
THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 726 Session of
2021

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

REFERRED TO JUDICIARY, MAY 28, 2021

AN ACT

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

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

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

9 SUBCHAPTER F

10 RANSOMWARE

11 Sec.

12 7671. Purposes of subchapter.

13 7672. Definitions.

14 7673. Prohibited actions.

15 7674. Grading of offense.

16 7675. Forfeiture.

17 7676. Limitation of time.

18 7677. Notification.

19 7678. Payments.

1 7679. Civil actions.

2 7680. Remedies not exclusive.

3 7681. Office of Administration.

4 § 7671. Purposes of subchapter.

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

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

10 (2) Prevent and detect ransomware attacks.

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

13 (4) Provide timely public notification of ransomware
14 attacks.

15 (5) Pursue and prosecute perpetrators of ransomware
16 attacks.

17 § 7672. Definitions.

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

21 "Commonwealth agency." Any of the following:

22 (1) The Governor's Office.

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

26 (3) The office of Lieutenant Governor.

27 (4) An independent department.

28 (5) An independent agency.

29 (6) A municipality.

30 (7) A school district.

1 (8) An intermediate unit.

2 (9) An area career and technical school.

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

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

8 (12) A State-owned institution.

9 (13) A State-related institution.

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

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

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

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

20 "Independent department." Any of the following:

21 (1) The Department of the Auditor General.

22 (2) The Treasury Department.

23 (3) The Office of Attorney General.

24 (4) A board or commission of an entity under paragraph
25 (1), (2) or (3).

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

28 "Public School Code of 1949." Act of March 10, 1949 (P.L.30,
29 No.14), known as the Public School Code of 1949.

30 "Ransomware." As follows:

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

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

11 (A) remove the computer contaminant or lock;

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

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

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

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

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

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

1 University and their branch campuses.

2 § 7673. Prohibited actions.

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

10 (1) Knowingly possess ransomware.

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

13 (3) Sell, transfer or develop ransomware.

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

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

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

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

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

25 § 7674. Grading of offense.

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

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

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

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

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

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

20 (1) is a second or subsequent offense;

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

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

26 § 7675. Forfeiture.

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

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

5 (b) Procedures.--The forfeiture under this section shall be
6 conducted in accordance with 42 Pa.C.S. §§ 5803 (relating to
7 asset forfeiture), 5805 (relating to forfeiture procedure), 5806
8 (relating to motion for return of property), 5807 (relating to
9 restrictions on use), 5807.1 (relating to prohibition on
10 adoptive seizures) and 5808 (relating to exceptions).
11 § 7676. Limitation of time.

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

15 § 7677. Notification.

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

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

25 (1) As necessary and appropriate, notify the Office of
26 Administration and an entity with jurisdiction or supervision
27 over the Commonwealth agency of the ransomware or extortion
28 attempt, in which case the Office of Administration or entity
29 shall, within two hours of the notification by the
30 Commonwealth agency, notify an appropriate official of the

1 Federal Bureau of Investigation of the ransomware or
2 extortion attempt.

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

7 § 7678. Payments.

8 (a) General rule.--Except as provided in subsection (b),
9 notwithstanding any other provision of law, after December 31,
10 2021, State and local taxpayer money or other public money may
11 not be used to pay an extortion attempt involving ransomware.

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

19 § 7679. Civil actions.

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

24 (1) Actual damages.

25 (2) Punitive damages.

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

28 § 7680. Remedies not exclusive.

29 The commencement of a criminal prosecution or civil action
30 under this subchapter shall not prohibit or limit the

1 commencement of a criminal prosecution or civil action under any
2 other law.

3 § 7681. Office of Administration.

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

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

10 (2) Evaluate current data encryption and backup
11 strategies.

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

15 (4) Develop guidelines for Commonwealth agencies on
16 responding to a ransomware attack.

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

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

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

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

30 (2) The number of ransomware attacks against

1 Commonwealth agencies during the period covered by the
2 report, including:

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

5 (ii) The effect of the ransomware attacks.

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

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

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