



Reprinted  
February 24, 2015

---

---

## SENATE BILL No. 413

---

DIGEST OF SB 413 (Updated February 23, 2015 5:01 pm - DI 101)

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

**Synopsis:** Disclosures of security breaches. Makes the following changes to the statute concerning the breach of the security of data that includes the sensitive personal information of Indiana residents and that is collected and maintained by a person other than a state agency or the judicial or legislative department of state government: (1) Specifies that the statute is not limited to breaches of computerized data. (2) Repeals the definition of a term ("doing business in Indiana") that is not used in the statute. (3) Replaces the term "data base owner" with "data owner". (4) Defines the term "data collector" as a person that: (A) is not a data owner; and (B) collects, maintains, disseminates, or handles data that includes sensitive personal information. (5) Defines the term "data user" as a data owner or a data collector. (6) Replaces the term "personal information" with "sensitive personal information" and makes conforming amendments. (7) Requires a data user to post certain information concerning the data user's privacy practices on the data user's Internet web site. (8) Increases the amount of the civil penalty that a court may impose in an action by the attorney general to enforce the provisions concerning the safeguarding of data if the court finds that a violation: (A) was done knowingly; or (B) contributed to a breach of the security of data that includes the sensitive personal information of Indiana residents. (9) Sets forth certain information that a data owner must include in a disclosure of a security breach. (10) Specifies the applicability of different enforcement procedures available to the attorney general under the statute.

**Effective:** July 1, 2015.

---

---

### Merritt, Ford, Stoops, Randolph

---

---

January 12, 2015, read first time and referred to Committee on Homeland Security & Transportation.  
February 12, 2015, amended, reported favorably — Do Pass.  
February 23, 2015, read second time, amended, ordered engrossed.

---

---

SB 413—LS 6837/DI 101





Reprinted  
February 24, 2015

First Regular Session 119th General Assembly (2015)

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 2014 Regular Session and 2014 Second Regular Technical Session of the General Assembly.

## SENATE BILL No. 413

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:*

1 SECTION 1. IC 4-6-14-3, AS ADDED BY P.L.84-2010, SECTION  
2 1, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1,  
3 2015]: Sec. 3. As used in this chapter, "personal information" ~~has the~~  
4 ~~meaning set forth in IC 24-4.9-2-10.~~ **means:**

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

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

10 **(A) A driver's license number.**

11 **(B) A state identification card number.**

12 **(C) A credit card number.**

13 **(D) A financial account number or debit card number in**  
14 **combination with a security code, password, or access code**  
15 **that would permit access to the person's account.**

16 **The term does not include information that is lawfully obtained**

SB 413—LS 6837/DI 101



1 **from publicly available information or from federal, state, or local**  
 2 **government records lawfully made available to the general public.**

3 SECTION 2. IC 24-4-14-6, AS ADDED BY P.L.125-2006,  
 4 SECTION 5, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 5 JULY 1, 2015]: Sec. 6. (a) As used in this chapter, "personal  
 6 information" has the meaning set forth in IC 24-4-9-2-10: means:

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

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

12 (A) A driver's license number.

13 (B) A state identification card number.

14 (C) A credit card number.

15 (D) A financial account number or debit card number in  
 16 combination with a security code, password, or access code  
 17 that would permit access to the person's account.

18 The term includes information stored in a digital format.

19 (b) The term does not include information that is lawfully  
 20 obtained from publicly available information or from federal,  
 21 state, or local government records lawfully made available to the  
 22 general public.

23 SECTION 3. IC 24-4.9-2-2, AS AMENDED BY P.L.137-2009,  
 24 SECTION 3, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 25 JULY 1, 2015]: Sec. 2. (a) "Breach of the security of data" means  
 26 unauthorized acquisition of computerized data that compromises the  
 27 security, confidentiality, or integrity of sensitive personal information  
 28 maintained by a person. The term includes the unauthorized acquisition  
 29 of computerized data that have been transferred to another medium;  
 30 including paper, microfilm, or a similar medium, even if the transferred  
 31 data are no longer in a computerized format. data user.

32 (b) The term does not include the following:

33 (1) Good faith acquisition of sensitive personal information by an  
 34 employee or agent of the person data user for lawful purposes of  
 35 the person; data user, if the sensitive personal information is not  
 36 used for unlawful purposes or subject to further unauthorized  
 37 disclosure.

