual's username or email address, in combination with a password or security question and answer, that allows access to an online account.

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

Notice Required.

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

- Written notice;
- Telephonic notice, if made directly with the affected individuals and not through a pre-recorded message; or
- Email notice, if the Entity has email addresses for the individuals subject to the notice.

The notice shall include at least the following:

- The approximate date of the breach;
- Type of PI included in the breach;
- The toll-free telephone numbers and addresses of the three largest credit reporting agencies; and
- The toll-free number, address, and website for the FTC or any federal agency that assists consumers with identity theft matters.

For online account credentials. If the breach involves only online account credentials and no other PI, the Entity may comply with this section by providing the notification in an electronic or other form that directs the individual whose PI has been breached to promptly change their password and security question or answer, as

applicable, or to take other steps that are appropriate to protect the online account and all other online accounts for which the individual uses the same username and email address and password or security question or answer.

For email account credentials. For the breach of credentials to an email account furnished by the Entity, the Entity may comply with this section by providing notification by another method described in this subsection or by providing clear and conspicuous notification delivered to the individual online when connected to the online account from an IP address or online location from which the Entity knows the individual customarily accesses the account. The Entity satisfies the notification requirement with regard to the individual's account with the person by requiring the individual to reset their password or security question and answer for that account, if the person also notifies the individual to change the same password or security question and answer for all other online accounts for which the individual uses the same username or email address and password or security question or answer.

Substitute Notice Available. If the Entity can demonstrate that the cost of providing notice will exceed $50,000 or that the affected class of persons to be notified exceeds 100,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- A written letter to the attorney general that demonstrates the facts necessary for substitute notice;
- Conspicuous posting of the notice on the website of the Entity, if the Entity maintains one.

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.
- **Gramm-Leach-Bliley Act.** The provisions of this statute shall not apply to any Entity who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act.
- **HIPAA-Covered Entities.** The provisions of the statute do not apply to a covered entity or business associate as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or a charitable fund-raising foundation or nonprofit corporation whose primary purpose is to support a specified covered entity, if they comply with applicable provisions of HIPAA.
- **Own Notification Policy.** Any 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 the statute shall be deemed to be in compliance with the notification requirements of the statute if the Entity notifies affected persons in accordance with its policies.

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. Notice required by the statute must be made within 45 days after the law enforcement agency determines that notification will no longer impede the investigation.
- **Attorney General Enforcement.** A knowing and willful violation of this section is an unlawful practice pursuant to ARS 44-1522. The Attorney General may impose a civil penalty for a violation of this article not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed $500,000.