

1 AN ACT concerning business.

2 **Be it enacted by the People of the State of Illinois,**  
3 **represented in the General Assembly:**

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  
17 compromises the security, confidentiality, or integrity of  
18 personal information maintained by the data collector. "Breach  
19 of the security of the system data" does not include good faith  
20 acquisition of personal information by an employee or agent of  
21 the data collector for a legitimate purpose of the data  
22 collector, provided that the personal information is not used  
23 for a purpose unrelated to the data collector's business or

1 subject to further unauthorized disclosure.

2 "Health insurance information" means an individual's  
3 health insurance policy number or subscriber identification  
4 number, any unique identifier used by a health insurer to  
5 identify the individual, or any medical information in an  
6 individual's health insurance application and claims history,  
7 including any appeals records.

8 "Medical information" means any information regarding an  
9 individual's medical history, mental or physical condition, or  
10 medical treatment or diagnosis by a healthcare professional,  
11 including such information provided to a website or mobile  
12 application.

13 "Personal information" means either of the following:

14 (1) an individual's first name or first initial and  
15 last name in combination with any one or more of the  
16 following data elements, when either the name or the data  
17 elements are not encrypted or redacted or are encrypted or  
18 redacted but the keys to unencrypt or unredact or otherwise  
19 read the name or data elements have been acquired without  
20 authorization through the breach of security:

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

22 (B) ~~(2)~~ Driver's license number or State  
23 identification card number.

24 (C) ~~(3)~~ Account number or credit or debit card  
25 number, or an account number or credit card number in  
26 combination with any required security code, access

1 code, or password that would permit access to an  
2 individual's financial account.

3 (D) Medical information.

4 (E) Health insurance information.

5 (F) Unique biometric data generated from  
6 measurements or technical analysis of human body  
7 characteristics used by the owner or licensee to  
8 authenticate an individual, such as a fingerprint,  
9 retina or iris image, or other unique physical  
10 representation or digital representation of biometric  
11 data.

12 (2) user name or email address, in combination with a  
13 password or security question and answer that would permit  
14 access to an online account, when either the user name or  
15 email address or password or security question and answer  
16 are not encrypted or redacted or are encrypted or redacted  
17 but the keys to unencrypt or unredact or otherwise read the  
18 data elements have been obtained through the breach of  
19 security.

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

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

24 (815 ILCS 530/10)

25 Sec. 10. Notice of Breach.

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

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

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

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

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

22 The notification shall not, however, include information  
23 concerning the number of Illinois residents affected by the  
24 breach.

25 (2) With respect to personal information defined in  
26 Section 5 in paragraph (2) of the definition of "personal

1 information", notice may be provided in electronic or other  
2 form directing the Illinois resident whose personal  
3 information has been breached to promptly change his or her  
4 user name or password and security question or answer, as  
5 applicable, or to take other steps appropriate to protect  
6 all online accounts for which the resident uses the same  
7 user name or email address and password or security  
8 question and answer.

9 (b) Any data collector that maintains or stores, but does  
10 not own or license, computerized data that includes personal  
11 information that the data collector does not own or license  
12 shall notify the owner or licensee of the information of any  
13 breach of the security of the data immediately following  
14 discovery, if the personal information was, or is reasonably  
15 believed to have been, acquired by an unauthorized person. In  
16 addition to providing such notification to the owner or  
17 licensee, the data collector shall cooperate with the owner or  
18 licensee in matters relating to the breach. That cooperation  
19 shall include, but need not be limited to, (i) informing the  
20 owner or licensee of the breach, including giving notice of the  
21 date or approximate date of the breach and the nature of the  
22 breach, and (ii) informing the owner or licensee of any steps  
23 the data collector has taken or plans to take relating to the  
24 breach. The data collector's cooperation shall not, however, be  
25 deemed to require either the disclosure of confidential  
26 business information or trade secrets or the notification of an

1 Illinois resident who may have been affected by the breach.

2 (b-5) The notification to an Illinois resident required by  
3 subsection (a) of this Section may be delayed if an appropriate  
4 law enforcement agency determines that notification will  
5 interfere with a criminal investigation and provides the data  
6 collector with a written request for the delay. However, the  
7 data collector must notify the Illinois resident as soon as  
8 notification will no longer interfere with the investigation.