38 (2) Unauthorized acquisition of a portable electronic device on  
 39 which sensitive personal information is stored, if all sensitive  
 40 personal information on the device is protected by encryption and  
 41 the encryption key:

42 (A) has not been compromised or disclosed; and



- 1 (B) is not in the possession of or known to the person who,  
 2 without authorization, acquired or has access to the portable  
 3 electronic device.
- 4 SECTION 4. IC 24-4.9-2-2.7 IS ADDED TO THE INDIANA  
 5 CODE AS A **NEW** SECTION TO READ AS FOLLOWS  
 6 [EFFECTIVE JULY 1, 2015]: **Sec. 2.7. "Data" means electronic or**  
 7 **printed information that is collected, maintained, disseminated, or**  
 8 **handled:**
- 9 (1) in a computerized format;
  - 10 (2) on paper;
  - 11 (3) on microfilm; or
  - 12 (4) in another medium.
- 13 SECTION 5. IC 24-4.9-2-2.8 IS ADDED TO THE INDIANA  
 14 CODE AS A **NEW** SECTION TO READ AS FOLLOWS  
 15 [EFFECTIVE JULY 1, 2015]: **Sec. 2.8. "Data collector" means a**  
 16 **person that:**
- 17 (1) is not a data owner; and
  - 18 (2) collects, maintains, disseminates, or handles data that
  - 19 includes the sensitive personal information of an Indiana
  - 20 resident.
- 21 SECTION 6. IC 24-4.9-2-3, AS ADDED BY P.L.125-2006,  
 22 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 23 JULY 1, 2015]: **Sec. 3. "Data base owner" means a person that owns or**  
 24 **licenses computerized data that includes the sensitive personal**  
 25 **information of an Indiana resident.**
- 26 SECTION 7. IC 24-4.9-2-3.2 IS ADDED TO THE INDIANA  
 27 CODE AS A **NEW** SECTION TO READ AS FOLLOWS  
 28 [EFFECTIVE JULY 1, 2015]: **Sec. 3.2. "Data user" means a:**
- 29 (1) data owner; or
  - 30 (2) data collector.
- 31 SECTION 8. IC 24-4.9-2-4 IS REPEALED [EFFECTIVE JULY 1,  
 32 2015]. **Sec. 4. "Doing business in Indiana" means owning or using the**  
 33 **personal information of an Indiana resident for commercial purposes:**
- 34 SECTION 9. IC 24-4.9-2-7, AS ADDED BY P.L.125-2006,  
 35 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 36 JULY 1, 2015]: **Sec. 7. "Indiana resident" means a person whose**  
 37 **principal mailing address is in Indiana, as reflected in records**  
 38 **maintained by the a data base owner: user.**
- 39 SECTION 10. IC 24-4.9-2-10, AS ADDED BY P.L.125-2006,  
 40 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 41 JULY 1, 2015]: **Sec. 10. "Personal "Sensitive personal information"**  
 42 **means:**



1 (1) a Social Security number that is not encrypted or redacted; or  
 2 (2) an individual's first and last names, or first initial and last  
 3 name, and one (1) or more of the following data elements that are  
 4 not encrypted or redacted:

5 (A) A driver's license number.

6 (B) A state identification card number.

7 (C) A credit card number.

8 (D) A financial account number or debit card number in  
 9 combination with a security code, password, or access code  
 10 that would permit access to the person's account.

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

14 SECTION 11. IC 24-4.9-2-11, AS ADDED BY P.L.125-2006,  
 15 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 16 JULY 1, 2015]: Sec. 11. (a) Data are redacted for purposes of this  
 17 article if the data have been altered or truncated so that not more than  
 18 the last four (4) digits of:

19 (1) a driver's license number;

20 (2) a state identification number; or

21 (3) an account number;

22 is accessible as part of **sensitive** personal information.

