AN ACT concerning business.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 5. The Personal Information Protection Act is amended by changing Section 10 as follows:

(815 ILCS 530/10)

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

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

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

(A) the toll-free numbers and addresses for consumer reporting agencies;
(B) the toll-free number, address, and website
address for the Federal Trade Commission; and

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

(2) With respect to personal information defined in
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.

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

(b-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 data
collector with a written request for the delay. However, the
data collector must notify the Illinois resident as soon as
notification will no longer interfere with the investigation.

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

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

(e)(1) This subsection does not apply to data collectors that are covered entities or business associates and are in
(2) Any data collector required to issue notice pursuant to this Section to more than 500 Illinois residents as a result of a single breach of the security system shall provide notice to the Attorney General of the breach, including:

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

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

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

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

Upon receiving notification from a data collector of a breach of personal information, the Attorney General may publish the name of the data collector that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.

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