AN ACT

relating to cybercrime; creating criminal offenses.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. This Act may be cited as the Texas Cybercrime Act.

SECTION 2. Section 33.01, Penal Code, is amended by amending Subdivision (2) and adding Subdivisions (11-a), (13-a), (13-b), (13-c), and (15-a) to read as follows:

(2) "Aggregate amount" means the amount of:

(A) any direct or indirect loss incurred by a victim, including the value of money, property, or service stolen, appropriated, or rendered unrecoverable by the offense; or

(B) any expenditure required by the victim to:

(i) determine whether data or [~~verify that~~] a computer, computer network, computer program, or computer system was [~~not~~] altered, acquired, appropriated, damaged, deleted, or disrupted by the offense; or

(ii) attempt to restore, recover, or replace any data altered, acquired, appropriated, damaged, deleted, or disrupted.

(11-a) "Decryption," "decrypt," or "decrypted" means the decoding of encrypted communications or information, whether by use of a decryption key, by breaking an encryption formula or algorithm, or by the interference with a person's use of an encryption service in a manner that causes

information or communications to be stored or transmitted without encryption.

(13-a) "Encrypted private information" means encrypted data, documents, wire or electronic communications, or other information stored on a computer or computer system, whether in the possession of the owner or a provider of an electronic communications service or a remote computing service, and which has not been accessible to the public.

(13-b) "Encryption," "encrypt," or "encrypted" means the encoding of data, documents, wire or electronic communications, or other information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized access to, such information.

(13-c) "Encryption service" means a computing service, a computer device, computer software, or technology with encryption capabilities, and includes any subsequent version of or update to an encryption service.

(15-a) "Privileged information" means:

(A) protected health information, as that term is defined by Section 182.002, Health and Safety Code;

(B) information that is subject to the attorney-client privilege; or

(C) information that is subject to the accountant-client privilege under Section 901.457, Occupations Code, or other law, if the

information is on a computer, computer network, or computer system owned by a person possessing a license issued under Subchapter H, Chapter 901, Occupations Code.

SECTION 3. Chapter 33, Penal Code, is amended by adding Sections 33.022, 33.023, and 33.024 to read as follows:

Sec. 33.022. ELECTRONIC ACCESS INTERFERENCE. (a) A person, other than a network provider or online service provider acting for a legitimate business purpose, commits an offense if the person intentionally interrupts or suspends access to a computer system or computer network without the effective consent of the owner.

(b) An offense under this section is a third degree felony.

(c) It is a defense to prosecution under this section that the person acted with the intent to facilitate a lawful seizure or search of, or lawful access to, a computer, computer network, or computer system for a legitimate law enforcement purpose.

Sec. 33.023. ELECTRONIC DATA TAMPERING. (a) In this section, "ransomware" means a computer contaminant or lock that restricts access by an unauthorized person to a computer, computer system, or computer network or any data in a computer, computer system, or computer network under circumstances in which a person demands money, property, or a service to remove the computer contaminant or lock, restore access to the computer,

computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock.

(b) A person commits an offense if the person intentionally alters data as it transmits between two computers in a computer network or computer system through deception and without a legitimate business purpose.

(c) A person commits an offense if the person intentionally introduces ransomware onto a computer, computer network, or computer system through deception and without a legitimate business purpose.

(d) Subject to Subsections (d-1) and (d-2), an offense under this section is a Class C misdemeanor.

(d-1) Subject to Subsection (d-2), if it is shown on the trial of the offense that the defendant acted with the intent to defraud or harm another, an offense under this section is:

(1) a Class C misdemeanor if the aggregate amount involved is less than $100 or cannot be determined;

(2) a Class B misdemeanor if the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the aggregate amount involved is $750 or more but less than $2,500;

(4) a state jail felony if the aggregate amount involved is $2,500 or more but less than $30,000;

(5) a felony of the third degree if the aggregate amount involved

is $30,000 or more but less than $150,000;

(6) a felony of the second degree if the aggregate amount involved is $150,000 or more but less than $300,000; and

(7) a felony of the first degree if the aggregate amount involved is $300,000 or more.