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

27 SECTION 12. IC 24-4.9-3-1, AS AMENDED BY P.L.137-2009,  
 28 SECTION 4, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 29 JULY 1, 2015]: Sec. 1. (a) Except as provided in section ~~4(c), 4(d), and~~  
 30 ~~4(e), 4(f), and 4(g)~~ of this chapter, after discovering or being notified  
 31 of a breach of the security of data, ~~the a data base~~ owner shall disclose  
 32 the breach to an Indiana resident whose:

33 (1) unencrypted **sensitive** personal information was or may have  
 34 been **accessed or** acquired by an unauthorized person; or

35 (2) encrypted **sensitive** personal information was or may have  
 36 been **accessed or** acquired by an unauthorized person with access  
 37 to the encryption key;

38 if the data ~~base~~ owner knows, should know, or should have known that  
 39 the unauthorized **access or** acquisition constituting the breach has  
 40 resulted in or could result in identity deception (as defined in  
 41 IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.

42 (b) A data ~~base~~ owner required to make a disclosure under



1 subsection (a) to more than one thousand (1,000) ~~consumers~~ **Indiana**  
 2 **residents** shall also disclose to each consumer reporting agency **that**  
 3 **compiles and maintains files on consumers on a nationwide basis**  
 4 (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the  
 5 consumer reporting agency in preventing fraud, including **fraud**  
 6 **involving the sensitive** personal information of an Indiana resident  
 7 affected by the breach of the security of a system.

8 (c) If a data ~~base~~ owner makes a disclosure described in subsection  
 9 (a), the data ~~base~~ owner shall also disclose the breach to the attorney  
 10 general.

11 SECTION 13. IC 24-4.9-3-2, AS ADDED BY P.L.125-2006,  
 12 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 13 JULY 1, 2015]: Sec. 2. A **person data collector** that maintains  
 14 **computerized data but that is not a data base owner** shall notify the data  
 15 **base** owner if the **person data collector** discovers that **sensitive**  
 16 personal information was or may have been acquired by an  
 17 unauthorized person.

18 SECTION 14. IC 24-4.9-3-3, AS ADDED BY P.L.125-2006,  
 19 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 20 JULY 1, 2015]: Sec. 3. (a) A **person data user** required to make a  
 21 disclosure or notification under this chapter shall make the disclosure  
 22 or notification without unreasonable delay. For purposes of this section,  
 23 a delay is reasonable if the delay is:

- 24 (1) necessary to restore the integrity of ~~the a~~ computer system;
- 25 (2) necessary to discover the scope of the breach; or
- 26 (3) in response to a request from the attorney general or a law  
 27 enforcement agency to delay disclosure because disclosure will:
  - 28 (A) impede a criminal or civil investigation; or
  - 29 (B) jeopardize national security.

30 (b) A **person data user** required to make a disclosure or notification  
 31 under this chapter shall make the disclosure or notification as soon as  
 32 possible after:

- 33 (1) delay is no longer necessary to restore the integrity of ~~the a~~  
 34 computer system or to discover the scope of the breach; or
- 35 (2) the attorney general or a law enforcement agency notifies the  
 36 **person data user** that delay will no longer impede a criminal or  
 37 civil investigation or jeopardize national security.

38 SECTION 15. IC 24-4.9-3-3.5, AS ADDED BY P.L.137-2009,  
 39 SECTION 5, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 40 JULY 1, 2015]: Sec. 3.5. (a) This section does not apply to a data ~~base~~  
 41 **owner user** that **maintains is required to maintain** its own data  
 42 security procedures, **and maintains such procedures**, as part of an



1 information privacy, security policy, or compliance plan under:

- 2 (1) the federal USA PATRIOT Act (P.L. 107-56);  
 3 (2) Executive Order 13224;  
 4 (3) the federal Driver's Privacy Protection Act (18 U.S.C. 2721 et  
 5 seq.);  
 6 (4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);  
 7 (5) the federal Financial Modernization Act of 1999 (15 U.S.C.  
 8 6801 et seq.); or  
 9 (6) the federal Health Insurance Portability and Accountability  
 10 Act (HIPAA) (P.L. 104-191), **as amended by the Health**  
 11 **Information Technology for Economic and Clinical Health**  
 12 **(HITECH) Act (P.L. 111-5);**

13 if the data ~~base owner's~~ **user's** information privacy, security policy, or  
 14 compliance plan requires the data ~~base owner~~ **user** to maintain  
 15 reasonable procedures to protect and safeguard from unlawful use or  
 16 disclosure **sensitive** personal information of Indiana residents that is  
 17 collected or maintained by the data ~~base owner~~ **user** and the data ~~base~~  
 18 ~~owner~~ **user** complies with the data ~~base owner's~~ **user's** information  
 19 privacy, security policy, or compliance plan.

