



Rep. Ann Williams

**Filed: 11/9/2015**

09900HB1260ham001

LRB099 05116 KTG 39629 a

1 AMENDMENT TO HOUSE BILL 1260

2 AMENDMENT NO. \_\_\_\_\_. Amend House Bill 1260 by replacing  
3 everything after the enacting clause with the following:

4 "Section 5. The Personal Information Protection Act is  
5 amended by changing Sections 5, 10, and 12 and adding Sections  
6 45 and 50 as follows:

7 (815 ILCS 530/5)

8 Sec. 5. Definitions. In this Act:

9 "Data Collector" may include, but is not limited to,  
10 government agencies, public and private universities,  
11 privately and publicly held corporations, financial  
12 institutions, retail operators, and any other entity that, for  
13 any purpose, handles, collects, disseminates, or otherwise  
14 deals with nonpublic personal information.

15 "Breach of the security of the system data" or "breach"  
16 means unauthorized acquisition of computerized data that

1 compromises the security, confidentiality, or integrity of  
2 personal information maintained by the data collector. "Breach  
3 of the security of the system data" does not include good faith  
4 acquisition of personal information by an employee or agent of  
5 the data collector for a legitimate purpose of the data  
6 collector, provided that the personal information is not used  
7 for a purpose unrelated to the data collector's business or  
8 subject to further unauthorized disclosure.

9 "Health insurance information" means an individual's  
10 health insurance policy number or subscriber identification  
11 number, any unique identifier used by a health insurer to  
12 identify the individual, or any medical information in an  
13 individual's health insurance application and claims history,  
14 including any appeals records.

15 "Medical information" means any information regarding an  
16 individual's medical history, mental or physical condition, or  
17 medical treatment or diagnosis by a healthcare professional,  
18 including such information provided to a website or mobile  
19 application.

20 "Personal information" means either of the following:

21 (1) an individual's first name or first initial and  
22 last name in combination with any one or more of the  
23 following data elements, when either the name or the data  
24 elements are not encrypted or redacted or are encrypted or  
25 redacted but the keys to unencrypt or unredact or otherwise  
26 read the name or data elements have been acquired without

1 authorization through the breach of security:

2 (A) ~~(1)~~ Social Security number.

3 (B) ~~(2)~~ Driver's license number or State  
4 identification card number.

5 (C) ~~(3)~~ Account number or credit or debit card  
6 number, or an account number or credit card number in  
7 combination with any required security code, access  
8 code, or password that would permit access to an  
9 individual's financial account.

10 (D) Medical information.

11 (E) Health insurance information.

12 (F) Unique biometric data generated from  
13 measurements or technical analysis of human body  
14 characteristics used by the owner or licensee to  
15 authenticate an individual, such as a fingerprint,  
16 retina or iris image, or other unique physical  
17 representation or digital representation of biometric  
18 data.

19 (2) user name or email address, in combination with a  
20 password or security question and answer that would permit  
21 access to an online account, when either the user name or  
22 email address or password or security question and answer  
23 are not encrypted or redacted or are encrypted or redacted  
24 but the keys to unencrypt or unredact or otherwise read the  
25 data elements have been obtained through the breach of  
26 security.

1 "Personal information" does not include publicly available  
2 information that is lawfully made available to the general  
3 public from federal, State, or local government records.

4 (Source: P.A. 97-483, eff. 1-1-12.)

5 (815 ILCS 530/10)

6 Sec. 10. Notice of Breach.

7 (a) Any data collector that owns or licenses personal  
8 information concerning an Illinois resident shall notify the  
9 resident at no charge that there has been a breach of the  
10 security of the system data following discovery or notification  
11 of the breach. The disclosure notification shall be made in the  
12 most expedient time possible and without unreasonable delay,  
13 consistent with any measures necessary to determine the scope  
14 of the breach and restore the reasonable integrity, security,  
15 and confidentiality of the data system. The disclosure  
16 notification to an Illinois resident shall include, but need  
17 not be limited to, information as follows:

18 (1) With respect to personal information as defined in  
19 Section 5 in paragraph (1) of the definition of "personal  
20 information":

21 (A) ~~(i)~~ the toll-free numbers and addresses for  
22 consumer reporting agencies; ~~7~~

23 (B) ~~(ii)~~ the toll-free number, address, and  
24 website address for the Federal Trade Commission; ~~7~~

25 (C) ~~(iii)~~ a statement that the individual can

1           obtain information from these sources about fraud  
2           alerts and security freezes.

