

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 563 Session of
2023

INTRODUCED BY PHILLIPS-HILL, STEFANO, LAUGHLIN AND VOGEL,
MARCH 28, 2023

REFERRED TO JUDICIARY, MARCH 28, 2023

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." The act of March 10, 1949
29 (P.L.30, 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 the branch campuses of each.

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, email, 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.--Any computer, computer system, computer
28 network, software or data that is used during the commission of
29 an offense under this subchapter or used as a repository for the
30 storage of software or data illegally obtained in violation of

1 this subchapter shall be subject to forfeiture.

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

8 § 7676. Limitation of time.

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

12 § 7677. Notification.

13 (a) Managed service providers.--A managed service provider
14 of information technology in the service of a Commonwealth
15 agency shall notify an appropriate official of the Commonwealth
16 agency of the discovery of ransomware or receipt of a ransomware
17 demand within one hour of the discovery of ransomware or receipt
18 of the ransomware demand.

19 (b) Commonwealth agencies.--

20 (1) Within two hours of a Commonwealth agency's
21 discovery of ransomware or receipt of a ransomware demand,
22 the Commonwealth agency shall, as necessary and appropriate,
23 notify the Office of Administration and an entity with
24 jurisdiction or supervision over the Commonwealth agency of
25 the discovery of ransomware or receipt of a ransomware
26 demand.

27 (2) If a Commonwealth agency or managed service provider
28 is in receipt of a ransomware demand, the Office of
29 Administration shall, within 24 hours of the notification by
30 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,
2023, 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;

1 (iii) identity theft protection for persons affected
2 by a ransomware attack; and
3 (iv) other related expenses involving a ransomware
4 attack.

5 § 7679. Civil actions.

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

10 (1) Actual damages.

11 (2) Punitive damages.

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

14 § 7680. Remedies not exclusive.

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

19 § 7681. Office of Administration.

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

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

26 (2) Evaluate current data encryption and backup
27 strategies.

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

1 (4) Develop guidelines for Commonwealth agencies on
2 responding to a ransomware attack.

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

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

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

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

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

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

21 (ii) The effect of the ransomware attacks.

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

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

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