

# SB1833



## 99TH GENERAL ASSEMBLY

### State of Illinois

2015 and 2016

SB1833

Introduced 2/20/2015, by Sen. Daniel Biss

#### SYNOPSIS AS INTRODUCED:

815 ILCS 530/5  
815 ILCS 530/10  
815 ILCS 530/45 new  
815 ILCS 530/50 new

Amends the Personal Information Protection Act. Expands the scope of information to be protected to include medical, health insurance, biometric, consumer marketing, and geolocation information. Requires notice of breaches of security to be provided to the Attorney General. Requires privacy policies to be posted.

LRB099 09064 JLS 31312 b

FISCAL NOTE ACT  
MAY APPLY

A BILL FOR

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 and 10 and by 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 "Consumer marketing information" means information related  
3 to a consumer's online browsing history, online search history,  
4 or purchasing history.

5 "Geolocation information" means information generated or  
6 derived from the operation or use of an electronic  
7 communications device that is sufficient to identify the street  
8 name and name of the city or town in which the device is  
9 located. "Geolocation information" does not include the  
10 contents of an electronic communication.

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

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

22 "Personal information" means either of the following:

23 (1) an individual's first name or first initial and  
24 last name in combination with any one or more of the  
25 following data elements, when either the name or the data  
26 elements are not encrypted or redacted or are encrypted or

1 redacted but the keys to unencrypt or unredact or otherwise  
2 read the name or data elements have been obtained through  
3 the breach of security:

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

5 (B) ~~(2)~~ Driver's license number or State  
6 identification card number.

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

12 (D) Medical information.

13 (E) Health insurance information.

14 (F) Unique biometric data, such as a fingerprint,  
15 retina or iris image, or other unique physical  
16 representation or digital representation of biometric  
17 data.

18 (G) Geolocation information.

19 (H) Consumer marketing information.

20 (I) Any 2 of the following data elements:

21 (i) home address, telephone number, or email  
22 address;

23 (ii) mother's maiden name;

24 (iii) month, day, and year of birth.

25 (2) user name or email address, in combination with a  
26 password or security question and answer that would permit

1       access to an online account, when either the user name or  
2       email address or password or security question and answer  
3       are not encrypted or redacted or are encrypted or redacted  
4       but the keys to unencrypt or unredact or otherwise read the  
5       data elements have been obtained through the breach of  
6       security.

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

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

11           (815 ILCS 530/10)

12           Sec. 10. Notice of Breach.

13           (a) Any data collector that owns or licenses personal  
14       information concerning an Illinois resident shall notify the  
15       resident at no charge that there has been a breach of the  
16       security of the system data following discovery or notification  
17       of the breach. The disclosure notification shall be made in the  
18       most expedient time possible and without unreasonable delay,  
19       consistent with any measures necessary to determine the scope  
20       of the breach and restore the reasonable integrity, security,  
21       and confidentiality of the data system. The disclosure  
22       notification to an Illinois resident shall include, but need  
23       not be limited to, (i) the toll-free numbers and addresses for  
24       consumer reporting agencies, (ii) the toll-free number,  
25       address, and website address for the Federal Trade Commission,

1 and (iii) a statement that the individual can obtain  
2 information from these sources about fraud alerts and security  
3 freezes. The notification shall not, however, include  
4 information concerning the number of Illinois residents  
5 affected by the breach.

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

25 (b-5) The notification to an Illinois resident required by  
26 subsection (a) of this Section may be delayed if an appropriate

1 law enforcement agency determines that notification will  
2 interfere with a criminal investigation and provides the data  
3 collector with a written request for the delay. However, the  
4 data collector must notify the Illinois resident as soon as  
5 notification will no longer interfere with the investigation.

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

8 (1) written notice;

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

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

1       calculated to give actual notice to persons whom notice is  
2       required.

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

12      (e) Notice to Attorney General.

13      (1) Any data collector required to issue notice  
14      pursuant to this Section to more than 100 Illinois  
15      residents as a result of a single breach of the security  
16      system shall provide notice to the Attorney General of the  
17      breach, including:

18              (A) a description of the nature of the breach of  
19              security or unauthorized acquisition or use.

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

22              (C) any steps the data collector has taken or plans  
23              to take relating to the incident.

