PRIOR PRINTER'S NO. 829 PRINTER'S NO. 1326

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 726 Session of 2021

INTRODUCED BY PHILLIPS-HILL, ARGALL, MARTIN, PITTMAN AND STEFANO, MAY 28, 2021

AS AMENDED ON THIRD CONSIDERATION, JANUARY 18, 2022

AN ACT

Amending Title 18 (Crimes and Offenses) of the Pennsylvania Consolidated Statutes, in computer offenses, providing for the offense of ransomware; and imposing duties on the Office of Administration.

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

Section 1. Chapter 76 of Title 18 of the Pennsylvania Consolidated Statutes is amended by adding a subchapter to read:

SUBCHAPTER F

RANSOMWARE

Sec.

§ 7671. Purposes of subchapter.

This subchapter is intended to ensure that Commonwealth agencies have strong capabilities in place to:

(1) Prohibit persons from engaging in ransomware attacks and from extorting payments to resolve or prevent ransomware attacks.

(2) Prevent and detect ransomware attacks.

(3) Restore systems and captured information quickly that were disrupted or obtained through ransomware attacks.

(4) Provide timely public notification of ransomware attacks.

(5) Pursue and prosecute perpetrators of ransomware attacks.

§ 7672. Definitions.

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

"Commonwealth agency." Any of the following:

(1) The Governor's Office.

(2) A department, board, commission, authority or other agency of the Commonwealth that is subject to the policy supervision and control of the Governor.

(3) The office of Lieutenant Governor.

(4) An independent department.

(5) An independent agency.

(6) A municipality.

(7) A school district.

(8) An intermediate unit.

(9) An area career and technical school.

(10) A charter school, cyber charter school or regional charter school, as those terms are defined in section 1703-A of the Public School Code of 1949.

(11) A community college, as defined in section 1901-A of the Public School Code of 1949.

(12) A State-owned institution.

(13) A State-related institution.

(14) A court or agency of the unified judicial system.

(15) The General Assembly or an agency of the General Assembly.

"Computer contaminant." A set of computer instructions that is designed to modify, damage, destroy, record or transmit data held by a computer, computer system or computer network without the intent or permission of the owner of the data.

"Independent agency." A board, commission, authority or other agency of the Commonwealth that is not subject to the policy supervision and control of the Governor.

"Independent department." Any of the following:

(1) The Department of the Auditor General.

(2) The Treasury Department.

(3) The Office of Attorney General.

(4) A board or commission of an entity under paragraph (1), (2) or (3).

"Municipality." A county, city, borough, incorporated town or township.

"Public School Code of 1949." ~~Act~~ The act of March 10, 1949 **<--** (P.L.30, No.14), known as the Public School Code of 1949.

"Ransomware." As follows:

(1) A computer contaminant or lock placed or introduced without authorization into a computer, computer system or computer network that does any of the following:

(i) Restricts access by an authorized person to the computer, computer system or computer network or to any data held by the computer, computer system or computer network, under circumstances in which the person responsible for the placement or introduction of the computer contaminant or lock demands payment of money or other consideration to:

(A) remove the computer contaminant or lock;

(B) restore access to the computer, computer system, computer network or data; or

(C) otherwise remediate the impact of the computer contaminant or lock.

(ii) Transforms data held by the computer, computer system or computer network into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

(2) The term does not include authentication required to upgrade or access purchased content or the blocking of access to subscription content in the case of nonpayment for the access.

"State-owned institution." An institution that is part of the State System of Higher Education under Article XX-A of the Public School Code of 1949 and all branches and campuses of a State-owned institution.

"State-related institution." The Pennsylvania State University, including the Pennsylvania College of Technology, the University of Pittsburgh, Temple University and Lincoln

University and their branch campuses.

§ 7673. Prohibited actions.

(a) General rule.--Except as provided in subsection (b), a person may not, with the intent to extort money or other consideration from another person or a Commonwealth agency for the purpose of removing a computer contaminant or lock, restoring access to a computer, computer system, computer network or data or otherwise remediating the impact of a computer contaminant or lock:

(1) Knowingly possess ransomware.

(2) Use ransomware without the authorization of the owner of the computer, computer system or computer network.

(3) Sell, transfer or develop ransomware.

(4) Threaten to use ransomware against another person or a Commonwealth agency if the threat is:

(i) made in an express or implied manner; and

(ii) transmitted in person, by mail or through facsimile, e-mail, the Internet, a telecommunication device or other electronic means.

(5) Induce another person to commit an act described in paragraph (1), (2), (3) or (4).

(b) Exception.--Subsection (a) does not apply to the use of ransomware for research purposes by an authorized agent of the Commonwealth or the Federal Government.

§ 7674. Grading of offense.

