Indiana Code
Title 24 – Trade Regulation; Consumer Sales and Credit
Article 4.9 – Disclosure of Security Breach

Chapter 1. Application

§ 24-4.9-1-1. Article does not apply to state agency or judicial or legislative department of state government. This article does not apply to:

(1) a state agency (as defined in IC 4-1-10-2); or

(2) the judicial or legislative department of state government.

Chapter 2. Definitions

§ 24-4.9-2-1. Application of definitions. The definitions in this chapter apply throughout this article.

§ 24-4.9-2-2. Breach of the security of a system.
(a) "Breach of the security of a system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

(b) The term does not include the following:

(1) Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.

(2) Unauthorized acquisition of a portable electronic device on which personal information is stored, if access to the device is protected by a password that has not been disclosed.

§ 24-4.9-2-3. Data base owner. "Data base owner" means a person that owns or licenses computerized data that includes personal information.

§ 24-4.9-2-4. Doing business in Indiana. "Doing business in Indiana" means owning or using the personal information of an Indiana resident for commercial purposes.

§ 24-4.9-2-5. Encrypted. Data are encrypted for purposes of this article if the data:

(1) have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a

confidential process or key; or

(2) are secured by another method that renders the data unreadable or unusable.

§ 24-4.9-2-6. Financial institution. "Financial institution" means a financial institution as defined in:

(1) IC 28-1-1-3, other than a consumer finance institution licensed to make supervised or regulated loans under IC 24-4.5; or

(2) 15 U.S.C. 6809(3).

§ 24-4.9-2-7. Indiana resident. "Indiana resident" means a person whose principal mailing address is in Indiana, as reflected in records maintained by the data base owner.

§ 24-4.9-2-8. Mail. "Mail" has the meaning set forth in IC 23-1-20-15.

§ 24-4.9-2-9. Person. "Person" means an individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity.

§ 24-4.9-2-10. Personal information. "Personal information" means:

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

(A) A driver's license number.

(B) A state identification card number.

(C) A credit card number.

(D) 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.

The term 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.

§ 24-4.9-2-11. Redacted. (a) Data are redacted for purposes of this article if the data have been altered or truncated so that not more than the last four (4) digits of:

(1) a driver's license number;

(2) a state identification number; or

(3) an account number;

is accessible as part of personal information.

(b) For purposes of this article, personal information is "redacted" if the personal information has been altered or truncated so that not more than five (5) digits of a Social Security number are accessible as part of personal information.

Chapter 3. Disclosure and Notification Requirements

§ 24-4.9-3-1. Persons to be notified by data base owner in event of breach of security.
(a) Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident whose:

(1) unencrypted personal information was or may have been acquired by an unauthorized person; or

(2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, 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 IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.

(b) A data base owner required to make a disclosure under subsection (a) to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.

§ 24-4.9-3-2. Person maintaining computerized data to notify data base owner if personal information has been acquired by an unauthorized person. A person that maintains computerized data but that is not a data base owner shall notify the data base owner if the person discovers that personal information was or may have been acquired by an unauthorized person.

§ 24-4.9-3-3. Person to make disclosure or notification without unreasonable delay - When delay is reasonable.
(a) A person required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay. For purposes of this section, a

delay is reasonable if the delay is:

(1) necessary to restore the integrity of the computer system;

(2) necessary to discover the scope of the breach; or

(3) in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will:

(A) impede a criminal or civil investigation; or

(B) jeopardize national security.

(b) A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after:

(1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or

(2) the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.

§ 24-4.9-3-4. Methods of disclosure.

(a) Except as provided in subsection (b), a data base owner required to make a disclosure under this chapter shall make the disclosure using one (1) of the following methods:

(1) Mail.

(2) Telephone.

(3) Facsimile (fax).

(4) Electronic mail, if the data base owner has the electronic mail address of the affected Indiana resident.

(b) If a data base owner required to make a disclosure under this chapter is required to make the disclosure to more than five hundred thousand (500,000) Indiana residents, or if the data base owner required to make a disclosure under this chapter determines that the cost of the disclosure will be more than two hundred fifty thousand dollars ($250,000), the data base owner required to make a disclosure under this chapter may elect to make the disclosure by using both of the following methods:

(1) Conspicuous posting of the notice on the web site of the data base owner, if the data base owner maintains a web site.

(2) Notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.

(c) A data base owner 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 this chapter if the data base owner's information privacy policy or security policy is at least as stringent as the disclosure requirements described in:

(1) sections 1 through 4(b) of this chapter;

(2) subsection (d); or

(3) subsection (e).

(d) A data base owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under:

(1) the federal USA Patriot Act (P.L. 107-56);

(2) Executive Order 13224;

(3) the federal Driver's Privacy Protection Act (18 U.S.C. 2781 et seq.);

(4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(5) the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or

(6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191); is not required to make a disclosure under this chapter if the data base owner's information privacy, security policy, or compliance plan requires that Indiana residents be notified of a breach of the security of a system without unreasonable delay and the data base owner complies with the data base owner's information privacy, security policy, or compliance plan.

(e) A financial institution that complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, as applicable, is not required to make a disclosure under this chapter.

(f) A person required to make a disclosure under this chapter may elect to make all or part of the disclosure in accordance with subsection (a) even if the person could make the disclosure in accordance with subsection (b).

Chapter 4. Enforcement

§ 24-4.9-4-1. Failure to comply with article is deceptive act actionable by attorney general - Related series of breaches of security constitutes one deceptive act.
(a) A person that is required to make a disclosure or notification in accordance with IC 24-4.9-3 and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general under this chapter.

(b) A failure to make a required disclosure or notification in connection with a related series of breaches of the security of a system constitutes one (1) deceptive act.

§ 24-4.9-4-2. Action by attorney general. The attorney general may bring an action under this chapter to obtain any or all of the following:

(1) An injunction to enjoin future violations of IC 24-4.9-3.

(2) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act.

(3) The attorney general's reasonable costs in:

(A) the investigation of the deceptive act; and

(B) maintaining the action.

Chapter 5. Preemption

§ 24-4.9-5-1. Authority of unit to make enactment dealing with subject matter of this article preempted. This article preempts the authority of a unit (as defined in IC 36-1-2-23) to make an enactment dealing with the same subject matter as this article.