

SB2353



102ND GENERAL ASSEMBLY

State of Illinois

2021 and 2022

SB2353

Introduced 2/26/2021, by Sen. Michael E. Hastings

SYNOPSIS AS INTRODUCED:

815 ILCS 530/10

Amends the Personal Information Protection Act. Provides that data collectors that maintain or store, but do not own or license, computerized data that includes personal information and that are required to issue notice pursuant to this Section to the owner or licensee of the information that there has been a breach of the security of the data shall notify the Attorney General regarding the breach. Effective immediately.

LRB102 05119 JLS 15140 b

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 Section 10 as follows:

6 (815 ILCS 530/10)

7 Sec. 10. Notice of breach; notice to Attorney General.

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

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

22 (A) the toll-free numbers and addresses for
23 consumer reporting agencies;

1 (B) the toll-free number, address, and website
2 address for the Federal Trade Commission; and

3 (C) a statement that the individual can obtain
4 information from these sources about fraud alerts and
5 security freezes.

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
9 other form directing the Illinois resident whose personal
10 information has been breached to promptly change his or
11 her user name or password and security question or answer,
12 as applicable, or to take other steps appropriate to
13 protect all online accounts for which the resident uses
14 the same user name or email address and password or
15 security question and answer.

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

19 (b) Any data collector that maintains or stores, but does
20 not own or license, computerized data that includes personal
21 information that the data collector does not own or license
22 shall notify the owner or licensee of the information of any
23 breach of the security of the data immediately following
24 discovery, if the personal information was, or is reasonably
25 believed to have been, acquired by an unauthorized person. In
26 addition to providing such notification to the owner or

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

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

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

23 (1) written notice;

24 (2) electronic notice, if the notice provided is
25 consistent with the provisions regarding electronic
26 records and signatures for notices legally required to be

1 in writing as set forth in Section 7001 of Title 15 of the
2 United States Code; or

3 (3) substitute notice, if the data collector
4 demonstrates that the cost of providing notice would
5 exceed \$250,000 or that the affected class of subject
6 persons to be notified exceeds 500,000, or the data
7 collector does not have sufficient contact information.

8 Substitute notice shall consist of all of the following:

9 (i) email notice if the data collector has an email
10 address for the subject persons; (ii) conspicuous posting
11 of the notice on the data collector's web site page if the
12 data collector maintains one; and (iii) notification to
13 major statewide media or, if the breach impacts residents
14 in one geographic area, to prominent local media in areas
15 where affected individuals are likely to reside if such
16 notice is reasonably calculated to give actual notice to
17 persons whom notice is required.

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

1 (e) (1) This subsection does not apply to data collectors
2 that are covered entities or business associates and are in
3 compliance with Section 50.

4 (2) Any data collector required to issue notice pursuant
5 to this Section to more than 500 Illinois residents as a result
6 of a single breach of the security system shall provide notice
7 to the Attorney General of the breach, including:

8 (A) A description of the nature of the breach of
9 security or unauthorized acquisition or use.

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

12 (C) Any steps the data collector has taken or plans to
13 take relating to the incident.

14 (3) Any data collector that maintains or stores, but does
15 not own or license, computerized data that includes personal
16 information and that is required to issue notice pursuant to
17 this Section to the owner or licensee of the information that
18 there has been a breach of the security of the data shall
19 notify the Attorney General of the following:

20 (A) A description of the nature of the breach of
21 security or unauthorized acquisition or use.

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

24 (C) Any steps the data collector has taken or plans to
25 take relating to the incident.

26 (4) Notifications required under paragraphs (2) and (3) of

1 this subsection ~~Such notification~~ must be made in the most
2 expedient time possible and without unreasonable delay but in
3 no event later than when the data collector provides notice to
4 consumers pursuant to this Section. If the date of the breach
5 is unknown at the time the notice is sent to the Attorney
6 General, the data collector shall send the Attorney General
7 the date of the breach as soon as possible.

8 Upon receiving notification pursuant to paragraph (2) or
9 (3) of this subsection from a data collector of a breach of
10 personal information, the Attorney General may publish the
11 name of the data collector that suffered the breach, the types
12 of personal information compromised in the breach, and the
13 date range of the breach.

14 (Source: P.A. 100-201, eff. 8-18-17; 101-343, eff. 1-1-20.)

15 Section 99. Effective date. This Act takes effect upon
16 becoming law.