(a) General rule.--Except as provided in subsection (b), if a person is convicted of, found guilty of or pleads guilty or nolo contendere in a court of record to an offense specified in section 7673 (relating to prohibited actions), the person shall be subject to the following:

(1) If the aggregate amount of money or other consideration involved in the offense is less than $10,000, the penalties applicable to a misdemeanor of the first degree.

(2) If the aggregate amount of money or other consideration involved in the offense is at least $10,000 but less than $100,000, the penalties applicable to a felony of the third degree.

(3) If the aggregate amount of money or other consideration involved in the offense is at least $100,000 but less than $500,000, the penalties applicable to a felony of the second degree.

(4) If the aggregate amount of money or other consideration involved in the offense is at least $500,000, the penalties applicable to a felony of the first degree.

(b) Exception.--For an offense under subsection (a)(1), (2) or (3), the offense shall be classified one degree higher than the classification specified under the respective paragraph of subsection (a) if the commission of the offense:

(1) is a second or subsequent offense;

(2) involves the infliction of a physical injury; or

(3) involves a computer, computer system or computer network, or any data held by the computer, computer system or computer network, of a court or agency of the unified judicial system.

§ 7675. Forfeiture.

~~(a) Authorization. Upon a conviction, finding of guilty or plea of guilty or nolo contendere to an offense under this subchapter, the court may, in addition to any other sentence authorized under law, direct the forfeiture of any computer,~~ <--

~~computer system, computer network, software or data that is used during the commission of the offense or used as a repository for the storage of software or data illegally obtained in violation of this subchapter.~~

(A) AUTHORIZATION.--ANY COMPUTER, COMPUTER SYSTEM, COMPUTER NETWORK, SOFTWARE OR DATA THAT IS USED DURING THE COMMISSION OF AN OFFENSE UNDER THIS SUBCHAPTER OR USED AS A REPOSITORY FOR THE STORAGE OF SOFTWARE OR DATA ILLEGALLY OBTAINED IN VIOLATION OF THIS SUBCHAPTER SHALL BE SUBJECT TO FORFEITURE. <--

(b) Procedures.--The forfeiture under this section shall be conducted in accordance with 42 Pa.C.S. §§ 5803 (relating to asset forfeiture), 5805 (relating to forfeiture procedure), 5806 (relating to motion for return of property), 5807 (relating to restrictions on use), 5807.1 (relating to prohibition on adoptive seizures) and 5808 (relating to exceptions).

§ 7676. Limitation of time.

An action to prosecute an offense under this subchapter must be commenced within three years from the date of discovery of the commission of the offense.

§ 7677. Notification.

~~(a) Managed service providers. A managed service provider of information technology in the service of a Commonwealth agency shall notify an appropriate official of the Commonwealth agency of the discovery of ransomware or of an extortion attempt involving ransomware within one hour of the discovery.~~ <--

~~(b) Commonwealth agencies.--Within two hours of a Commonwealth agency's discovery of ransomware or of an extortion attempt involving ransomware against the Commonwealth agency, the Commonwealth agency shall:~~

~~(1) As necessary and appropriate, notify the Office of~~

~~Administration and an entity with jurisdiction or supervision over the Commonwealth agency of the ransomware or extortion attempt, in which case the Office of Administration or entity shall, within two hours of the notification by the Commonwealth agency, notify an appropriate official of the Federal Bureau of Investigation of the ransomware or extortion attempt.~~

~~(2) If notification to the Office of Administration or entity is not provided under paragraph (1), notify an appropriate official of the Federal Bureau of Investigation of the ransomware or extortion attempt.~~

(A) MANAGED SERVICE PROVIDERS.--A MANAGED SERVICE PROVIDER OF INFORMATION TECHNOLOGY IN THE SERVICE OF A COMMONWEALTH AGENCY SHALL NOTIFY AN APPROPRIATE OFFICIAL OF THE COMMONWEALTH AGENCY OF THE DISCOVERY OF RANSOMWARE OR RECEIPT OF A RANSOMWARE DEMAND WITHIN ONE HOUR OF THE DISCOVERY OF RANSOMWARE OR RECEIPT OF THE RANSOMWARE DEMAND. <--

(B) COMMONWEALTH AGENCIES.--

(1) WITHIN TWO HOURS OF A COMMONWEALTH AGENCY'S DISCOVERY OF RANSOMWARE OR RECEIPT OF A RANSOMWARE DEMAND, THE COMMONWEALTH AGENCY SHALL, AS NECESSARY AND APPROPRIATE, NOTIFY THE OFFICE OF ADMINISTRATION AND AN ENTITY WITH JURISDICTION OR SUPERVISION OVER THE COMMONWEALTH AGENCY OF THE DISCOVERY OF RANSOMWARE OR RECEIPT OF A RANSOMWARE DEMAND.

