PRINTER'S NO. 289

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 308

Session of 2019

INTRODUCED BY PHILLIPS-HILL, LAUGHLIN, FOLMER, MENSCH, K. WARD AND J. WARD, FEBRUARY 19, 2019

REFERRED TO COMMUNICATIONS AND TECHNOLOGY, FEBRUARY 19, 2019

AN ACT

Amending the act of December 22, 2005 (P.L.474, No.94), entitled "An act providing for the notification of residents whose personal information data was or may have been disclosed due to a security system breach; and imposing penalties," further providing for definitions and for notification of breach; and providing for contents and nature of notice and for storage policies.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. The definitions of "notice" and "personal information" in section 2 of the act of December 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, are amended and the section is amended by adding definitions to read:

Section 2. Definitions.

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

* * *

"Health insurance information." Any of the following regarding an individual:

(1) The individual's health insurance policy number or subscriber identification number.

(2) A unique identifier used by a health insurer to identify the individual.

(3) Information in the individual's application and claims history, including any appeals records.

* * *

"Medical information." Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

"Notice." May be provided by any of the following methods of notification:

(1) Written notice to the last known home address for the individual.

(2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.

(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.

(4) (i) Substitute notice, if the entity demonstrates one of the following:

(A) The cost of providing notice would exceed $100,000.

(B) The affected class of subject persons to be notified exceeds 175,000.

(C) The entity does not have sufficient contact information.

(ii) Substitute notice shall consist of all of the following:

(A) E-mail notice when the entity has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the entity's publicly accessible Internet website if the entity maintains one. The posting shall occur for a minimum of 30 days and provide a link to the notice on the home page of the website or on the first significant page after entering the website.

(C) Notification to major Statewide media.

"Personal information." As follows:

(1) [An] The term includes an individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

(i) Social Security number.

(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.

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

(1.1) The term also includes any of the following:

(i) Health insurance information.

(ii) Medical information.

(iii) Educational records.

(iv) Income or other socioeconomic information.

(v) Religious information or information regarding other beliefs.

(vi) Information regarding food purchases.

(vii) Unique biometric data generated from measurements or technical analyses of human body characteristics, including, but not limited to, a fingerprint, voice print, retinal or iris image or any other unique physical representation or digital representation of biometric data.

(viii) Geolocation data.

(ix) Information or data collected through the use or operation of an automated license plate recognition system.

(x) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

(2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.

* * *

Section 2. Section 3(a) of the act is amended and the section is amended by adding a subsection to read:

Section 3. Notification of breach.

(a) General rule.--

(1) An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the

system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.

(2) Except as provided in subsection (d) or section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay.

(3) For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

* * *

(d) Notification by specific entities.--

(1) If a State agency is the subject of the breach of the security of the system, the State agency shall notify the following:

(i) The head of the State agency within two hours of the detection of the breach of the security of the system.

(ii) The Governor's Office of Administration and the office of Attorney General within four hours of the detection of the breach of the security of the system.

(2) If a political subdivision of the Commonwealth is the subject of the breach of the security of the system, the political subdivision shall notify the following:

(i) The head of the political subdivision of the Commonwealth within two hours of the detection of the breach of the security of the system.

(ii) The district attorney of the county in which the political subdivision is located within three business days of the detection of the breach of the security of the system.

(3) If an individual or a business doing business in this Commonwealth is the subject of the breach of the security of the system, the individual or business shall notify the following:

(i) The district attorney of the county in which the business is located within three business days of the detection of the breach of the security of the system.

(ii) Individuals affected by the breach of the security of the system within 14 days of the detection of the breach of the security of the system.

(4) Notification under this subsection shall occur regardless of whether the notice exemption applies under section 7.

Section 3. The act is amended by adding sections to read:

Section 3.1. Contents and nature of notice.

(a) Mandatory contents.--Each written, e-mail or website notice under this act shall include, at a minimum, the following:

(1) The name and contact information of the entity providing the notice.

(2) The date of the notice.

(3) A list of the types of personal information that were or are reasonably believed to have been the subject of the breach of the security of the system.

(4) If possible to determine at the time the notice is

provided, all of the following:

(i) The date of the breach of the security of the system.

(ii) The estimated date of the breach of the security of the system.

(iii) The date range within which the breach of the security of the system occurred.

(5) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(6) A statement regarding whether notice was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(7) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach of the security of the system exposed an individual's Social Security number, driver's license number or State identification card number issued in lieu of a driver's license.

(8) Information regarding the steps taken to protect the individuals whose personal information is the subject of the breach of the security of the system.

(9) An offer by the entity providing the notice to provide free credit reports, credit protection and identity theft protection for 12 months to each individual affected by the breach of the security of the system.

(10) Advice on steps that the individual affected by the breach of the security of the system may take to protect the individual.

(b) Mandatory format.--Each written, e-mail or website notice under this act shall:

(1) Be written in plain language.

(2) Be titled "Notice of Data Breach."

(3) Present the information under the following headings:

(i) "What Happened."

(ii) "What Information Was Involved."

(iii) "What We Are Doing."

(iv) "What You Can Do."

(v) "For More Information."

(4) Provide for the possibility of additional information to be provided as a supplement to the notice.

(5) Be designed to call attention to the nature and significance of the information contained in the notice.

(6) Display the title, headings and text of the notice in a clear and conspicuous manner.

(7) Provide that the text of the notice and any other written notification provided under this section be no smaller than 10-point type.

Section 9. Storage policies.

(a) Development.--The head of each State agency, whether or not under the Governor's jurisdiction, the Court Administrator of Pennsylvania and the administrators of the legislative caucuses of the Senate and House of Representatives shall develop policies for the offices under their jurisdiction to govern the safe and proper storage of computerized data containing personal information and other sensitive personally identifiable information. A goal of the policies shall be to reduce the risk of future breaches of the security of the system.

(b) Subject matter.--As permitted by Federal or State law or regulation, the policies developed under subsection (a) shall address:

(1) identifying, collecting, maintaining, displaying, restoring, protecting and transferring personally identifiable information;

(2) using personally identifiable information in test environments;

(3) remediating the negative effects concerning the breach or corruption of personally identifiable information stored on legacy systems; and

(4) other relevant issues.

(c) Considerations.--In developing the policies under subsection (a), consideration shall be given to Federal and State law and regulations, similar existing policies in other states, best practices identified by other states, relevant studies and other sources as appropriate.

(d) Review.--The policies developed under this section shall be reviewed at least annually and updated as necessary.

Section 4. This act shall take effect in 120 days.