HB5454

LRB10336595JRC66704b

103RD GENERAL ASSEMBLY

State of Illinois

2023 and 2024

HB5454

Introduced 2/9/2024, by Rep. Carol Ammons

SYNOPSIS AS INTRODUCED:

815 ILCS 530/5
815 ILCS 530/10
815 ILCS 530/60 new

Amends the Personal Information Protection Act. Provides protections for social media users and creates a private cause of action for them if their accounts have been hacked and not restored by social media websites under certain circumstances. Defines a social media website as an Internet website or mobile application that enables users to communicate with each other by posting information, comments, messages, or images; is open to the public; has more than 75 million subscribers; and has never been specifically affiliated with any religion or political party. Provides that, if a court finds that a social media website has violated this Act, the court may award actual damages computed at a rate of $1,000 per violation per day and reasonable attorney's fees and costs incurred in maintaining that civil action. Requires the social media website to restore access to the user's online account within 24 hours of the discovery of the security breach; provide notice of the breach of security within seven days of the discovery; and provide instructions for restoring the integrity of the user's online account of a social media website in compliance with this Act.

LRB103 36595 JRC 66704 b

A BILL FOR

AN ACT concerning civil actions.

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 and 10 and by adding Section 60 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 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.

"Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records.

"Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application.

"Personal information" means either of the following:

(1) 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 or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

(A) Social Security number.

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

(C) 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.

(D) Medical information.

(E) Health insurance information.

(F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

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

"Social media website" means an Internet website or mobile application that enables users to communicate with each other by posting information, comments, messages, or images, and

that meets the following criteria: is open to the public; has more than 75,000,000 subscribers; and has never been specifically affiliated with any religion or political party.

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

(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 compliance with Section 50.

(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.

(f) In accordance with federal law, any business that operates a social media website shall, within 24 hours of discovery of a breach of security to a user whose online account or personal information was, or is reasonably believed

to have been, accessed by an unauthorized person, determine the scope of the breach of security and restore the reasonable integrity of, and access to, the online account to the user. Any discovery of breach of security shall be documented in writing by the business that operates the social media website and retained for 5 years.

(g) Within 7 days of the discovery of the breach of security to a user's account, the business that operates the social media website shall provide clear and conspicuous notice delivered to the user through the email and mobile phone number that was associated with the online account prior to the breach of security.

(h) The business that operates the social media website shall include within the notification instructions that directs the customer whose online account has been breached to promptly change any password and security question or answer, as applicable, and to take other appropriate steps to protect and restore the integrity of the online account of the social media website.

(i) The Department of Innovation and Technology may promulgate rules and regulations necessary to effectuate this subsection.

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

(815 ILCS 530/60 new)

Sec. 60. Private cause of action for violation of this Act

by a business operating a social media website.

(a) Any user of a social media website may bring an action in any court of competent jurisdiction following the discovery of a breach of security by the business that operates the social media website, if the user:

(1) has not had access restored to the user's online account within 24 hours of the discovery of the security breach as required by this Act;

(2) has not been provided notice of the breach of security within seven days of such discovery, as required by this Act; or

(3) has not been provided instructions for restoring the integrity of the user's online account of a social media website in compliance with this Act.

(b) If a court of competent jurisdiction finds that a social media website has violated this Section, the court may award actual damages computed at a rate of $1,000 per violation per day and reasonable attorney's fees and costs incurred in maintaining that civil action.

(c) This private right of action authorized pursuant to this Section does not supplant any other claim or cause of action available to a customer under common law or by statute. The provisions of this subsection are in addition to any other common law and statutory remedies.

(d) Nothing in this Section may be construed as creating a private right of action against the State or any political

subdivision.