

# SB0707



## 100TH GENERAL ASSEMBLY

### State of Illinois

2017 and 2018

SB0707

Introduced 1/30/2017, by Sen. Michael E. Hastings

#### SYNOPSIS AS INTRODUCED:

815 ILCS 530/12

Amends the Personal Information Protection Act. Provides that a State agency that has been subject to a single breach or aggravated computer tampering to the security of its data shall submit a comprehensive report to the Attorney General and the General Assembly. Specifies the content of the report. Requires the report to be made available to the public. Effective immediately.

LRB100 08839 JLS 18980 b

FISCAL NOTE ACT  
MAY APPLY

A BILL FOR

1 AN ACT concerning cybersecurity.

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 12 as follows:

6 (815 ILCS 530/12)

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

8 (a) Any State agency that collects personal information  
9 concerning an Illinois resident shall notify the resident at no  
10 charge that there has been a breach of the security of the  
11 system data or written material 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 defined in  
20 Section 5 in paragraph (1) of the definition of "personal  
21 information":

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

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

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

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

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

26           (b) For purposes of this Section, notice to residents may

1 be provided by one of the following methods:

2 (1) written notice;

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

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

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

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

11 (e) Notice to Attorney General. Any State agency that  
12 suffers a single breach of the security of the data concerning  
13 the personal information of more than 250 Illinois residents  
14 shall provide notice to the Attorney General of the breach,  
15 including:

16 (A) The types of personal information compromised in  
17 the breach.

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

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

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

24 Such notification must be made within 45 days of the State  
25 agency's discovery of the security breach or when the State  
26 agency provides any notice to consumers required by this

1 Section, whichever is sooner, unless the State agency has good  
2 cause for reasonable delay to determine the scope of the breach  
3 and restore the integrity, security, and confidentiality of the  
4 data system, or when law enforcement requests in writing to  
5 withhold disclosure of some or all of the information required  
6 in the notification under this Section. If the date or  
7 timeframe of the breach is unknown at the time the notice is  
8 sent to the Attorney General, the State agency shall send the  
9 Attorney General the date or timeframe of the breach as soon as  
10 possible.

11 (f) Any State agency that has been subject to a single  
12 breach or aggravated computer tampering to the security of its  
13 data shall submit a comprehensive report to both the Attorney  
14 General and the General Assembly to disclose in specified ways  
15 any breach of the security of the system or data following  
16 discovery or notification of the security breach.

17 (g) In accordance with subsection (e), the notification  
18 must be made within 45 days after the State agency's discovery  
19 of the security breach or aggravated computer tampering.  
20 Nonetheless, a State agency subject to a single breach or  
21 aggravated computer tampering is also required to present a  
22 comprehensive and searchable Adobe PDF report to both the  
23 Attorney General and the General Assembly outlining in  
24 specified ways any breach of the security of the system or data  
25 following discovery or notification of the security breach. The  
26 report shall include the following:

1           (i) an executive summary;  
2           (ii) a timeline of events concerning the breach;  
3           (iii) a description of the attack;  
4           (iv) the named actors; and  
5           (v) an overview of corrective and preventative  
6           measures implemented.

7           (h) After receiving the comprehensive report, the Attorney  
8           General shall immediately make the report available to the  
9           public without unreasonable delay and consistent with the  
10           legitimate needs of law enforcement in order to determine the  
11           scope of the breach and measures necessary to restore the  
12           reasonable integrity, security, and confidentiality of the  
13           data system. Both the Attorney General and the State agency  
14           shall publish the results of the report on its respective  
15           Internet websites indefinitely after submission.

16           (Source: P.A. 99-503, eff. 1-1-17.)

17           Section 99. Effective date. This Act takes effect upon  
18           becoming law.