Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Indiana

Ind. Code § 4-1-11 *et seq.*; § 24-4.9-1 *et seq.*

S.B. 503 (signed into law April 26, 2005, Act 503)

Effective July 1, 2006

H.E.A. No. 1197 (signed into law March 24, 2008)

H.E.A. No. 1121 (signed into law May 12, 2009)

Effective July 1, 2009

H.E.A, No. 1341 (signed into law March 18, 2022)

S.B. 17 (signed into law March 13, 2024)

Effective July 1, 2024

Application. Any individual or legal entity (collectively, Entity) that owns or licenses computerized data that includes PI.

- State agencies are separately covered by § 4-1-11, which has similar individual notification requirements.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity. The term includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

- Unauthorized acquisition of a portable electronic device on which PI is stored does not constitute a security breach if all PI on the device is protected by encryption and the encryption key (i) has not been compromised or disclosed, and (ii) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.
- Good-faith acquisition of PI by an employee or agent of the Entity for lawful purposes of the Entity does not constitute a security breach if the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. An Entity shall disclose the breach to affected IN residents y if the Entity knows, or should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in Ind. Code § 35-43-5-3.5), identity theft, or fraud affecting the IN resident.

Notice must be provided to whose unencrypted PI was or may have been acquired by an unauthorized person and those whose encrypted PI was or may have been acquired by an unauthorized person with access to the encryption key.

Attorney General Notification. If the Entity makes such a disclosure, the data base owner shall also disclose the breach to the Attorney General.

Notification to Consumer Reporting Agencies. An Entity required to make a disclosure to more than 1,000 consumers shall also disclose to all nationwide consumer reporting agencies that compile and maintain files on consumers on a nationwide basis information necessary to assist the consumer reporting agency in preventing fraud, including PI of an IN resident affected by the breach of the security of a system.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI but that does not own or license the PI shall notify the owner of the PI if the Entity discovers that PI was or may have been acquired by an unauthorized person.

Timing of Notification. The disclosure notification shall be made without unreasonable delay, but not more than 45 days after the discovery of the breach, and consistent with any measures necessary to determine the scope of the breach and restore the integrity of the system.

Personal Information Definition. (1) A Social Security number that is not encrypted or redacted, (2) an individual's first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted:

- A driver's license number or state identification card number;
- A credit card number; or
- A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account; or

(3) information collected by an adult oriented website operator, or their designee, under **IC 24-4-23**.

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

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

- Mail;
- Telephone;
- Fax; or
- Email, if the Entity has the email address of the affected IN resident.

State agencies are subject to slightly different notice requirements.

Substitute Notice Available. If an Entity demonstrates that the cost of the disclosure exceeds $250,000, or that the affected class of subject persons to be notified exceeds 500,000. Substitute notice shall consist of all of the following:

- Conspicuous posting of the notice on the website of the Entity, if the Entity maintains one; and
- Notice to major news reporting media in the geographic area where IN residents affected by the breach of the security of a system reside.

Exception: Own Notification Policy. Any Entity that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate disclosure under the statute if the Entity's information privacy policy or security policy is at least as stringent as the disclosure requirements under the statute.

Exception: Compliance with Other Laws. This section does not apply to an Entity that maintains its own data security procedures as part of an information privacy, security policy, or compliance plan under:

- The Gramm-Leach-Bliley Act;
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- The USA Patriot Act (P.L. 107-56);
- Executive Order 13224;
- The Driver Privacy Protection Act (18 U.S.C. § 2781 *et seq.*); or
- The Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*).

If the Entity's information privacy, security policy, or compliance plan requires the Entity to maintain reasonable procedures to protect and safeguard from unlawful use or disclosure PI of IN residents that is collected or maintained by the Entity and the Entity complies with the Entity's information privacy, security policy, or compliance plan.

Other Key Provisions:

- **Attorney General Enforcement.** A person that knowingly or intentionally fails to comply with the database maintenance obligations commits a deceptive act that is actionable only by the state Attorney General. Penalties include injunctive relief, a civil penalty of not more than $150,000 per violation, and reasonable costs.