HB3025

LRB09706857AEK46950b

97TH GENERAL ASSEMBLY

State of Illinois

2011 and 2012

HB3025

Introduced 2/23/2011, by Rep. Kelly Burke

SYNOPSIS AS INTRODUCED:

815 ILCS 530/5
815 ILCS 530/10
815 ILCS 530/12
815 ILCS 530/35 new
815 ILCS 530/40 new

Amends the Personal Information Protection Act. Provides that "breach of the security of the system data" includes the unauthorized use (instead of only the unauthorized acquisition) of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector. Provides that a data collector that owns or licenses personal information shall notify the Attorney General of a breach. Provides that a data collector that maintains or stores (instead of only maintains) computerized or other data (instead of only computerized data) that includes personal information must cooperate with the owner or licensee of the information in relation to a breach. Requires that notification of a breach sent to an Illinois resident by a data collector that owns or licenses personal information or by a State agency must contain certain information, including information concerning placing a security freeze on the release of information from the resident's credit report. Sets forth the Attorney General's duties upon receiving notice of a security breach, as well as additional duties of data collectors and State agencies. Sets forth standards for disposal of materials containing personal information, and provides penalties for a violation.

LRB097 06857 AEK 46950 b

FISCAL NOTE ACT MAY APPLY

STATE MANDATES ACT MAY REQUIRE REIMBURSEMENT

A BILL FOR

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 Sections 5, 10, and 12 and by adding Sections 35 and 40 as follows:

(815 ILCS 530/5)

Sec. 5. Definitions. In this Act:

"Data Collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

"Breach of the security of the system data" or "breach" means unauthorized acquisition or use of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or

subject to further unauthorized disclosure.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(1) Social Security number.

(2) Driver's license number or State identification card number.

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

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

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/10)

Sec. 10. Notice of Breach.

(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 concerning (i) the resident's right to obtain a police report relating to the breach, (ii) how the resident may request a security freeze pursuant to Section 2MM of the Consumer Fraud and Deceptive Business Practices Act and the necessary information that must be provided when requesting the security freeze, and (iii) any fees that must be paid to a consumer reporting agency in connection with a request for a security freeze. The notification shall not, however, include information concerning the nature of the breach or the number of Illinois residents affected by the breach.

In addition, a data collector that owns or licenses such personal information shall notify the Attorney General of the breach. The notification to the Attorney General shall include, but need not be limited to, information concerning (i) the nature of the breach, (ii) the number of Illinois residents affected by the breach at the time of notification, and (iii) any steps the data collector has taken or plans to take relating to 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.

(d) Notwithstanding subsection (c), 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.

(Source: P.A. 94-36, eff. 1-1-06; 94-947, eff. 6-27-06.)

(815 ILCS 530/12)

Sec. 12. Notice of breach; State agency.

(a) Any State agency that collects 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 or written material 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 concerning (i) the resident's right to obtain a police report relating to the breach, (ii) how the resident may request a security freeze pursuant to Section 2MM of the Consumer Fraud and Deceptive Business Practices Act and the necessary information that must be provided when requesting the security freeze, and (iii) any fees that must be paid to a consumer reporting agency in connection with a request for a security freeze. The notification to an Illinois resident shall not, however, include information concerning the nature of the breach or the number of Illinois residents affected by the breach.

(b) For purposes of this Section, notice to residents 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 State agency 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 State agency does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the State agency has an email address for the subject persons; (ii) conspicuous posting of the notice on the State agency's web site page if the State agency maintains one; and (iii) notification to major statewide media.

(c) Notwithstanding subsection (b), a State agency 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 State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.

(d) If a State agency is required to notify more than 1,000 persons of a breach of security pursuant to this Section, the State agency shall also notify, without unreasonable delay, all

consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/35 new)

Sec. 35. Attorney General's duties; data collector; State agencies.

(a) Upon receiving notification of a breach of the security of the system data from a data collector under subsection (a) of Section 10, the Attorney General shall identify any relevant consumer reporting agency or State agency, as deemed appropriate by the Attorney General, and forward the names of the identified consumer reporting agencies and State agencies to the data collector who provided the notification. The data collector shall thereafter, as soon as practicable and without unreasonable delay, also provide notification of the breach to each consumer reporting agency and State agency identified by the Attorney General.

(b) A State agency that receives notification of a breach of the security of the system data from a data collector under subsection (a) of this Section shall provide written

notification of the nature and circumstances of the breach to the Department of Central Management Services as soon as practicable and without unreasonable delay. The agency shall thereafter comply with all policies and procedures adopted by the Department of Central Management Services pertaining to the reporting and investigation of a breach of the security of the system data.

(815 ILCS 530/40 new)

Sec. 40. Disposal of materials containing personal information; Attorney General.

(a) In this Section, "person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.

(b) When disposing of materials containing personal information, a person must meet the following minimum standards for proper disposal of such materials:

(1) Paper documents containing personal information must be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.

(2) Electronic media and other non-paper media containing personal information must be destroyed or

erased so that personal information cannot practicably be read or reconstructed.

(c) Any person disposing of materials containing personal information may contract with a third party to dispose of such materials in accordance with this Section. Any third party that contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.

(d) Any person who violates this Section is subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed $50,000 for each instance of improper disposal of materials containing personal information. The Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any penalty imposed under this Section.

(e) In addition to the authority to impose a civil penalty under subsection (d), the Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.