AN ACT concerning cybersecurity.

**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 12 as follows:

(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 as follows:

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

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

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

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

(2) With respect to personal information as 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.

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

(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.

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

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

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

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

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

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

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

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

(g) A State agency directly responsible to the Governor that has been subject to or has reason to believe it has been subject to a single breach of the security of the data concerning the personal information of more than 250 Illinois residents or an instance of aggravated computer tampering, as defined in Section 17-53 of the Criminal Code of 2012, shall notify the Office of the Chief Information Security Officer of the Illinois Department of Innovation and Technology and the Attorney General regarding the breach or instance of aggravated

computer tampering. The notification shall be made without delay, but no later than 72 hours following the discovery of the incident.

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

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

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

(iii) identify the root cause of the incident;

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

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

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

(h) Upon receiving notification from a State agency of a breach of personal information or from the Department of Innovation and Technology in lieu of the impacted agency, the

Attorney General may publish the name of the State agency 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.)

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