AN ACT

ENTITLED, An Act to provide for the notification related to a breach of certain data and to provide a penalty therefor.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF SOUTH DAKOTA:

Section 1. That chapter 22-40 be amended by adding a NEW SECTION to read:

Terms in this Act mean:

(1) "Breach of system security," the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. The term does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure;

(2) "Encrypted," computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key or in accordance with the Federal Information Processing Standard 140-2 in effect on January 1, 2018;

(3) "Information holder," any person or business that conducts business in this state, and that owns or licenses computerized personal or protected information of residents of this state;

(4) "Personal information," a person's first name or first initial and last name, in combination with any one or more of the following data elements:

(a) Social security number;

(b) Driver license number or other unique identification number created or collected by a government body;

(c) Account, credit card, or debit card number, in combination with any required

security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account;

(d) Health information as defined in 45 CFR 160.103; or

(e) An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes.

The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable; and

(5) "Protected information," includes:

(a) A user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and

(b) Account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account;

(6) "Unauthorized person," any person not authorized to acquire or disclose personal information, or any person authorized by the information holder to access personal information who has acquired or disclosed the personal information outside the guidelines for access of disclosure established by the information holder.

Section 2. That chapter 22-40 be amended by adding a NEW SECTION to read:

Following the discovery by or notification to an information holder of a breach of system security an information holder shall disclose in accordance with section 4 of this Act the breach of system security to any resident of this state whose personal or protected information was, or is reasonably

believed to have been, acquired by an unauthorized person. A disclosure under this section shall be made not later than sixty days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement as provided under section 3 of this Act. An information holder is not required to make a disclosure under this section if, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person. The information holder shall document the determination under this section in writing and maintain the documentation for not less than three years.

Any information holder that experiences a breach of system security under this section shall disclose to the attorney general by mail or electronic mail any breach of system security that exceeds two hundred fifty residents of this state.

Section 3. That chapter 22-40 be amended by adding a NEW SECTION to read:

A notification required under section 2 of this Act may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, the notification shall be made not later than thirty days after the law enforcement agency determines that notification will not compromise the criminal investigation.

Section 4. That chapter 22-40 be amended by adding a NEW SECTION to read:

A disclosure under section 2 of this Act may be provided by:

(1) Written notice;

(2) Electronic notice, if the electronic notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 in effect as of January 1, 2018, or if the information holder's primary method of communication with the resident of this state has been by electronic means; or

(3) Substitute notice, if the information holder demonstrates that the cost of providing notice

would exceed two hundred fifty thousand dollars, that the affected class of persons to be notified exceeds five hundred thousand persons, or that the information holder does not have sufficient contact information and the notice consists of each of the following:

(a) Email notice, if the information holder has an email address for the subject persons;

(b) Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and

(c) Notification to statewide media.

Section 5. That chapter 22-40 be amended by adding a NEW SECTION to read:

Notwithstanding section 4 of this Act, if an information holder maintains its own notification procedure as part of an information security policy for the treatment of personal or protected information and the policy is otherwise consistent with the timing requirements of this section, the information holder is in compliance with the notification requirements of section 4 of this Act if the information holder notifies each person in accordance with the information holder's policies in the event of a breach of system security.

Section 6. That chapter 22-40 be amended by adding a NEW SECTION to read:

If an information holder discovers circumstances that require notification pursuant to section 2 of this Act the information holder shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice.

Section 7. That chapter 22-40 be amended by adding a NEW SECTION to read:

The attorney general may prosecute each failure to disclose under the provisions of this Act as a deceptive act or practice under § 37-24-6. In addition to any remedy provided under chapter 37-24,

the attorney general may bring an action to recover on behalf of the state a civil penalty of not more than ten thousand dollars per day per violation. The attorney general may recover attorney's fees and any costs associated with any action brought under this section.

Section 8. That chapter 22-40 be amended by adding a NEW SECTION to read:

Notwithstanding any other provisions in this Act, any information holder that is regulated by federal law or regulation, including the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, as amended) or the Gramm Leach Bliley Act (15 U.S.C. § 6801 et seq., as amended) and that maintains procedures for a breach of system security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional federal regulator is deemed to be in compliance with this chapter if the information holder notifies affected South Dakota residents in accordance with the provisions of the applicable federal law or regulation.

An Act to provide for the notification related to a breach of certain data and to provide a penalty therefor.

==========

I certify that the attached Act originated in the

SENATE as Bill No. 62

_____
Secretary of the Senate

==========

_____
President of the Senate

Attest:

_____
Secretary of the Senate

_____
Speaker of the House

Attest:

_____
Chief Clerk

Senate Bill No. 62
File No. ____
Chapter No. _____

==========

Received at this Executive Office this _____ day of _____ ,

20____ at _____ M.

By _____
for the Governor

==========

The attached Act is hereby approved this _____ day of _____ , A.D., 20___

_____
Governor

==========

STATE OF SOUTH DAKOTA,
ss.
Office of the Secretary of State

Filed _____ , 20___
at _____ o'clock __ M.

_____
Secretary of State

By _____
Asst. Secretary of State