20 (b) A data ~~base owner~~ **user** shall:

21 **(1) subject to subsection (c)**, implement and maintain reasonable  
 22 procedures, including taking any appropriate corrective action, to  
 23 protect and safeguard from unlawful use or disclosure any **data**  
 24 **that includes the sensitive** personal information of Indiana  
 25 residents **and that is** collected or maintained by the data ~~base~~  
 26 ~~owner~~ **user**; and

27 **(2) conspicuously post on the Internet web site, if any:**

28 **(A) that is publicly accessible; and**

29 **(B) through which data that includes the sensitive personal**  
 30 **information of Indiana residents is collected;**

31 **the data user's privacy policy with respect to sensitive**  
 32 **personal information collected through the Internet web site**  
 33 **and maintained by the data user.**

34 **(c) Procedures implemented and maintained by a data user**  
 35 **under subsection (b)(1) must require that the data user:**

36 **(1) retain sensitive personal information only as reasonably**  
 37 **necessary for:**

38 **(A) a legitimate business, governmental, academic, or**  
 39 **nonprofit purpose; or**

40 **(B) compliance with applicable law;**

41 **(2) not use sensitive personal information in contravention of**  
 42 **law; and**





1           **(3) not use sensitive personal information unless:**

2           **(A) the use is reasonably necessary for a legitimate**  
 3           **business, governmental, academic, or nonprofit purpose;**  
 4           **and**

5           **(B) the individual to whom the sensitive personal**  
 6           **information relates has not previously communicated to**  
 7           **the data user that such use is not authorized by the**  
 8           **individual.**

9           ~~(e)~~ **(d)** A data base owner user shall not dispose of records or  
 10 documents containing unencrypted ~~and~~ **or** unredacted sensitive  
 11 personal information of Indiana residents without shredding,  
 12 incinerating, mutilating, erasing, or otherwise rendering the sensitive  
 13 personal information illegible or unusable.

14           **(e) A data user shall not:**

15           **(1) make a misrepresentation to an Indiana resident**  
 16           **concerning the data user's collection, storage, use, sharing, or**  
 17           **destruction of sensitive personal information; or**

18           **(2) require a vendor or contractor to make a**  
 19           **misrepresentation described in subdivision (1).**

20           ~~(d)~~ **(f)** A person that knowingly or intentionally fails to comply with  
 21 any provision of this section commits a deceptive act that is actionable  
 22 only by the attorney general under this section. **A person that fails to**  
 23 **comply with section 1, 2, 3, or 4 of this chapter commits a deceptive**  
 24 **act that is actionable only by the attorney general under**  
 25 **IC 24-4.9-4. The enforcement procedures available under this**  
 26 **section are cumulative and an enforcement procedure available**  
 27 **under this section is supplemental to any other enforcement**  
 28 **procedure available under:**

29           **(1) this section;**

30           **(2) IC 24-4.9-4; or**

31           **(3) any other law, rule, or regulation of this state;**

32 **for a violation of this article.**

33           ~~(e)~~ **(g)** The attorney general may bring an action under this section  
 34 to obtain any or all of the following:

35           **(1) An injunction to enjoin further violations of this section.**

36           **(2) Subject to subsections (i) and (j), a civil penalty of not more**  
 37           **than five one thousand dollars (~~\$5,000~~) (\$1,000) per deceptive**  
 38           **act.**

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

40           **(A) the investigation of the deceptive act; and**

41           **(B) maintaining the action.**

42           ~~(h)~~ **(h)** Subject to subsection (i), a failure to comply with subsection



1 (b) or ~~(e)~~ (d) in connection with related acts or omissions constitutes  
 2 one (1) deceptive act.