3           The notification shall not, however, include information  
4           concerning the number of Illinois residents affected by the  
5           breach.

6           (2) With respect to personal information defined in  
7           Section 5 in paragraph (2) of the definition of "personal  
8           information", notice may be provided in electronic or other  
9           form directing the Illinois resident whose personal  
10           information has been breached to promptly change his or her  
11           user name or password and security question or answer, as  
12           applicable, or to take other steps appropriate to protect  
13           all online accounts for which the resident uses the same  
14           user name or email address and password or security  
15           question and answer.

16           (b) Any data collector that maintains or stores, but does  
17           not own or license, computerized data that includes personal  
18           information that the data collector does not own or license  
19           shall notify the owner or licensee of the information of any  
20           breach of the security of the data immediately following  
21           discovery, if the personal information was, or is reasonably  
22           believed to have been, acquired by an unauthorized person. In  
23           addition to providing such notification to the owner or  
24           licensee, the data collector shall cooperate with the owner or  
25           licensee in matters relating to the breach. That cooperation  
26           shall include, but need not be limited to, (i) informing the

1 owner or licensee of the breach, including giving notice of the  
2 date or approximate date of the breach and the nature of the  
3 breach, and (ii) informing the owner or licensee of any steps  
4 the data collector has taken or plans to take relating to the  
5 breach. The data collector's cooperation shall not, however, be  
6 deemed to require either the disclosure of confidential  
7 business information or trade secrets or the notification of an  
8 Illinois resident who may have been affected by the breach.

9 (b-5) The notification to an Illinois resident required by  
10 subsection (a) of this Section may be delayed if an appropriate  
11 law enforcement agency determines that notification will  
12 interfere with a criminal investigation and provides the data  
13 collector with a written request for the delay. However, the  
14 data collector must notify the Illinois resident as soon as  
15 notification will no longer interfere with the investigation.

16 (c) For purposes of this Section, notice to consumers may  
17 be provided by one of the following methods:

18 (1) written notice;

19 (2) electronic notice, if the notice provided is  
20 consistent with the provisions regarding electronic  
21 records and signatures for notices legally required to be  
22 in writing as set forth in Section 7001 of Title 15 of the  
23 United States Code; or

24 (3) substitute notice, if the data collector  
25 demonstrates that the cost of providing notice would exceed  
26 \$250,000 or that the affected class of subject persons to

1 be notified exceeds 500,000, or the data collector does not  
2 have sufficient contact information. Substitute notice  
3 shall consist of all of the following: (i) email notice if  
4 the data collector has an email address for the subject  
5 persons; (ii) conspicuous posting of the notice on the data  
6 collector's web site page if the data collector maintains  
7 one; and (iii) notification to major statewide media or, if  
8 the breach impacts residents in one geographic area, to  
9 prominent local media in areas where affected individuals  
10 are likely to reside if such notice is reasonably  
11 calculated to give actual notice to persons whom notice is  
12 required.

13 (d) Notwithstanding any other subsection in this Section, a  
14 data collector that maintains its own notification procedures  
15 as part of an information security policy for the treatment of  
16 personal information and is otherwise consistent with the  
17 timing requirements of this Act, shall be deemed in compliance  
18 with the notification requirements of this Section if the data  
19 collector notifies subject persons in accordance with its  
20 policies in the event of a breach of the security of the system  
21 data.

22 (e) Notice to Attorney General. Any data collector that  
23 owns or licenses personal information and suffers a single  
24 breach of the security of the data concerning the personal  
25 information of more than 250 Illinois residents shall provide  
26 notice to the Attorney General of the breach, including:

1           (A) The types of personal information compromised in  
2           the breach.

