

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, 50, and 55 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 "Consumer marketing information" means information related  
3 to a consumer's online browsing history, online search history,  
4 or purchasing history, including, but not limited to, consumer  
5 profiles that are based upon the information. "Consumer  
6 marketing information" does not include information related to  
7 a consumer's online browsing history, online search history, or  
8 purchasing history held by a data collector that has a direct  
9 relationship with the consumer.

10 "Geolocation information" means information generated or  
11 derived from the operation or use of an electronic  
12 communications device that is stored and sufficient to identify  
13 the street name and name of the city or town in which an  
14 individual is located and the information is likely to enable  
15 someone to determine an individual's regular pattern of  
16 behavior. "Geolocation information" does not include the  
17 contents of an electronic communication.

18 "Health insurance information" means an individual's  
19 health insurance policy number or subscriber identification  
20 number, any unique identifier used by a health insurer to  
21 identify the individual, or any information in an individual's  
22 health insurance application and claims history, including any  
23 appeals records.

24 "Medical information" means any information regarding an  
25 individual's medical history, mental or physical condition, or  
26 medical treatment or diagnosis by a healthcare professional,

1 including health information provided to a website or mobile  
2 application.

3 "Personal information" means either of the following:

4 (1) an individual's first name or first initial and  
5 last name in combination with any one or more of the  
6 following data elements, when either the name or the data  
7 elements are not encrypted or redacted or are encrypted or  
8 redacted but the keys to unencrypt or unredact or otherwise  
9 read the name or data elements have been acquired without  
10 authorization through the breach of security:

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

12 (B) ~~(2)~~ Driver's license number or State  
13 identification card number.

14 (C) ~~(3)~~ Account number or credit or debit card  
15 number, or an account number or credit card number in  
16 combination with any required security code, access  
17 code, or password that would permit access to an  
18 individual's financial account.

19 (D) Medical information.

20 (E) Health insurance information.

21 (F) Unique biometric data generated from  
22 measurements or technical analysis of human body  
23 characteristics that could be used to identify an  
24 individual, such as a fingerprint, retina or iris  
25 image, or other unique physical representation or  
26 digital representation of biometric data.

1           (G) Geolocation information.

2           (H) Consumer marketing information.

3           (I) Home address, telephone number, and email  
4           address in combination with either:

5                   (i) mother's maiden name when not part of an  
6                   individual's surname; or

7                   (ii) month, day, and year of birth.

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

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

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

20           (815 ILCS 530/10)

21           Sec. 10. Notice of Breach.

22           (a) Any data collector that owns or licenses personal  
23           information, excluding geolocation information and consumer  
24           marketing information, concerning an Illinois resident shall  
25           notify the resident at no charge that there has been a breach

1 of the security of the system data following discovery or  
2 notification of the breach. The disclosure notification shall  
3 be made in the most expedient time possible and without  
4 unreasonable delay, consistent with any measures necessary to  
5 determine the scope of the breach and restore the reasonable  
6 integrity, security, and confidentiality of the data system.  
7 The disclosure notification to an Illinois resident shall  
8 include, but need not be limited to, information as follows:

9 (1) With respect to personal information as defined in  
10 Section 5 in paragraph (1) of the definition of "personal  
11 information", excluding geolocation information and  
12 consumer marketing information:

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

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

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

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

23 (2) With respect to personal information defined in  
24 Section 5 in paragraph (2) of the definition of "personal  
25 information", notice may be provided in electronic or other  
26 form directing the Illinois resident whose personal

1       information has been breached to promptly change his or her  
2       username or password and security question or answer, as  
3       applicable, or to take other steps appropriate to protect  
4       all online accounts for which the resident uses the same  
5       user name or email address and password or security  
6       question and answer.

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

26      (b-5) The notification to an Illinois resident required by

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

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

9 (1) written notice;

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

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

1       are likely to reside if such notice is reasonably  
2       calculated to give actual notice to persons whom notice is  
3       required.

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

13      (e) Notice to Attorney General.

14      (1) Any data collector that owns or licenses personal  
15      information and suffers a single breach of the security of  
16      the data concerning the personal information of more than  
17      250 Illinois residents shall provide notice to the Attorney  
18      General of the breach, including:

19              (A) The types of personal information compromised  
20              in the breach.

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

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

26              (D) The date and timeframe of the breach, if known



1           at the time notification is provided.

