

# HB4174



## 100TH GENERAL ASSEMBLY

### State of Illinois

2017 and 2018

**HB4174**

by Rep. Barbara Wheeler

#### SYNOPSIS AS INTRODUCED:

815 ILCS 530/10  
815 ILCS 530/12

Amends the Personal Information Protection Act. Requires any data collector that owns or licenses personal information concerning an Illinois resident and any State agency that collects personal information concerning an Illinois resident to notify the resident of any security breach of the system data within 48 hours of discovery of the breach (rather than requiring notification in the most expedient time possible and without unreasonable delay).

LRB100 15879 KTG 30990 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 10 and 12 as follows:

6 (815 ILCS 530/10)

7 Sec. 10. Notice of breach.

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 notification  
12 of the breach. The disclosure notification shall be made within  
13 48 hours of discovery of the breach ~~in the most expedient time~~  
14 ~~possible and without unreasonable delay~~, consistent with any  
15 measures necessary to determine the scope of the breach and  
16 restore the reasonable integrity, security, and  
17 confidentiality of the data system. The disclosure  
18 notification to an Illinois resident shall include, but need  
19 not be limited to, information as follows:

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

23 (A) the toll-free numbers and addresses for

1 consumer reporting agencies;

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

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

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

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

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

1 addition to providing such notification to the owner or  
2 licensee, the data collector shall cooperate with the owner or  
3 licensee in matters relating to the breach. That cooperation  
4 shall include, but need not be limited to, (i) informing the  
5 owner or licensee of the breach, including giving notice of the  
6 date or approximate date of the breach and the nature of the  
7 breach, and (ii) informing the owner or licensee of any steps  
8 the data collector has taken or plans to take relating to the  
9 breach. The data collector's cooperation shall not, however, be  
10 deemed to require either the disclosure of confidential  
11 business information or trade secrets or the notification of an  
12 Illinois resident who may have been 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 appropriate  
15 law enforcement agency determines that notification will  
16 interfere with a criminal investigation and provides the data  
17 collector with a written request for the delay. However, the  
18 data collector must notify the Illinois resident as soon as  
19 notification will no longer interfere with the investigation.

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

22 (1) written notice;

23 (2) electronic notice, if the notice provided is  
24 consistent with the provisions regarding electronic  
25 records and signatures for notices legally required to be  
26 in writing as set forth in Section 7001 of Title 15 of the

1 United States Code; or

2 (3) substitute notice, if the data collector  
3 demonstrates that the cost of providing notice would exceed  
4 \$250,000 or that the affected class of subject persons to  
5 be notified exceeds 500,000, or the data collector does not  
6 have sufficient contact information. Substitute notice  
7 shall consist of all of the following: (i) email notice if  
8 the data collector has an email address for the subject  
9 persons; (ii) conspicuous posting of the notice on the data  
10 collector's web site page if the data collector maintains  
11 one; and (iii) notification to major statewide media or, if  
12 the breach impacts residents in one geographic area, to  
13 prominent local media in areas where affected individuals  
14 are likely to reside if such notice is reasonably  
15 calculated to give actual notice to persons whom notice is  
16 required.

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

26 (Source: P.A. 99-503, eff. 1-1-17; 100-201, eff. 8-18-17.)

1 (815 ILCS 530/12)

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

3 (a) Any State agency that collects personal information  
4 concerning an Illinois resident shall notify the resident at no  
5 charge that there has been a breach of the security of the  
6 system data or written material following discovery or  
7 notification of the breach. The disclosure notification shall  
8 be made within 48 hours of discovery of the breach ~~in the most~~  
9 ~~expedient time possible and without unreasonable delay,~~  
10 consistent with any measures necessary to determine the scope  
11 of the breach and restore the reasonable integrity, security,  
12 and confidentiality of the data system. The disclosure  
13 notification to an Illinois resident shall include, but need  
14 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

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

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

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

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

22 (1) written notice;

23 (2) electronic notice, if the notice provided is  
24 consistent with the provisions regarding electronic  
25 records and signatures for notices legally required to be  
26 in writing as set forth in Section 7001 of Title 15 of the

1 United States Code; or

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

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

21 (d) If a State agency is required to notify more than 1,000  
22 persons of a breach of security pursuant to this Section, the  
23 State agency shall also notify, without unreasonable delay, all  
24 consumer reporting agencies that compile and maintain files on  
25 consumers on a nationwide basis, as defined by 15 U.S.C.  
26 Section 1681a(p), of the timing, distribution, and content of



1 the notices. Nothing in this subsection (d) shall be construed  
2 to require the State agency to provide to the consumer  
3 reporting agency the names or other personal identifying  
4 information of breach notice recipients.

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

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

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

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

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

18 Such notification must be made within 45 days of the State  
19 agency's discovery of the security breach or when the State  
20 agency provides any notice to consumers required by this  
21 Section, whichever is sooner, unless the State agency has good  
22 cause for reasonable delay to determine the scope of the breach  
23 and restore the integrity, security, and confidentiality of the  
24 data system, or when law enforcement requests in writing to  
25 withhold disclosure of some or all of the information required  
26 in the notification under this Section. If the date or

1 timeframe of the breach is unknown at the time the notice is  
2 sent to the Attorney General, the State agency shall send the  
3 Attorney General the date or timeframe of the breach as soon as  
4 possible.

5 (f) In addition to the report required by Section 25 of  
6 this Act, if the State agency that suffers a breach determines  
7 the identity of the actor who perpetrated the breach, then the  
8 State agency shall report this information, within 5 days after  
9 the determination, to the General Assembly, provided that such  
10 report would not jeopardize the security of Illinois residents  
11 or compromise a security investigation.

12 (g) A State agency directly responsible to the Governor  
13 that has been subject to or has reason to believe it has been  
14 subject to a single breach of the security of the data  
15 concerning the personal information of more than 250 Illinois  
16 residents or an instance of aggravated computer tampering, as  
17 defined in Section 17-53 of the Criminal Code of 2012, shall  
18 notify the Office of the Chief Information Security Officer of  
19 the Illinois Department of Innovation and Technology and the  
20 Attorney General regarding the breach or instance of aggravated  
21 computer tampering. The notification shall be made without  
22 delay, but no later than 72 hours following the discovery of  
23 the incident.

24 Upon receiving notification of such incident, the Chief  
25 Information Security Officer shall without delay take  
26 necessary and reasonable actions to:

1           (i) assess the incident to determine the potential  
2           impact on the overall confidentiality, security, and  
3           availability of State of Illinois data and information  
4           systems;

5           (ii) ensure the security incident is contained to  
6           minimize additional impact and risk to the State;

7           (iii) identify the root cause of the incident;

8           (iv) provide recommendations to the impacted State  
9           agency to assist with eradicating the threat and removing  
10           and mitigating any vulnerabilities to reduce the risk of  
11           further compromise; and

12           (v) assist the impacted State agency in any necessary  
13           recovery efforts to ensure effective return to a state of  
14           normal operations.

15           The Department of Innovation and Technology may agree to  
16           submit the reports required in subsections (e) and (f) of this  
17           Section and in Section 25 in lieu of the impacted agency.

18           (h) Upon receiving notification from a State agency of a  
19           breach of personal information or from the Department of  
20           Innovation and Technology in lieu of the impacted agency, the  
21           Attorney General may publish the name of the State agency that  
22           suffered the breach, the types of personal information  
23           compromised in the breach, and the date range of the breach.

24           (Source: P.A. 99-503, eff. 1-1-17; 100-412, eff. 8-25-17.)