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

11 (1) written notice;

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

17 (3) substitute notice, if the data collector  
18 demonstrates that the cost of providing notice would exceed  
19 \$250,000 or that the affected class of subject persons to  
20 be notified exceeds 500,000, or the data collector does not  
21 have sufficient contact information. Substitute notice  
22 shall consist of all of the following: (i) email notice if  
23 the data collector has an email address for the subject  
24 persons; (ii) conspicuous posting of the notice on the data  
25 collector's web site page if the data collector maintains  
26 one; and (iii) notification to major statewide media or, if

1       the breach impacts residents in one geographic area, to  
2       prominent local media in areas where affected individuals  
3       are likely to reside if such notice is reasonably  
4       calculated to give actual notice to persons whom notice is  
5       required.

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

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

16           (815 ILCS 530/12)

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

18           (a) Any State agency that collects personal information  
19      concerning an Illinois resident shall notify the resident at no  
20      charge that there has been a breach of the security of the  
21      system data or written material following discovery or  
22      notification of the breach. The disclosure notification shall  
23      be made in the most expedient time possible and without  
24      unreasonable delay, consistent with any measures necessary to  
25      determine the scope of the breach and restore the reasonable

1 integrity, security, and confidentiality of the data system.  
2 The disclosure notification to an Illinois resident shall  
3 include, but need not be limited to information as follows:

4 (1) With respect to personal information defined in  
5 Section 5 in paragraph (1) of the definition of "personal  
6 information":

7 (i) the toll-free numbers and addresses for  
8 consumer reporting agencies;

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

11 (iii) a statement that the individual can obtain  
12 information from these sources about fraud alerts and  
13 security freezes.

14 (2) With respect to personal information as defined in  
15 Section 5 in paragraph (2) of the definition of "personal  
16 information", notice may be provided in electronic or other  
17 form directing the Illinois resident whose personal  
18 information has been breached to promptly change his or her  
19 user name or password and security question or answer, as  
20 applicable, or to take other steps appropriate to protect  
21 all online accounts for which the resident uses the same  
22 user name or email address and password or security  
23 question and answer.

24 The notification shall not, however, include information  
25 concerning the number of Illinois residents affected by the  
26 breach.



1 (a-5) The notification to an Illinois resident required by  
2 subsection (a) of this Section may be delayed if an appropriate  
3 law enforcement agency determines that notification will  
4 interfere with a criminal investigation and provides the State  
5 agency with a written request for the delay. However, the State  
6 agency must notify the Illinois resident as soon as  
7 notification will no longer interfere with the investigation.

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

10 (1) written notice;

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

16 (3) substitute notice, if the State agency  
17 demonstrates that the cost of providing notice would exceed  
18 \$250,000 or that the affected class of subject persons to  
19 be notified exceeds 500,000, or the State agency does not  
20 have sufficient contact information. Substitute notice  
21 shall consist of all of the following: (i) email notice if  
22 the State agency has an email address for the subject  
23 persons; (ii) conspicuous posting of the notice on the  
24 State agency's web site page if the State agency maintains  
25 one; and (iii) notification to major statewide media.

26 (c) Notwithstanding subsection (b), a State agency that

1 maintains its own notification procedures as part of an  
2 information security policy for the treatment of personal  
3 information and is otherwise consistent with the timing  
4 requirements of this Act shall be deemed in compliance with the  
5 notification requirements of this Section if the State agency  
6 notifies subject persons in accordance with its policies in the  
7 event of a breach of the security of the system data or written  
8 material.

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

19 (e) Notice to Attorney General. Any State agency that  
20 suffers a single breach of the security of the data concerning  
21 the personal information of more than 250 Illinois residents  
22 shall provide notice to the Attorney General of the breach,  
23 including:

24 (A) The types of personal information compromised in  
25 the breach.

26 (B) The number of Illinois residents affected by such

1 incident at the time of notification.

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

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

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

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

20 (815 ILCS 530/45 new)

21 Sec. 45. Data security.

22 (a) A data collector that owns or licenses, or maintains or  
23 stores but does not own or license, records that contain  
24 personal information concerning an Illinois resident shall  
25 implement and maintain reasonable security measures to protect

1 those records from unauthorized access, acquisition,  
2 destruction, use, modification, or disclosure.

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

10 (c) If a state or federal law requires a data collector to  
11 provide greater protection to records that contain personal  
12 information concerning an Illinois resident that are  
13 maintained by the data collector and the data collector is in  
14 compliance with the provisions of that state or federal law,  
15 the data collector shall be deemed to be in compliance with the  
16 provisions of this Section.

17 (d) A data collector that is subject to and in compliance  
18 with the standards established pursuant to Section 501(b) of  
19 the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801,  
20 shall be deemed to be in compliance with the provisions of this  
21 Section.

22 (815 ILCS 530/50 new)

23 Sec. 50. Entities subject to the federal Health Insurance  
24 Portability and Accountability Act of 1996. Any covered entity  
25 or business associate that is subject to and in compliance with

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