24      Such notification must be made within 14 business days  
25      of the data collector's discovery of the security breach,  
26      or when the data collector provides notice to consumers



1 pursuant to this Section, whichever is sooner. If the date  
2 of the breach is unknown at the time the notice is sent to  
3 the Attorney General, the data collector shall send the  
4 Attorney General the date of the breach as soon as  
5 possible.

6 (2) Any data collector that maintains or stores, but  
7 does not own or license, computerized data that includes  
8 personal information that is required to notify the owner  
9 or licensee of the information that there has been a breach  
10 of the security of the data, shall notify the Attorney  
11 General of the following:

12 (A) a description of the nature of the breach of  
13 security or unauthorized acquisition or use.

14 (B) the number of Illinois residents affected by  
15 such incident at the time of notification.

16 (C) any steps the data collector has taken or plans  
17 to take relating to the incident, including the steps  
18 the data collector has taken to inform the owner or  
19 licensee of the breach and what measures, if any, the  
20 data collector has taken to notify Illinois residents.

21 Such notification must be made within 14 business days  
22 of the data collector's discovery of the security breach,  
23 or when the data collector provides notice to the owner or  
24 licensee of the information pursuant to this section,  
25 whichever is sooner. If the date of the breach is unknown  
26 at the time the notice is sent to the Attorney General, the

1 data collector shall send the Attorney General the date of  
2 the breach as soon as possible.

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

4 (815 ILCS 530/45 new)

5 Sec. 45. Data security.

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

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

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

1 (815 ILCS 530/50 new)

2 Sec. 50. Posting of privacy policy.

3 (a) As used in this Section:

4 "Conspicuously post" means posting the privacy policy  
5 through any of the following:

6 (1) A Web page on which the actual privacy policy is  
7 posted if the Web page is the homepage or first significant  
8 page after entering the Web site.

9 (2) An icon that hyperlinks to a Web page on which the  
10 actual privacy policy is posted, if the icon is located on  
11 the homepage or the first significant page after entering  
12 the Web site, and if the icon contains the word "privacy."  
13 The icon shall also use a color that contrasts with the  
14 background color of the Web page or is otherwise  
15 distinguishable.

16 (3) A text link that hyperlinks to a Web page on which  
17 the actual privacy policy is posted, if the text link is  
18 located on the homepage or first significant page after  
19 entering the Web site, and if the text link does one of the  
20 following:

21 (A) Includes the word "privacy".

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

24 (C) Is written in larger type than the surrounding  
25 text, or in contrasting type, font, or color to the

1 surrounding text of the same size, or set off from the  
2 surrounding text of the same size by symbols or other  
3 marks that call attention to the language.

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

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

9 "Operator" means any person or entity that owns a Web site  
10 located on the Internet or an online service that collects and  
11 maintains personal information from a consumer residing in  
12 Illinois who uses or visits the Web site or online service if  
13 the Web site or online service is operated for commercial  
14 purposes. It does not include any third party that operates,  
15 hosts, or manages, but does not own, a Web site or online  
16 service on the owner's behalf or by processing information on  
17 behalf of the owner.

18 (b) An operator of a commercial Web site or online service  
19 that collects personal information through the Internet about  
20 individual consumers residing in Illinois who use or visit its  
21 commercial Web site or online service shall conspicuously post  
22 its privacy policy on its Web site or online service. An  
23 operator shall be in violation of this subdivision only if the  
24 operator fails to post its policy within 30 days after being  
25 notified of noncompliance.

26 (c) The privacy policy required by subsection (b) shall, at

1 a minimum, do the following:

2 (1) Identify the categories of personal information  
3 that the operator collects through the Web site or online  
4 service about individual consumers who use or visit its  
5 commercial Web site or online service and the categories of  
6 third-party persons or entities with whom the operator may  
7 share that personal information.

8 (2) If the operator maintains a process for an  
9 individual consumer who uses or visits its commercial Web  
10 site or online service to review and request changes to any  
11 of his or her personal information that is collected  
12 through the Web site or online service, provide a  
13 description of that process.

14 (3) Describe the process by which the operator notifies  
15 consumers who use or visit its commercial Web site or  
16 online service of material changes to the operator's  
17 privacy policy for that Web site or online service.

18 (4) Identify its effective date.

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

26 (6) Disclose whether other parties may collect

1       personal information about an individual consumer's online  
2       activities over time and across different Web sites or  
3       online services when a consumer uses the operator's Web  
4       site or online service.

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