2           Such notification must be made within 30 business days  
3           of the data collector's discovery of the security breach or  
4           when the data collector provides any notice to consumers  
5           required by this Section, whichever is sooner, unless the  
6           data collector has good cause for reasonable delay to  
7           determine the scope of the breach and restore the  
8           integrity, security, and confidentiality of the data  
9           system, or when law enforcement requests in writing to  
10          withhold disclosure of some or all of the information  
11          required in the notification under this Section. If the  
12          date or timeframe of the breach is unknown at the time the  
13          notice is sent to the Attorney General, the data collector  
14          shall send the Attorney General the date or timeframe of  
15          the breach as soon as possible.

16          (2) Any data collector that maintains or stores, but  
17          does not own or license, computerized data that includes  
18          personal information that suffers a single breach of the  
19          security of the data concerning the personal information of  
20          more than 250 Illinois residents shall notify the Attorney  
21          General of the following:

22                (A) The types of personal information compromised  
23                in the breach.

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

26                (C) Any steps the data collector has taken or plans

1           to take relating to notification of the owner or  
2           licensee of the breach and what measures, if any, the  
3           data collector has taken to notify Illinois residents.

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

6           Such notification must be made within 30 business days  
7           of the data collector's discovery of the security breach or  
8           when the data collector provides notice to the owner or  
9           licensee of the information pursuant to this Section,  
10          whichever is sooner, unless the data collector has good  
11          cause for reasonable delay to determine the scope of the  
12          breach and restore the integrity, security, and  
13          confidentiality of the data system, or when law enforcement  
14          requests in writing to withhold disclosure of some or all  
15          of the information required in the notification under this  
16          Section. If the date or timeframe of the breach is unknown  
17          at the time the notice is sent to the Attorney General, the  
18          data collector shall send the Attorney General the date or  
19          timeframe of the breach as soon as possible.

20          (f) Upon receiving notification from a data collector of a  
21          breach of personal information, the Attorney General may  
22          publish the name of the data collector that suffered the  
23          breach, the types of personal information compromised in the  
24          breach, and the date range of the breach.

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

1 (815 ILCS 530/12)

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

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

15 (1) With respect to personal information defined in  
16 Section 5 in paragraph (1) of the definition of "personal  
17 information":

18 (i) the toll-free numbers and addresses for  
19 consumer reporting agencies;

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

22 (iii) a statement that the individual can obtain  
23 information from these sources about fraud alerts and  
24 security freezes.

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

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

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

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

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

(1) written notice;

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

1           (3) substitute notice, if the State agency  
2 demonstrates that the cost of providing notice would exceed  
3 \$250,000 or that the affected class of subject persons to  
4 be notified exceeds 500,000, or the State agency does not  
5 have sufficient contact information. Substitute notice  
6 shall consist of all of the following: (i) email notice if  
7 the State agency has an email address for the subject  
8 persons; (ii) conspicuous posting of the notice on the  
9 State agency's web site page if the State agency maintains  
10 one; and (iii) notification to major statewide media.

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

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

1 to require the State agency to provide to the consumer  
2 reporting agency the names or other personal identifying  
3 information of breach notice recipients.

4 (e) Notice to Attorney General.

5 (1) Any State agency that suffers a single breach of  
6 the security of the data concerning the personal  
7 information of more than 250 Illinois residents shall  
8 provide notice to the Attorney General of the breach,  
9 including:

10 (A) The types of personal information compromised  
11 in the breach.

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

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

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

19 Such notification must be made within 30 business days  
20 of the State agency's discovery of the security breach or  
21 when the State agency provides any notice to consumers  
22 required by this Section, whichever is sooner, unless the  
23 State agency has good cause for reasonable delay to  
24 determine the scope of the breach and restore the  
25 integrity, security, and confidentiality of the data  
26 system, or when law enforcement requests in writing to

1 withhold disclosure of some or all of the information  
2 required in the notification under this Section. If the  
3 date or timeframe of the breach is unknown at the time the  
4 notice is sent to the Attorney General, the State agency  
5 shall send the Attorney General the date or timeframe of  
6 the breach as soon as possible.

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

8 (815 ILCS 530/45 new)

9 Sec. 45. Data security.

10 (a) A data collector that owns or licenses, or maintains or  
11 stores but does not own or license, records that contain  
12 personal information concerning an Illinois resident shall  
13 implement and maintain reasonable security measures to protect  
14 those records from unauthorized access, acquisition,  
15 destruction, use, modification, or disclosure.

16 (b) A contract for the disclosure of personal information  
17 concerning an Illinois resident that is maintained by a data  
18 collector must include a provision requiring the person to whom  
19 the information is disclosed to implement and maintain  
20 reasonable security measures to protect those records from  
21 unauthorized access, acquisition, destruction, use,  
22 modification, or disclosure.