(2) IF A COMMONWEALTH AGENCY OR MANAGED SERVICE PROVIDER IS IN RECEIPT OF A RANSOMWARE DEMAND, THE OFFICE OF ADMINISTRATION SHALL, WITHIN 24 HOURS OF THE NOTIFICATION BY THE COMMONWEALTH AGENCY OF THE RANSOMWARE DEMAND, NOTIFY AN APPROPRIATE OFFICIAL OF THE FEDERAL BUREAU OF INVESTIGATION

OF THE RANSOMWARE DEMAND.

§ 7678. Payments.

(a) General rule.--Except as provided in subsection (b), notwithstanding any other provision of law, after December 31, 2021, State and local taxpayer money or other public money may not be used to pay an extortion attempt involving ransomware.

(b) Exception.--Subsection (a) does not apply if the Governor authorizes a Commonwealth agency to expend public money for payment to a person responsible for, or reasonably believed to be responsible for, the commission of an offense under this subchapter, in the event of a declaration of disaster emergency under 35 Pa.C.S. § 7301 (relating to general authority of Governor).

(C) INSURANCE COVERAGE.--NOTHING IN THIS SECTION SHALL <-- PROHIBIT A COMMONWEALTH AGENCY FROM EXPENDING PUBLIC MONEY FOR THE PURPOSES OF PURCHASING OR MAINTAINING INSURANCE COVERAGE FOR RANSOMWARE ATTACKS, INCLUDING THE PAYMENT OF ANY DEDUCTIBLE OR COINSURANCE BY THE COMMONWEALTH AGENCY THAT IS REQUIRED UNDER THE TERMS OF THE INSURANCE POLICY. THE FOLLOWING APPLY:

(1) THE COMMONWEALTH AGENCY MAY NOT USE PUBLIC MONEY DESIGNATED FOR INSURANCE COVERAGE TO PAY AN EXTORTION ATTEMPT INVOLVING RANSOMWARE.

(2) SUBJECT TO PARAGRAPH (1), PUBLIC MONEY DESIGNATED FOR INSURANCE COVERAGE MAY BE USED TO PAY COSTS ASSOCIATED WITH:

(I) THE RECOVERY AND RESTORATION OF SYSTEMS AND CAPTURED INFORMATION AS A RESULT OF A RANSOMWARE ATTACK;

(II) PUBLIC NOTIFICATION REGARDING A RANSOMWARE ATTACK;

(III) IDENTITY THEFT PROTECTION FOR PERSONS AFFECTED

BY A RANSOMWARE ATTACK; AND

(IV) OTHER RELATED EXPENSES INVOLVING A RANSOMWARE ATTACK.

§ 7679. Civil actions.

A person or Commonwealth agency that is a victim of an offense under this subchapter may bring an action against a person violating this subchapter to recover any one or more of the following:

(1) Actual damages.

(2) Punitive damages.

(3) Reasonable attorney fees and other litigation costs reasonably incurred.

§ 7680. Remedies not exclusive.

The commencement of a criminal prosecution or civil action under this subchapter shall not prohibit or limit the commencement of a criminal prosecution or civil action under any other law.

§ 7681. Office of Administration.

(a) Study.--The Office of Administration shall study the susceptibility, preparedness and ability to respond on the part of Commonwealth agencies to ransomware attacks. In conducting the study, the Office of Administration shall:

(1) Develop guidelines and best practices to prevent a ransomware attack.

(2) Evaluate current data encryption and backup strategies.

(3) Evaluate the availability of tools to monitor unusual access requests, computer viruses and computer network traffic.

(4) Develop guidelines for Commonwealth agencies on

responding to a ransomware attack.

(5) Develop a coordinated law enforcement response strategy that uses forensic investigative techniques to identify the source of a ransomware attack.

(6) Provide recommendations on legislative or regulatory action to protect Commonwealth agencies from a ransomware attack.

(b) Reports.--No later than July 1, ~~2021~~ 2023, and each July <-- 1 thereafter, the Office of Administration shall prepare and transmit to the General Assembly a report, which must include the following:

(1) The information specified under subsection (a), including any updates on policies and procedures regarding ransomware.

(2) The number of ransomware attacks against Commonwealth agencies during the period covered by the report, including:

(i) The nature and extent of the ransomware and extortion attempts involving ransomware.

(ii) The effect of the ransomware attacks.

(3) Any other information that the Office of Administration deems necessary or proper.

(c) Cooperation.--A Commonwealth agency shall cooperate with the Office of Administration in providing information necessary for the preparation of a report under this section.

Section 2. This act shall take effect in 60 days.