(d-2) If it is shown on the trial of the offense that the defendant knowingly restricted a victim's access to privileged information, an offense under this section is:

(1) a state jail felony if the value of the aggregate amount involved is less than $2,500;

(2) a felony of the third degree if:

(A) the value of the aggregate amount involved is $2,500 or more but less than $30,000; or

(B) a client or patient of a victim suffered harm attributable to the offense;

(3) a felony of the second degree if:

(A) the value of the aggregate amount involved is $30,000 or more but less than $150,000; or

(B) a client or patient of a victim suffered bodily injury attributable to the offense; and

(4) a felony of the first degree if:

(A) the value of the aggregate amount involved is $150,000 or more; or

(B) a client or patient of a victim suffered serious bodily injury or death attributable to the offense.

(e) When benefits are obtained, a victim is defrauded or harmed, or property is altered, appropriated, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, appropriation, damage, or deletion of property may be aggregated in determining the grade of the offense.

(f) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

(g) Software is not ransomware for the purposes of this section if the software restricts access to data because:

(1) authentication is required to upgrade or access purchased content; or

(2) access to subscription content has been blocked for nonpayment.

Sec. 33.024. UNLAWFUL DECRYPTION. (a) A person commits an offense if the person intentionally decrypts encrypted private information through

deception and without a legitimate business purpose.

(b) Subject to Subsections (b-1) and (b-2), an offense under this section is a Class C misdemeanor.

(b-1) Subject to Subsection (b-2), if it is shown on the trial of the offense that the defendant acted with the intent to defraud or harm another, an offense under this section is:

(1) a Class C misdemeanor if the value of the aggregate amount involved is less than $100 or cannot be determined;

(2) a Class B misdemeanor if the value of the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the value of the aggregate amount involved is $750 or more but less than $2,500;

(4) a state jail felony if the value of the aggregate amount involved is $2,500 or more but less than $30,000;

(5) a felony of the third degree if the value of the aggregate amount involved is $30,000 or more but less than $150,000;

(6) a felony of the second degree if the value of the aggregate amount involved is $150,000 or more but less than $300,000; and

(7) a felony of the first degree if the value of the aggregate amount involved is $300,000 or more.

(b-2) If it is shown on the trial of the offense that the defendant

knowingly decrypted privileged information, an offense under this section is:

(1) a state jail felony if the value of the aggregate amount involved is less than $2,500;

(2) a felony of the third degree if:

(A) the value of the aggregate amount involved is $2,500 or more but less than $30,000; or

(B) a client or patient of a victim suffered harm attributable to the offense;

(3) a felony of the second degree if:

(A) the value of the aggregate amount involved is $30,000 or more but less than $150,000; or

(B) a client or patient of a victim suffered bodily injury attributable to the offense; and

(4) a felony of the first degree if:

(A) the value of the aggregate amount involved is $150,000 or more; or

(B) a client or patient of a victim suffered serious bodily injury or death attributable to the offense.

(c) It is a defense to prosecution under this section that the actor's conduct was pursuant to an agreement entered into with the owner for the

purpose of:

(1) assessing or maintaining the security of the information or of a computer, computer network, or computer system; or

(2) providing other services related to security.

(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

SECTION 4. Section 33.03, Penal Code, is amended to read as follows:

Sec. 33.03. DEFENSES. It is an affirmative defense to prosecution under Section 33.02 or 33.022 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

SECTION 5. The change in law made by this Act applies only to an offense committed on or after the effective date of this Act. An offense committed before the effective date of this Act is governed by the law in effect on the date the offense was committed, and the former law is continued in effect for that purpose. For purposes of this section, an offense was committed before the effective date of this Act if any element of the offense occurred before that date.

SECTION 6. This Act takes effect September 1, 2017.

_____ _____

President of the Senate Speaker of the House

I certify that H.B. No. 9 was passed by the House on April 13, 2017, by the following vote: Yeas 139, Nays 0, 2 present, not voting; and that the House concurred in Senate amendments to H.B. No. 9 on May 26, 2017, by the following vote: Yeas 142, Nays 0, 2 present, not voting.

_____

Chief Clerk of the House

I certify that H.B. No. 9 was passed by the Senate, with amendments, on May 24, 2017, by the following vote: Yeas 31, Nays 0.

_____

Secretary of the Senate

APPROVED: _____

Date

_____

Governor