PRINTER'S NO. 1367

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1181 Session of 2019

INTRODUCED BY FRITZ, ROTHMAN, MILLARD, FRANKEL, SCHLOSSBERG, GALLOWAY, BERNSTINE, WILLIAMS, BROWN, DeLUCA, KAUFER, OBERLANDER, JOZWIAK, PICKETT AND RADER, APRIL 10, 2019

REFERRED TO COMMITTEE ON STATE GOVERNMENT, APRIL 10, 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, for notification of breach and for notice exemption.

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

Section 1. The definitions of "breach of the security of the system," "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:

"Breach of the security of the system." The unauthorized [access and acquisition of computerized data that materially

compromises] access and acquisition of unencrypted data, or encrypted data with the confidential process or key required to decrypt the data, that is likely to compromise the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

"Bureau." The Bureau of Consumer Protection in the Office of Attorney General.

* * *

"Discovery." The final determination that a breach of the security of the system has occurred, including, but not limited to, the final determination regarding material compromise of security and reasonable causation of loss or injury.

* * *

"Health insurance information." An individual's health insurance policy number or subscriber identification number.

* * *

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

"Notice." The term shall include notice of residents and notice of Commonwealth.

"Notice of Commonwealth." Written notice to the Director of

the Bureau of Consumer Protection of the Office of Attorney General.

"Notice of residents." [May be provided by any] For residents of this Commonwealth, 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 Internet website if the entity maintains one.

(C) Notification to major Statewide media.

"Personal information." As follows:

(1) 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 elements are not encrypted or redacted:

[(1) 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.] The following identification numbers:

(A) Social Security number.

(B) Driver's license number.

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

(D) Passport number.

(E) Taxpayer identification number.

(F) Medical Information.

(G) Health insurance information.

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

(iv) Biometric data, meaning data gathered by measurement of the human body, including fingerprints,

voice prints, eyes, retinas or irises, that is used by the owner or licensee to uniquely authenticate the identity of a person when the individual accesses a system or 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[.] or from another publicly available source, including news reports, periodicals, public social media posts or other widely distributed media.

* * *

Section 2. Section 3 of the act is amended to read:

Section 3. Notification of breach.

(a) General rule.--An entity that [maintains, stores or manages] owns or licenses 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]. Except as provided in 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.] within 45 days of discovery of the breach of the security of the system by the owner or licensee. 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.

[(b) Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.]

(c) Vendor notification.--A vendor that maintains, stores or manages computerized data on behalf of [another entity] an owner or licensee of personal information shall provide notice of any breach of the security system following discovery by the vendor to the [entity] owner or licensee on whose behalf the vendor maintains, stores or manages the data. The [entity] owner or licensee shall be responsible for making the determinations and discharging any remaining duties under this act.

(d) Notice to residents of this Commonwealth.--

(1) Notification must be in plain language.

(2) Notice of the breach of the security of the system under this section shall be made to the affected residents of this Commonwealth and must include the following:

(i) The date, estimated date or date range of the breach of the security of the system.

(ii) Whether the notification was delayed as a result of a law enforcement investigation.

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

(iv) A general description of the breach of the security of the system.

(v) Toll-free telephone numbers and addresses of consumer reporting agencies if the breach of the security of the system exposed a Social Security number or a

government-issued identification card number.

(vi) The name and contact information of the reporting agency that was notified under section 5.

(3) The entity providing notice under this subsection may include information about what the entity has done to protect affected individuals and offer advice on what steps affected individuals may take to protect their information and what steps the individual whose information has been breached may take to protect himself or herself.

(4) Notice under this subsection shall be made within 45 days of discovery of the breach of the security of the system by the owner or licensee.

(e) Notice to Attorney General.--

(1) When notice of the breach of the security of the system under this section must be given to more than 1,000 affected individuals in this Commonwealth, the notice shall be made to the bureau not less than five days prior to the notice to affected individuals under subsection (d).

(2) Notice under this subsection must include the nature of the breach of the security of the system.

(3) Notice under this subsection must include, no later than the time notice is given to the residents of this Commonwealth, the following:

(i) The number of residents of this Commonwealth affected by the breach of the security of the system.

(ii) Steps taken by the entity relating to the breach of the security of the system.

(f) State agencies.--If a State agency is the subject of a breach of security of the system, the State agency must provide notice of the breach of security of the system required under

subsection (a) without unreasonable delay following discovery of the breach. A State agency under the Governor's jurisdiction shall provide notice of a breach of the security of the system to the Governor's Office of Administration without unreasonable delay. Notification under this subsection shall occur notwithstanding the procedures and policies under section 7.

(g) Counties, school districts and municipalities.--A county, school district or municipality shall provide notice to the district attorney in the county in which the breach occurred of a breach of the security of the system required under subsection (a) without unreasonable delay following discovery of the breach. Notification under this subsection shall occur notwithstanding the procedures and policies under section 7.

Section 3. Section 7(b) of the act is amended by adding a paragraph to read:

Section 7. Notice exemption.

* * *

(b) Compliance with Federal requirements.--

* * *

(3) If an entity does not have a Federal or State notification rule, regulation, procedure or guideline in effect, the entity must comply with this act.

Section 4. This act shall take effect in 60 days.