

WEST VIRGINIA LEGISLATURE

2020 REGULAR SESSION

Enrolled

Committee Substitute

for

Senate Bill 261

SENATORS IHLENFELD, BALDWIN, STOLLINGS, AND

MAYNARD, *original sponsors*

[Passed March 7, 2020; in effect 90 days from
passage]

1 AN ACT to amend and reenact §61-3C-3 and §61-3C-4 of the Code of West Virginia, 1931, as
2 amended, all relating to contaminating a computer with ransomware; creating criminal
3 offense of introducing ransomware into any computer, computer system, or computer
4 network with the intent to extort money or other consideration; setting forth the elements
5 of the offense; defining terms; and establishing criminal penalties.

Be it enacted by the Legislature of West Virginia:

ARTICLE 3C. WEST VIRGINIA COMPUTER CRIME AND ABUSE ACT.

§61-3C-3. Definitions.

1 As used in this article, unless the context clearly indicates otherwise:

2 (1) "Access" means to instruct, communicate with, store data in, retrieve data from,
3 intercept data from, or otherwise make use of any computer, computer network, computer
4 program, computer software, computer data, or other computer resources.

5 (2) "Authorization" means the express or implied consent given by a person to another to
6 access or use said person's computer, computer network, computer program, computer software,
7 computer system, password, identifying code, or personal identification number.

8 (3) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-
9 speed data processing device performing logical, arithmetic, or storage functions and includes
10 any data storage facility or communication facility directly related to, or operating in conjunction
11 with, such device. The term "computer" includes any connected or directly related device,
12 equipment, or facility which enables the computer to store, retrieve, or communicate computer
13 programs, computer data, or the results of computer operations to or from a person, another
14 computer, or another device, file servers, mainframe systems, desktop personal computers,
15 laptop personal computers, tablet personal computers, cellular telephones, game consoles, and
16 any other electronic data storage device or equipment, but such term does not include an
17 automated typewriter or typesetter, a portable hand-held calculator, or other similar device.

18 (4) “Computer contaminant” means any set of computer instructions that are designed to
19 damage or destroy information within a computer, computer system, or computer network without
20 the consent or permission of the owner of the information. They include, but are not limited to, a
21 group of computer instructions commonly called viruses or worms that are self-replicating or self-
22 propagating and are designed to contaminate other computer programs or computer data,
23 consume computer resources, or damage or destroy the normal operation of the computer.

24 (5) “Computer data” means any representation of knowledge, facts, concepts, instruction,
25 or other information computed, classified, processed, transmitted, received, retrieved, originated,
26 stored, manifested, measured, detected, recorded, reproduced, handled, or utilized by a
27 computer, computer network, computer program, or computer software, and may be in any
28 medium, including, but not limited to, computer printouts, microfilm, microfiche, magnetic storage
29 media, optical storage media, punch paper tape, or punch cards, or it may be stored internally in
30 read-only memory or random access memory of a computer or any other peripheral device.

31 (6) “Computer network” means a set of connected devices and communication facilities,
32 including more than one computer, with the capability to transmit computer data among them
33 through such communication facilities.

34 (7) “Computer operations” means arithmetic, logical, storage, display, monitoring, or
35 retrieval functions or any combination thereof and includes, but is not limited to, communication
36 with, storage of data in or to, or retrieval of data from any device, and the human manual
37 manipulation of electronic magnetic impulses. A “computer operation” for a particular computer
38 shall also mean any function for which that computer was designed.

39 (8) “Computer program” means an ordered set of computer data representing instructions
40 or statements, in a form readable by a computer, which controls, directs, or otherwise influences
41 the functioning of a computer or computer network.

42 (9) "Computer software" means a set of computer programs, procedures, and associated
43 documentation concerned with computer data or with the operation of a computer, computer
44 program, or computer network.

45 (10) "Computer services" means computer access time, computer data processing, or
46 computer data storage, and the computer data processed or stored in connection therewith.

47 (11) "Computer supplies" means punch cards, paper tape, magnetic tape, magnetic disks
48 or diskettes, optical disks or diskettes, disk or diskette packs, paper, microfilm, and any other
49 tangible input, output, or storage medium used in connection with a computer, computer network,
50 computer data, computer software, or computer program.

51 (12) "Computer resources" includes, but is not limited to, information retrieval; computer
52 data processing, transmission, and storage; and any other functions performed, in whole or in
53 part, by the use of a computer, computer network, computer software, or computer program.