3 **(i) Subject to subsection (j), in an action brought under this**  
 4 **section, if the court determines that a failure to comply with this**  
 5 **section was done knowingly, the court may impose a civil penalty**  
 6 **of not more than the greater of:**

7 **(1) five thousand dollars (\$5,000); or**

8 **(2) fifty dollars (\$50) for each affected Indiana resident if the**  
 9 **failure to comply contributed to a breach of the security of**  
 10 **data.**

11 **(j) The total civil penalties imposed under subsection (g) or (i)**  
 12 **in connection with one (1) deceptive act may not exceed one**  
 13 **hundred fifty thousand dollars (\$150,000).**

14 **(k) The consumer protection division of the office of the**  
 15 **attorney general shall use civil penalties collected under this article**  
 16 **to enforce this article.**

17 SECTION 16. IC 24-4.9-3-4, AS AMENDED BY P.L.137-2009,  
 18 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 19 JULY 1, 2015]: Sec. 4. (a) Except as provided in subsection ~~(b)~~, (c), a  
 20 data base owner required to make a disclosure under **section 1** of this  
 21 chapter shall make the disclosure using one (1) of the following  
 22 methods:

23 (1) Mail.

24 (2) Telephone.

25 (3) Facsimile (fax).

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

28 **(b) A disclosure under section 1 of this chapter must include the**  
 29 **following:**

30 **(1) A description of the breach of the security of data in**  
 31 **general terms.**

32 **(2) A description of the sensitive personal information that**  
 33 **was subject to unauthorized access or acquisition.**

34 **(3) A general description of any actions by the data owner to**  
 35 **protect the sensitive personal information from further**  
 36 **unauthorized access.**

37 **(4) The toll free telephone numbers and addresses for the**  
 38 **consumer reporting agencies described in section 1(b) of this**  
 39 **chapter.**

40 **(5) The toll free telephone numbers, addresses, and Internet**  
 41 **web site addresses for the Federal Trade Commission and the**  
 42 **office of the attorney general, along with a statement that an**



1 individual may obtain from the Federal Trade Commission  
 2 and the office of the attorney general information about  
 3 preventing identity theft.

4 ~~(b)~~ (c) If a data base owner is required to make a disclosure under  
 5 section 1 of this chapter is required to make and:

6 (1) the disclosure **must be made** to more than five hundred  
 7 thousand (500,000) Indiana residents; ~~or if the data base owner~~  
 8 ~~required to make a disclosure under this chapter determines that~~

9 (2) the **associated** cost of the disclosure will be more than two  
 10 hundred fifty thousand dollars (\$250,000); ~~or~~

11 (3) the data base owner ~~required to make a disclosure under this~~  
 12 ~~chapter does not have sufficient contact information for~~  
 13 **Indiana residents to make the required disclosure;**

14 **the data owner** may elect to make the disclosure by using both of the  
 15 following methods **set forth in subsection (d), as an alternative to**  
 16 **the methods set forth in subsection (a).**

17 (d) **A data owner described in subsection (c) may elect to make**  
 18 **the disclosure required under section 1 of this chapter using both**  
 19 **of the following methods, as an alternative to the methods set forth**  
 20 **in subsection (a):**

21 (1) ~~Conspicuous~~ **Conspicuously** posting of the notice on the **data**  
 22 **owner's Internet** web site, ~~of the data base owner, if the data~~  
 23 ~~base owner maintains a web site. if any, a notice of the breach~~  
 24 **of the security of data.**

25 (2) **Providing** notice to major news reporting media in the  
 26 geographic area where Indiana residents affected by the breach of  
 27 the security of a ~~system~~ **the data** reside.

28 ~~(e)~~ (e) A data base owner that maintains its own disclosure  
 29 procedures as part of an information privacy policy or a security policy  
 30 is not required to make a separate disclosure under **section 1** of this  
 31 chapter if the data base owner's information privacy policy or security  
 32 policy is at least as stringent as the disclosure requirements described  
 33 in:

34 (1) sections 1 through ~~4(b)~~ **4(d)** of this chapter;

35 (2) subsection ~~(d)~~; **(f)**; or

36 (3) subsection ~~(e)~~; **(g)**.

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

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

41 (2) Executive Order 13224;

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



- 1 seq.);
- 2 (4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
- 3 (5) the federal Financial Modernization Act of 1999 (15 U.S.C.
- 4 6801 et seq.); or
- 5 (6) the federal Health Insurance Portability and Accountability
- 6 Act (HIPAA) (P.L. 104-191), **as amended by the Health**
- 7 **Information Technology for Economic and Clinical Health**
- 8 **(HITECH) Act (P.L. 111-5);**

9 is not required to make a disclosure under **section 1** of this chapter if  
 10 the data base owner's information privacy, security policy, or  
 11 compliance plan requires that Indiana residents be notified of a breach  
 12 of the security of data without unreasonable delay and the data base  
 13 owner complies with the data base owner's information privacy,  
 14 security policy, or compliance plan.

