Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Iowa

Iowa Code § 715C.1-2

2007 S.F. 2308 (signed into law May 9, 2008)

Effective July 1, 2008

2014 S.F. 2259 (signed into law April 3, 2014)

Effective July 1, 2014

2018 S.F. 2177 (signed into law April 10, 2018)

Effective July 1, 2018

Application. Any individual, government, legal or commercial entity (collectively, Entity) that owns or licenses computerized data that includes an IA resident's PI that is used in the course of the Entity's business, vocation, occupation, or volunteer activities and that was subject to a breach of security.

Security Breach Definition. Unauthorized acquisition of PI maintained in computerized form by an Entity that compromises the security, confidentiality, or integrity of the PI. Also, unauthorized acquisition of PI maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the PI.

- Good-faith acquisition of PI by an Entity or that Entity's employee or agent for a legitimate purpose of that Entity is not a breach of security, provided that the PI is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the PI.

Notification Obligation. An Entity to which the statute applies shall give notice of the breach of security following discovery, or receipt of notification of such breach, to any IA resident whose PI was included in the information that was breached.

- Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the Entity determines that no reasonable likelihood of financial harm to the IA residents whose PI has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for 5 years.

Attorney General Notification. An Entity required to notify more than 500 IA residents must give written notice to the director of the consumer protection division of the Attorney General's office. Notice or receipt of notice must be provided within 5 business days of giving notice to any consumer.

Third-Party Data Notification. Any Entity who maintains or otherwise possesses PI on behalf of another Entity shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach if an IA resident's PI was included in the information that was breached.

Timing of Notification. The notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with any measures necessary to sufficiently determine contact information for the affected IA residents, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

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 that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, un?redact, or otherwise read the data elements have also been obtained through the breach of security:

- Social Security number;
- Driver's license number or other unique identification number created or collected by a government body;
- 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;
- Account number or credit card number or debit card number in combination with any *required expiration date*, security code, access code, or password that would permit access to an individual's financial account;
- Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

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

Notice Required. Notice shall include, at a minimum, all of the following:

- A description of the breach of security;
- The approximate date of the breach of security;
- The type of PI obtained as a result of the breach of security;
- Contact information for consumer reporting agencies; and
- Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

Notification may be provided by one of the following methods:

- Written notice to the last available address the Entity has in the Entity's records; or
- Electronic notice, if the Entity's customary method of communication with the resident is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, that the affected class of IA residents to be notified exceeds 350,000 persons, or if the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of the following:

- Email notice when the Entity has email addresses for the affected IA residents;
- Conspicuous posting of the notice or a link to the notice on the Entity's website, if the Entity maintains one; and
- Notification to major statewide media.

Exception: Compliance with Other Laws.

- **Federal Regulator.** This statute does not apply to an Entity that complies with notification requirements or breach of security procedures that provide greater protection to PI and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the Entity's primary or functional federal regulator.
- **More Protective Law.** This statute does not apply to an Entity that complies with a state or federal law that provides greater protection to PI and at least as thorough disclosure requirements for a breach of security or PI than that provided by the statute.
- **Gramm-Leach-Bliley Act.** This statute does not apply to an Entity that is subject to and complies with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act.
- **HIPAA and HITECH.** This statute does not apply to an Entity that is subject to and complies with the regulations promulgated pursuant to the Title II, subtitle F of the Health Insurance Portability and Accountability Act (HIPAA) and Title XIII, subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH).

Other Key Provisions:

- **Delay for Law Enforcement.** The consumer notification requirements of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the Entity required to give notice in writing.
- Attorney General Enforcement.