Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Illinois

815 Ill. Comp. Stat. 530/5, 530/10, 530/12, 530/15, 530/20, 530/25

H.B. 1633 (signed into law June 16, 2005, Public Act 94-36)

Effective June 27, 2006

H.B. 3025 (signed Aug. 22, 2011, Public Act 97-483)

Effective Jan. 1, 2012

H.B. 1260 (signed into law May 6, 2016)

Effective January 1, 2017

S.B. 1624 (signed into law August 9, 2019)

Effective January 1, 2020

Application. Any entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic PI (collectively, Entity) that owns or licenses PI concerning an IL resident.

Security Breach Definition. An unauthorized acquisition of computerized 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 a legitimate purpose of the Entity does not constitute a security breach, provided that the PI is not used for a purpose unrelated to the Entity's business or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall notify the resident at no charge that there has been a breach following discovery or notification of the breach.

Attorney General Notification. Any Entity required to notify more than 500 Illinois residents must provide notice to the Attorney General of the breach. Notice must include:

- A description of the nature of the breach of security;
- The date of the breach;
- The number of Illinois residents affected by such incident at the time of notification; and
- Any steps the Entity has taken or plans to take relating to the incident.

If the date of the breach is unknown at the time the notice is sent to the Attorney General, the Entity shall send the Attorney General the date of the breach as soon as possible.

Third-Party Data Notification. Any Entity that maintains or stores computerized data that includes PI that the Entity does not own or license shall notify the owner or licensee of the information of any breach of the security

of the data immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person. In addition, such Entities shall cooperate with the data owner or licensee in matters relating to the breach, including (1) giving notice of the (approximate) date and nature of the breach and (2) informing the owner or licensee of steps taken or planned relating to the breach.

Timing of Notification. In the most expedient time possible and without unreasonable delay, but in no event later than when the data collector provides notice to consumers pursuant to this Section.

Personal Information Definition. Either of the following:

(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;
- Driver's license number or state identification card number;
- Account number, credit card number, or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical information (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application);
- Health insurance information (health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records); or
- Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(2) 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 lawfully made available to the general public from federal, state, or local government records.

PI does not include information that is encrypted or redacted where the keys to provide access to the information have not also been obtained.

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

- Written notice;
- Electronic notice, if consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act); or
- For breaches involving username/email and password/security questions only, in "electronic or other form."

Contents of Notice.

Generally. For a breach of PI other than username/email and password/security question, the notice shall include:

- The toll-free numbers and addresses for consumer reporting agencies;

- The toll-free number, address, and website address for the Federal Trade Commission; and
- A statement that the individual can obtain information from these sources about fraud alerts and security freezes.

The notice shall not include the number of IL residents affected by the breach.

Online account credentials only: Notice may be provided in electronic or other form directing the IL resident whose PI has been breached to promptly change his or her username or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same username or email address and password or security question and answer.

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, if 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 impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.

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 the statute, shall be deemed in compliance with the notification requirements of the statute if the Entity notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

Exception: Compliance with Other Laws. Any Entity that is subject to and in compliance with the privacy and security standards under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act ("HITECH") shall be deemed to be in compliance, provided that any Entity required to provide notification of a breach to the Secretary of Health and Human Services pursuant to HITECH also provides such notification to the Attorney General within 5 business days of notifying the Secretary.

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 and provides the Entity with a written request of delay. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
- Waiver Not Permitted.
- Violation of the statute constitutes an unlawful practice under the IL Consumer Fraud and Deceptive Business Practices Act.