3           (B) The number of Illinois residents affected by such  
4           incident at the time of notification.

5           (C) Any steps the data collector has taken or plans to  
6           take relating to notification of the breach to consumers.

7           (D) The date and timeframe of the breach, if known at  
8           the time notification is provided.

9           Such notification must be made within 45 days of the data  
10          collector's discovery of the security breach or when the data  
11          collector provides any notice to consumers required by this  
12          Section, whichever is sooner, unless the data collector has  
13          good cause for reasonable delay to determine the scope of the  
14          breach and restore the integrity, security, and  
15          confidentiality of the data system, or when law enforcement  
16          requests in writing to withhold disclosure of some or all of  
17          the information required in the notification under this  
18          Section. If the date or timeframe of the breach is unknown at  
19          the time the notice is sent to the Attorney General, the data  
20          collector shall send the Attorney General the date or timeframe  
21          of the breach as soon as possible.

22          (Source: P.A. 97-483, eff. 1-1-12.)

23           (815 ILCS 530/12)

24           Sec. 12. Notice of breach; State agency.

25           (a) Any State agency that collects personal information



1 concerning an Illinois resident shall notify the resident at no  
2 charge that there has been a breach of the security of the  
3 system data or written material following discovery or  
4 notification of the breach. The disclosure notification shall  
5 be made in the most expedient time possible and without  
6 unreasonable delay, consistent with any measures necessary to  
7 determine the scope of the breach and restore the reasonable  
8 integrity, security, and confidentiality of the data system.  
9 The disclosure notification to an Illinois resident shall  
10 include, but need not be limited to information as follows:

11 (1) With respect to personal information defined in  
12 Section 5 in paragraph (1) of the definition of "personal  
13 information":

14 (i) the toll-free numbers and addresses for  
15 consumer reporting agencies;

16 (ii) the toll-free number, address, and website  
17 address for the Federal Trade Commission; and

18 (iii) a statement that the individual can obtain  
19 information from these sources about fraud alerts and  
20 security freezes.

21 (2) With respect to personal information as defined in  
22 Section 5 in paragraph (2) of the definition of "personal  
23 information", notice may be provided in electronic or other  
24 form directing the Illinois resident whose personal  
25 information has been breached to promptly change his or her  
26 user name or password and security question or answer, as

1       applicable, or to take other steps appropriate to protect  
2       all online accounts for which the resident uses the same  
3       user name or email address and password or security  
4       question and answer.

5       The notification shall not, however, include information  
6       concerning the number of Illinois residents affected by the  
7       breach.

8       (a-5) The notification to an Illinois resident required by  
9       subsection (a) of this Section may be delayed if an appropriate  
10      law enforcement agency determines that notification will  
11      interfere with a criminal investigation and provides the State  
12      agency with a written request for the delay. However, the State  
13      agency must notify the Illinois resident as soon as  
14      notification will no longer interfere with the investigation.

15      (b) For purposes of this Section, notice to residents may  
16      be provided by one of the following methods:

17           (1) written notice;

18           (2) electronic notice, if the notice provided is  
19      consistent with the provisions regarding electronic  
20      records and signatures for notices legally required to be  
21      in writing as set forth in Section 7001 of Title 15 of the  
22      United States Code; or

23           (3) substitute notice, if the State agency  
24      demonstrates that the cost of providing notice would exceed  
25      \$250,000 or that the affected class of subject persons to  
26      be notified exceeds 500,000, or the State agency does not

1           have sufficient contact information. Substitute notice  
2           shall consist of all of the following: (i) email notice if  
3           the State agency has an email address for the subject  
4           persons; (ii) conspicuous posting of the notice on the  
5           State agency's web site page if the State agency maintains  
6           one; and (iii) notification to major statewide media.

