PRINTER'S NO. 214

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 245 Session of 2019

INTRODUCED BY KENYATTA, JANUARY 28, 2019

REFERRED TO COMMITTEE ON COMMERCE, JANUARY 28, 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; providing for privacy agreements; further providing for notification of breach; and providing for disposal of materials containing personal information.

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

Section 1. The definitions of "breach of the security of the system" 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 a definition 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 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.

* * *

"Cybersecurity coordinator." An individual responsible for overseeing information and communications systems and ensuring the information contained therein is protected and defended against damage, unauthorized use or modification or exploitation.

* * *

"Personal information."

(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 either the name or the data elements are not encrypted or redacted:

(i) [Social Security number.] Identification numbers, such as:

(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) Patient identification number.

(G) Insurance member number.

(H) Employee identification number.

(ii) [Driver's license number or a State identification card number issued in lieu of a driver's license.] Other associated names, such as:

(A) Maiden name.

(B) Mother's maiden name.

(C) Alias.

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

(iv) Electronic identifier or routing code, in combination with any required security code, access code or password that would permit access to an individual's financial account.

(v) Electronic account information, such as account name or user name.

(vi) Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular individual or small, well-defined group of individuals.

(vii) Biometric data, such as genetic information, a fingerprint, facial scan, retina or iris image, voice signature, x-ray image or other unique physical representation or digital representation of biometric data.

(viii) Date of birth.

(ix) Place of birth.

(x) Insurance information.

(xi) Employment information.

(xii) Education information.

(xiii) Vehicle information, such as:

(A) Registration number.

(B) Title number.

(xiv) Contact information, such as:

(A) Telephone number.

(B) Address.

(C) E-mail address.

(xv) Digitized or other electronic signature.

(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. The act is amended by adding a section to read:

Section 2.1. Privacy agreements.

An agreement regarding the privacy of personal information shall be written in plain language with clarity and conciseness so that it is easily read and understood by the public.

Section 3. Section 3(a) of the act is amended to read:

Section 3. Notification of breach.

(a) General rule.--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. Notice shall also be provided to the Attorney General and the

Cybersecurity Coordinator. 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] no later than 30 days after discovery of the breach. 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.

* * *

Section 4. The act is amended by adding a section to read:

Section 5.1. Disposal of materials containing personal information.

(a) Method of disposal.--A person shall dispose of material containing personal information in a manner that renders the personal information unreadable, unusable and undecipherable. Proper disposal methods include, but are not limited to:

(1) Redaction, burning, pulverization or shredding of paper documents so that personal information cannot practicably be read or reconstructed.

(2) Destruction or erasure of electronic media and other nonpaper media so that personal information cannot practicably be read or reconstructed.

(b) Third party contracts.--A person disposing of materials containing personal information may contract with a third party to dispose of the materials in accordance with this section. A third party that contracts with a person to dispose of materials containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to, acquisition of or use of personal

information during the collection, transportation and disposal of materials containing personal information.

(c) Penalties.--A person, including a third party referenced in subsection (b), 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 hearing. The Attorney General may file a civil action in the appropriate court of common pleas to recover a penalty imposed under this section.

(d) Action by Attorney General.--In addition to the authority to impose a civil penalty under subsection (c), the Attorney General may bring an action in the appropriate court of common pleas to remedy a violation of this section, seeking any appropriate relief.

(e) Exceptions.--A financial institution subject to 15 U.S.C. Ch. 94 (relating to privacy) or a person subject to 15 U.S.C. § 1681w (relating to disposal of records) is exempt from this section.

Section 5. This act shall take effect in 60 days.