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

21 ~~(f)~~ **(h)** A person required to make a disclosure under this chapter  
 22 may elect to make all or part of the disclosure in accordance with  
 23 subsection (a) even if the person could make the disclosure in  
 24 accordance with subsection ~~(b)~~: **(d)**.

25 SECTION 17. IC 24-4.9-4-1, AS AMENDED BY P.L.137-2009,  
 26 SECTION 7, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
 27 JULY 1, 2015]: Sec. 1. (a) A person that is required to make a  
 28 disclosure or notification in accordance with IC 24-4.9-3 and that fails  
 29 to comply with any provision of this article, **other than**  
 30 **IC 24-4.9-3-3.5**, commits a deceptive act that is actionable only by the  
 31 attorney general under this chapter. **A person that fails to comply**  
 32 **with IC 24-4.9-3-3.5 commits a deceptive act that is actionable only**  
 33 **by the attorney general under IC 24-4.9-3-3.5. The enforcement**  
 34 **procedures available under this chapter are cumulative and an**  
 35 **enforcement procedure available under this chapter is**  
 36 **supplemental to any other enforcement procedure available under:**

- 37 **(1) this chapter;**
- 38 **(2) IC 24-4.9-3-3.5; or**
- 39 **(3) any other law, rule, or regulation of this state;**
- 40 **for a violation of this article.**

41 (b) A failure to make a required disclosure or notification in  
 42 connection with a related series of breaches of the security of data



1 constitutes one (1) deceptive act.  
2 SECTION 18. IC 24-4.9-4-2, AS ADDED BY P.L.125-2006,  
3 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE  
4 JULY 1, 2015]: Sec. 2. **(a)** The attorney general may bring an action  
5 under this chapter to obtain any or all of the following:  
6 (1) An injunction to enjoin future violations of IC 24-4.9-3, **other**  
7 **than a violation of IC 24-4.9-3-3.5.**  
8 (2) A civil penalty of not more than one hundred fifty thousand  
9 dollars (\$150,000) per deceptive act.  
10 (3) The attorney general's reasonable costs in:  
11 (A) the investigation of the deceptive act; and  
12 (B) maintaining the action.  
13 **(b) The consumer protection division of the office of the**  
14 **attorney general shall use civil penalties collected under this article**  
15 **to enforce this article.**



## COMMITTEE REPORT

Madam President: The Senate Committee on Homeland Security and Transportation, to which was referred Senate Bill No. 413, has had the same under consideration and begs leave to report the same back to the Senate with the recommendation that said bill be AMENDED as follows:

Page 8, line 35, delete "section 1 of".

and when so amended that said bill do pass.

(Reference is to SB 413 as introduced.)

YODER, Chairperson

Committee Vote: Yeas 10, Nays 0.

---

 SENATE MOTION

Madam President: I move that Senate Bill 413 be amended to read as follows:

Page 1, between the enacting clause and line 1, begin a new paragraph and insert:

"SECTION 1. IC 4-6-14-3, AS ADDED BY P.L.84-2010, SECTION 1, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2015]: Sec. 3. As used in this chapter, "personal information" ~~has the meaning set forth in IC 24-4-9-2-10.~~ **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.**

SECTION 2. IC 24-4-14-6, AS ADDED BY P.L.125-2006,

SB 413—LS 6837/DI 101



SECTION 5, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2015]: Sec. 6. **(a)** As used in this chapter, "personal information" ~~has the meaning set forth in IC 24-4.9-2-10.~~ **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 includes information stored in a digital format.

**(b) 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."**

Page 1, line 5, after "of" insert "**sensitive**".

Page 1, line 11, after "of" insert "**sensitive**".

Page 1, line 13, after "the" insert "**sensitive**".

Page 1, line 16, after "which" insert "**sensitive**".

Page 1, line 16, after "all" insert "**sensitive**".

Page 2, line 21, after "the" insert "**sensitive**".