7           (c) Notwithstanding subsection (b), a State agency that  
8           maintains its own notification procedures as part of an  
9           information security policy for the treatment of personal  
10          information and is otherwise consistent with the timing  
11          requirements of this Act shall be deemed in compliance with the  
12          notification requirements of this Section if the State agency  
13          notifies subject persons in accordance with its policies in the  
14          event of a breach of the security of the system data or written  
15          material.

16          (d) If a State agency is required to notify more than 1,000  
17          persons of a breach of security pursuant to this Section, the  
18          State agency shall also notify, without unreasonable delay, all  
19          consumer reporting agencies that compile and maintain files on  
20          consumers on a nationwide basis, as defined by 15 U.S.C.  
21          Section 1681a(p), of the timing, distribution, and content of  
22          the notices. Nothing in this subsection (d) shall be construed  
23          to require the State agency to provide to the consumer  
24          reporting agency the names or other personal identifying  
25          information of breach notice recipients.

26          (e) Notice to Attorney General. Any State agency that

1 suffers a single breach of the security of the data concerning  
2 the personal information of more than 250 Illinois residents  
3 shall provide notice to the Attorney General of the breach,  
4 including:

5 (A) The types of personal information compromised in  
6 the breach.

7 (B) The number of Illinois residents affected by such  
8 incident at the time of notification.

9 (C) Any steps the State agency has taken or plans to  
10 take relating to notification of the breach to consumers.

11 (D) The date and timeframe of the breach, if known at  
12 the time notification is provided.

13 Such notification must be made within 45 days of the State  
14 agency's discovery of the security breach or when the State  
15 agency provides any notice to consumers required by this  
16 Section, whichever is sooner, unless the State agency has good  
17 cause for reasonable delay to determine the scope of the breach  
18 and restore the integrity, security, and confidentiality of the  
19 data system, or when law enforcement requests in writing to  
20 withhold disclosure of some or all of the information required  
21 in the notification under this Section. If the date or  
22 timeframe of the breach is unknown at the time the notice is  
23 sent to the Attorney General, the State agency shall send the  
24 Attorney General the date or timeframe of the breach as soon as  
25 possible.

26 (Source: P.A. 97-483, eff. 1-1-12.)

1 (815 ILCS 530/45 new)

2 Sec. 45. Data security.

3 (a) A data collector that owns or licenses, or maintains or  
4 stores but does not own or license, records that contain  
5 personal information concerning an Illinois resident shall  
6 implement and maintain reasonable security measures to protect  
7 those records from unauthorized access, acquisition,  
8 destruction, use, modification, or disclosure.

9 (b) A contract for the disclosure of personal information  
10 concerning an Illinois resident that is maintained by a data  
11 collector must include a provision requiring the person to whom  
12 the information is disclosed to implement and maintain  
13 reasonable security measures to protect those records from  
14 unauthorized access, acquisition, destruction, use,  
15 modification, or disclosure.

16 (c) If a state or federal law requires a data collector to  
17 provide greater protection to records that contain personal  
18 information concerning an Illinois resident that are  
19 maintained by the data collector and the data collector is in  
20 compliance with the provisions of that state or federal law,  
21 the data collector shall be deemed to be in compliance with the  
22 provisions of this Section.

23 (d) A data collector that is subject to and in compliance  
24 with the standards established pursuant to Section 501(b) of  
25 the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801,

1 shall be deemed to be in compliance with the provisions of this  
2 Section.

3 (815 ILCS 530/50 new)

4 Sec. 50. Entities subject to the federal Health Insurance  
5 Portability and Accountability Act of 1996. Any covered entity  
6 or business associate that is subject to and in compliance with  
7 the privacy and security standards for the protection of  
8 electronic health information established pursuant to the  
9 federal Health Insurance Portability and Accountability Act of  
10 1996 and the Health Information Technology for Economic and  
11 Clinical Health Act shall be deemed to be in compliance with  
12 the provisions of this Act, provided that any covered entity or  
13 business associate required to provide notification of a breach  
14 to the Secretary of Health and Human Services pursuant to the  
15 Health Information Technology for Economic and Clinical Health  
16 Act also provides such notification to the Attorney General  
17 within 5 business days of notifying the Secretary."