23 (c) If a state or federal law requires a data collector to  
24 provide greater protection to records that contain personal  
25 information concerning an Illinois resident that are

1 maintained by the data collector and the data collector is in  
2 compliance with the provisions of that state or federal law,  
3 the data collector shall be deemed to be in compliance with the  
4 provisions of this Section.

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

10 (815 ILCS 530/50 new)

11 Sec. 50. Posting of privacy policy.

12 (a) As used in this Section:

13 "Conspicuously post" means posting the privacy policy  
14 through any of the following:

15 (1) A Web page on which the actual privacy policy is  
16 posted if the Web page is the homepage or first significant  
17 page after entering the Web site.

18 (2) An icon that hyperlinks to a Web page on which the  
19 actual privacy policy is posted, if the icon is located on  
20 the homepage or the first significant page after entering  
21 the Web site, and if the icon contains the word "privacy".  
22 The icon shall also use a color that contrasts with the  
23 background color of the Web page or is otherwise  
24 distinguishable.

25 (3) A text link that hyperlinks to a Web page on which



1       the actual privacy policy is posted, if the text link is  
2       located on the homepage or first significant page after  
3       entering the Web site, and if the text link does one of the  
4       following:

5               (A) Includes the word "privacy".

6               (B) Is written in capital letters equal to or  
7       greater in size than the surrounding text.

8               (C) Is written in larger type than the surrounding  
9       text, or in contrasting type, font, or color to the  
10       surrounding text of the same size, or set off from the  
11       surrounding text of the same size by symbols or other  
12       marks that call attention to the language.

13               (4) Any other functional hyperlink that is displayed in  
14       a noticeable manner.

15               (5) In the case of an online service, any other  
16       reasonably accessible means of making the privacy policy  
17       available for a consumer of the online service.

18       "Operator" means any person or entity that owns a Web site  
19       located on the Internet or an online service that collects and  
20       maintains personal information from a consumer residing in  
21       Illinois who uses or visits the Web site or online service if  
22       the Web site or online service is operated for commercial  
23       purposes. It does not include any third party that operates,  
24       hosts, or manages, but does not own, a Web site or online  
25       service on the owner's behalf or by processing information on  
26       behalf of the owner.

1       (b) An operator of a commercial Web site or online service  
2       that collects personal information through the Internet about  
3       individual consumers residing in Illinois who use or visit its  
4       commercial Web site or online service shall conspicuously post  
5       its privacy policy on its Web site or, in the case of an  
6       operator of an online service, make the policy available in  
7       accordance with paragraph (5) of subsection (a) of this  
8       Section. An operator shall be in violation of this subdivision  
9       only if the operator fails to post its policy within 30 days  
10       after being notified of noncompliance.

11       (c) The privacy policy required by subsection (b) shall, at  
12       a minimum, do the following:

13               (1) Identify the categories of personal information  
14               that the operator collects through the Web site or online  
15               service about individual consumers who use or visit its  
16               commercial Web site or online service and the categories of  
17               third-party persons or entities with whom the operator may  
18               share that personal information.

19               (2) If the operator maintains a process for an  
20               individual consumer who uses or visits its commercial Web  
21               site or online service to review and request changes to any  
22               of his or her personal information that is collected  
23               through the Web site or online service, provide a  
24               description of that process.

25               (3) Describe the process by which the operator notifies  
26               consumers who use or visit its commercial Web site or

1 online service of material changes to the operator's  
2 privacy policy for that Web site or online service.

3 (4) Identify its effective date.

4 (5) Disclose how the operator responds to Web browser  
5 "do not track" signals or other mechanisms that provide  
6 consumers the ability to exercise choice regarding the  
7 collection of personal information about an individual  
8 consumer's online activities over time and across  
9 third-party Web sites or online services, if the operator  
10 engages in that collection.

11 (6) Disclose whether other parties may collect  
12 personal information about an individual consumer's online  
13 activities over time and across different Web sites or  
14 online services when a consumer uses the operator's Web  
15 site or online service.

16 An operator may satisfy the requirement of paragraph (5) by  
17 providing a clear and conspicuous hyperlink in the operator's  
18 privacy policy to an online location containing a description,  
19 including the effects, of any program or protocol the operator  
20 follows that offers the consumer that choice.

21 (815 ILCS 530/55 new)

22 Sec. 55. Entities subject to the federal Health Insurance  
23 Portability and Accountability Act of 1996. Any covered entity  
24 or business associate that is subject to and in compliance with  
25 the privacy and security standards for the protection of

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