

January 17, 2008

HOUSE BILL No. 1197

DIGEST OF HB 1197 (Updated January 15, 2008 12:46 pm - DI 114)

Citations Affected: IC 4-6; IC 24-4.9.

Synopsis: Data breaches. Requires the attorney general to publish notice of a breach of the security of a system on the attorney general's Internet web site, and authorizes the attorney general to initiate a program to educate consumers of risks posed by a security breach. Provides, for purposes of the law requiring the disclosure of a breach of the security of a system, that the unauthorized acquisition of a portable electronic device on which personal information is stored does not constitute a breach of the security of a system if the contents of the portable electronic device are encrypted and if the encryption key is not compromised. Provides that, in the event of a security breach requiring notification, the data base owner's primary regulator and the attorney general must also be notified.

Effective: July 1, 2008.

Pierce , Dermody

January 10, 2008, read first time and referred to Committee on Technology, Research and Development.
January 16, 2008, amended, reported _ Do Pass.

January 17, 2008

Second Regular Session 115th General Assembly (2008)

PRINTING CODE. Amendments: Whenever an existing statute (or a section of the Indiana Constitution) is being amended, the text of the existing provision will appear in this style type, additions will appear in **this style type**, and deletions will appear in ~~this style type~~.

Additions: Whenever a new statutory provision is being enacted (or a new constitutional provision adopted), the text of the new provision will appear in **this style type**. Also, the word **NEW** will appear in that style type in the introductory

clause of each SECTION that adds a new provision to the Indiana Code or the Indiana Constitution.
 Conflict reconciliation: Text in a statute in *this style type* or ~~this style type~~ reconciles conflicts between statutes enacted by the 2007 Regular Session of the General Assembly.

HOUSE BILL No. 1197

A BILL FOR AN ACT to amend the Indiana Code concerning trade regulation.

Be it enacted by the General Assembly of the State of Indiana:

SOURCE: IC 4-6-9-7.5; (08)HB1197.1.1. --> SECTION 1. IC 4-6-9-7.5 IS ADDED TO THE INDIANA CODE AS A NEW SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2008]: **Sec. 7.5. (a) Subject to subsection (d), if a data base owner discloses a breach of the security of a system (as defined in IC 24-4.9-2-2) to the attorney general in accordance with IC 24-4.9-3, or if the attorney general otherwise discovers a breach of the security of a system required to be disclosed to the attorney general in accordance with IC 24-4.9-3, the division shall publish a notice of the security breach on the web site maintained by the attorney general.**

(b) Subject to subsection (d), notice of a breach of the security of a system published on the web site maintained by the attorney general must include the following information, if available:

(1) The name of the organization whose system security has been breached.

(2) The number of individuals and the number of Indiana residents whose personal information may have been

compromised by the breach.

(3) The date on which the breach occurred.

(4) The circumstances under which the breach occurred.

(5) Any other information that, in the opinion of the attorney general, would assist an individual in determining whether the individual's personal information has been disclosed or compromised.

(c) The division may initiate and maintain an educational program to inform consumers of:

(1) risks involved in a breach of the security of a system; and

(2) steps that the victim of a security breach should take to prevent and mitigate the damage from the security breach.

(d) A notice of a breach of the security of a system must be redacted to exclude any information that:

(1) is confidential;

(2) would assist in the commission of:

(A) identity deception (IC 35-43-5-3.5);

(B) another crime; or

(C) fraud; or

(3) could jeopardize the security of a system.

SOURCE: IC 24-4.9-2-2; (08)HB1197.1.2. -->

SOURCE: IC 24-4.9-2-2. --> SECTION 2. IC 24-4.9-2-2, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2008]: **Sec. 2. (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~~ **all personal information on the device is protected by ~~a password that~~ **encryption and the encryption key:****

(A) has not been compromised or disclosed; and

(B) is not in the possession of or known to the person who, without authorization, acquired or has access

to the portable electronic device.

SOURCE: IC 24-4.9-2-5; (08)HB1197.1.3. --> SECTION 3. IC 24-4.9-2-5, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2008]: Sec. 5. **(a) Except as provided in subsection (b), data are encrypted for purposes of this article if, in a manner consistent with the best practices common in the industry, 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.

(b) Data that have been transformed or secured as described in subsection (a) are not encrypted for purposes of this article unless the key required to decrypt the data complies with the best practices common in the industry and has not been disclosed or compromised.

SOURCE: IC 24-4.9-3-1; (08)HB1197.1.4. --> SECTION 4. IC 24-4.9-3-1, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2008]: Sec. 1. (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.

(c) If a data base owner makes a disclosure described in subsection (a), the data base owner shall also disclose the breach to:

(1) the data base owner's primary regulator, if the data base owner is regulated; and

(2) the attorney general.

SOURCE: IC 24-4.9-3-4; (08)HB1197.1.5. --> SECTION 5. IC 24-4.9-3-4, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2008]: Sec. 4. (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, **the attorney general, and the owner's primary regulator** 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).