Page 2, line 25, after "the" insert "**sensitive**".

Page 2, between lines 39 and 40, begin a new paragraph and insert:  
"SECTION 10. IC 24-4.9-2-10, AS ADDED BY P.L.125-2006,

SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2015]: Sec. 10. ~~"Personal "~~**"Sensitive 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.

SECTION 11. IC 24-4.9-2-11, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2015]: Sec. 11. (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 **sensitive** personal information.

(b) For purposes of this article, **sensitive** personal information is "redacted" if the **sensitive** 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 **the sensitive** personal information."

Page 3, line 4, after "unencrypted" insert "**sensitive**".

Page 3, line 6, after "encrypted" insert "**sensitive**".

Page 3, line 14, strike "consumers" and insert "**Indiana residents**".

Page 3, line 18, after "including" insert "**fraud involving the sensitive**".

Page 3, line 27, after "that" insert "**sensitive**".

Page 4, line 10, strike "maintains" and insert "**is required to maintain**".

Page 4, line 10, after "procedures" insert ", **and maintains such procedures,**".

Page 4, line 20, delete ";" and insert ", **as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 111-5);**".

Page 4, line 24, after "disclosure" insert "**sensitive**".

Page 4, line 32, after "the" insert "**sensitive**".

Page 4, line 34, delete "subject to subsection (d),".

Page 4, line 37, after "the" insert "**sensitive**".

Page 4, line 39, after "to" insert "**sensitive**".

Page 5, line 1, delete "prohibit the data user from:" and insert "**require that the data user:**

(1) **retain sensitive personal information only as reasonably necessary for:**

(A) **a legitimate business, governmental, academic, or nonprofit purpose; or**

(B) **compliance with applicable law;**

(2) **not use sensitive personal information in contravention of law; and**





**(3) not use sensitive personal information unless:**

**(A) the use is reasonably necessary for a legitimate business, governmental, academic, or nonprofit purpose; and**

**(B) the individual to whom the sensitive personal information relates has not previously communicated to the data user that such use is not authorized by the individual."**

Page 5, delete lines 2 through 18.

Page 5, line 19, delete "(e)" and insert "**(d)**".

Page 5, line 20, after "unredacted" insert "**sensitive**".

Page 5, line 22, after "the" insert "**sensitive**".

Page 5, line 24, delete "(f)" and insert "**(e)**".

Page 5, line 27, after "of" insert "**sensitive**".

Page 5, line 30, delete "(g)" and insert "**(f)**".

Page 5, line 41, delete "state or federal law, rule, or regulation;" and insert "**law, rule, or regulation of this state;**".

Page 6, line 1, delete "(h)" and insert "**(g)**".

Page 6, line 4, delete "(j) and (k)," and insert "**(i) and (j)**".

Page 6, line 10, delete "(i) Subject to subsection (j)," and insert "**(h) Subject to subsection (i)**".

Page 6, line 11, delete "(e)" and insert "**(d)**".

Page 6, line 13, delete "(j) Subject to subsection (k)," and insert "**(i) Subject to subsection (j)**".

Page 6, line 19, after "security of" insert "**data**".

Page 6, delete lines 20 through 21.

Page 6, line 22, delete "(k)" and insert "**(j)**".

Page 6, line 22, delete "(h) or (j)" and insert "**(g) or (i)**".

Page 6, line 25, delete "(l)" and insert "**(k)**".

Page 7, line 1, after "the" insert "**sensitive**".

Page 7, line 4, after "the" insert "**sensitive**".

Page 7, line 32, after "on the" insert "**data owner's**".

Page 7, line 34, delete "any:" and insert "**any, a notice of the breach of the security of data**".

Page 7, delete lines 35 through 41.

Page 8, line 23, delete ";" and insert "**, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 111-5)**";".

Page 9, line 6, delete "IC 24-4.9-3.5." and insert "**IC 24-4.9-3-3.5**".



Page 9, line 11, delete "IC 24-4.9-3.5;" and insert "**IC 24-4.9-3-3.5;**".

Page 9, line 12, delete "state or federal law, rule, or regulation;" and insert "**law, rule, or regulation of this state;**".

Renumber all SECTIONS consecutively.

(Reference is to SB 413 as printed February 13, 2015.)

MERRITT