54 (13) "Financial instrument" includes, but is not limited to, a check, draft, warrant, money
55 order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction
56 authorization mechanism, marketable security, or any computerized representation thereof.

57 (14) "Owner" means any person who owns or leases or is a licensee of a computer,
58 computer network, computer data, computer program, computer software, computer resources,
59 or computer supplies.

60 (15) "Person" means any natural person, general partnership, limited partnership, trust,
61 association, corporation, joint venture, or any state, county, or municipal government and any
62 subdivision, branch, department, or agency thereof.

63 (16) "Property" includes:

64 (A) Real property;

65 (B) Computers and computer networks;

66 (C) Financial instruments, computer data, computer programs, computer software, and all
67 other personal property regardless of whether they are:

68 (i) Tangible or intangible;
69 (ii) In a format readable by humans or by a computer;
70 (iii) In transit between computers or within a computer network or between any devices
71 which comprise a computer; or

72 (iv) Located on any paper or in any device on which it is stored by a computer or by a
73 human; and

74 (D) Computer services.

75 (17) "Ransomware" means a computer contaminant, or lock placed or introduced without
76 authorization into a computer, computer system, or computer network that restricts access by an
77 authorized user to the computer, computer system, computer network, or any data therein under
78 circumstances in which the person responsible for the placement or introduction of the
79 ransomware demands payment of money or other consideration to remove the computer
80 contaminant, restore access to the computer, computer system, computer network, or data, or
81 otherwise remediate the impact of the computer contaminant or lock.

82 (18) "Value" means having any potential to provide any direct or indirect gain or advantage
83 to any person.

84 (19) "Value of property or computer services" shall be: (A) The market value of the
85 property or computer services at the time of a violation of this article; or (B) if the property or
86 computer services are unrecoverable, damaged, or destroyed as a result of a violation of §61-3C-
87 6 or §61-3C-7 of this code, the cost of reproducing or replacing the property or computer services
88 at the time of the violation.

§61-3C-4. Computer fraud; access to Legislature computer; criminal penalties.

1 (a) Any person who, knowingly and willfully, directly or indirectly, accesses or causes to
2 be accessed any computer, computer services, or computer network for the purpose of: (1)
3 Executing any scheme or artifice to defraud; or (2) obtaining money, property, or services by
4 means of fraudulent pretenses, representations, or promises is guilty of a felony and, upon

5 conviction thereof, shall be fined not more than \$10,000 or imprisoned in a state correctional
6 facility for a determinate sentence of not more than 10 years, or both fined and imprisoned.

7 (b) Any person who, with intent to extort money or other consideration from another,
8 introduces ransomware into any computer, computer system, or computer network is guilty of a
9 felony and, upon conviction thereof, shall be fined not more than \$100,000 or imprisoned in a
10 state correctional facility for a determinate sentence of not more than 10 years, or both fined and
11 imprisoned.

12 (c) A person is criminally responsible for placing or introducing ransomware into a
13 computer, computer system, or computer network if the person directly places or introduces the
14 ransomware or directs or induces another person to do so, with the intent of demanding payment
15 or other consideration for removing, restoring access, or other remediation of the impact of the
16 ransomware.

17 (d) (1) Any person who, knowingly and willfully, directly or indirectly, accesses, attempts
18 to access, or causes to be accessed any data stored in a computer owned by the Legislature
19 without authorization is guilty of a felony and, upon conviction thereof, shall be fined not more
20 than \$5,000 or imprisoned in a state correctional facility for a determinate sentence of not more
21 than five years, or both fined and imprisoned.

22 (2) Notwithstanding the provisions of §61-3C-17 of this code to the contrary, in any criminal
23 prosecution under this subsection against an employee or member of the Legislature, it shall not
24 be a defense: (A) That the defendant had reasonable grounds to believe that he or she had
25 authorization to access the data merely because of his or her employment or membership; or (B)
26 that the defendant could not have reasonably known he or she did not have authorization to
27 access the data: *Provided*, That the Joint Committee on Government and Finance shall
28 promulgate rules for the respective houses of the Legislature regarding appropriate access of
29 members and staff and others to the legislative computer system.

The Joint Committee on Enrolled Bills hereby certifies that the foregoing bill is correctly enrolled.

.....
Chairman, Senate Committee

.....
Chairman, House Committee

Originated in the Senate.

In effect 90 days from passage.

.....
Clerk of the Senate

.....
Clerk of the House of Delegates

.....
President of the Senate

.....
Speaker of the House of Delegates

The within this the.....
Day of, 2020.

.....
Governor