HOUSE BILL 635

E1 0lr3010

By: **Delegate Cox**
Introduced and read first time: January 29, 2020
Assigned to: Judiciary

A BILL ENTITLED

AN ACT concerning

Criminal Law – Crimes Involving Computers – Malware and Ransomware

FOR the purpose of prohibiting a person from knowingly possessing certain malware or ransomware with the intent to use that malware or ransomware for a certain purpose; creating a certain exception; establishing a certain penalty; providing for the application of this Act; defining a certain term; and generally relating to crimes involving computers.

BY repealing and reenacting, with amendments,
Article – Criminal Law
Section 7–302
Annotated Code of Maryland
(2012 Replacement Volume and 2019 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Criminal Law

7–302.

(a) (1) In this section the following words have the meanings indicated.

(2) "Access" means to instruct, communicate with, store data in, retrieve or intercept data from, or otherwise use the resources of a computer program, computer system, or computer network.

(3) (i) "Aggregate amount" means a direct loss of property or services incurred by a victim.

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

(ii) "Aggregate amount" includes:

1. the value of any money, property, or service lost, stolen, or rendered unrecoverable by the crime; or

2. any actual reasonable expenditure incurred by the victim to verify whether a computer program, computer, computer system, or computer network was altered, acquired, damaged, deleted, disrupted, or destroyed by access in violation of this section.

(4) (i) "Computer" means an electronic, magnetic, optical, organic, or other data processing device or system that performs logical, arithmetic, memory, or storage functions.

(ii) "Computer" includes property, a data storage facility, or a communications facility that is directly related to or operated with a computer.

(iii) "Computer" does not include an automated typewriter, a typesetter, or a portable calculator.

(5) "Computer control language" means ordered statements that direct a computer to perform specific functions.

(6) "Computer database" means a representation of information, knowledge, facts, concepts, or instructions that:

(i) is intended for use in a computer, computer system, or computer network; and

(ii) 1. is being prepared or has been prepared in a formalized manner; or

2. is being produced or has been produced by a computer, computer system, or computer network.

(7) "Computer network" means the interconnection of one or more computers through:

(i) the use of a satellite, microwave, line, or other communication medium; and

(ii) terminals or a complex consisting of two or more interconnected computers regardless of whether the interconnection is continuously maintained.

(8) "Computer program" means an ordered set of instructions or statements that may interact with related data and, when executed in a computer system, causes a computer to perform specified functions.

(9) "Computer services" includes computer time, data processing, and storage functions.

(10) "Computer software" means a computer program, instruction, procedure, or associated document regarding the operation of a computer system.

(11) "Computer system" means one or more connected or unconnected computers, peripheral devices, computer software, data, or computer programs.

(12) (I) "MALWARE" MEANS A COMPUTER OR DATA CONTAMINANT THAT IS DESIGNED TO:

1. DISRUPT OR DENY OPERATION OF AN AUTHORIZED PERSON TO A COMPUTER, COMPUTER DATA, A COMPUTER NETWORK, OR A COMPUTER SYSTEM;

2. GATHER INFORMATION THAT LEADS TO LOSS OF PRIVACY OR EXPLOITATION; OR

3. GAIN UNAUTHORIZED ACCESS TO SYSTEM RESOURCES.

(II) "MALWARE" INCLUDES SPYWARE.

(13) "RANSOMWARE" MEANS A COMPUTER OR DATA CONTAMINANT, ENCRYPTION, OR LOCK THAT:

(I) IS PLACED OR INTRODUCED WITHOUT AUTHORIZATION INTO A COMPUTER, A COMPUTER NETWORK, OR A COMPUTER SYSTEM; AND

(II) RESTRICTS ACCESS BY AN AUTHORIZED PERSON TO A COMPUTER, COMPUTER DATA, A COMPUTER NETWORK, OR A COMPUTER SYSTEM IN A MANNER THAT RESULTS IN THE PERSON RESPONSIBLE FOR THE PLACEMENT OR INTRODUCTION OF THE CONTAMINANT, ENCRYPTION, OR LOCK DEMANDING PAYMENT OF MONEY OR OTHER CONSIDERATION TO REMOVE THE CONTAMINANT, ENCRYPTION, OR LOCK.

(b) This section does not preclude the applicability of any other provision of this Code.

(c) (1) A person may not intentionally, willfully, and without authorization:

(i) access, attempt to access, cause to be accessed, or exceed the person's authorized access to all or part of a computer network, computer control language,

computer, computer software, computer system, computer service, or computer database; or

(ii) copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database accessed in violation of item (i) of this paragraph.

(2) A person may not commit an act prohibited by paragraph (1) of this subsection with the intent to:

(i) cause the malfunction or interrupt the operation of all or any part of a computer, computer network, computer control language, computer software, computer system, computer service, or computer data; or

(ii) alter, damage, or destroy all or any part of data or a computer program stored, maintained, or produced by a computer, computer network, computer software, computer system, computer service, or computer database.

(3) A person may not intentionally, willfully, and without authorization:

(i) possess, identify, or attempt to identify a valid access code; or

(ii) publicize or distribute a valid access code to an unauthorized person.

(4) A person may not commit an act prohibited under this subsection with the intent to interrupt or impair the functioning of:

(i) the State government;

(ii) a service, device, or system related to the production, transmission, delivery, or storage of electricity or natural gas in the State that is owned, operated, or controlled by a person other than a public service company, as defined in § 1–101 of the Public Utilities Article; or

(iii) a service provided in the State by a public service company, as defined in § 1–101 of the Public Utilities Article.

(5) (I) THIS PARAGRAPH DOES NOT APPLY TO THE USE OF MALWARE OR RANSOMWARE FOR RESEARCH PURPOSES.

(II) A PERSON MAY NOT KNOWINGLY POSSESS MALWARE OR RANSOMWARE WITH THE INTENT TO USE THE MALWARE OR RANSOMWARE FOR THE PURPOSE OF INTRODUCTION INTO THE COMPUTER, COMPUTER NETWORK, OR COMPUTER SYSTEM OF ANOTHER PERSON WITHOUT THE AUTHORIZATION OF THE OTHER PERSON.

(d) (1) A person who violates subsection (c)(1) of this section is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 3 years or a fine not exceeding $1,000 or both.

(2) A person who violates subsection (c)(2) or (3) of this section:

(i) if the aggregate amount of the loss is $10,000 or more, is guilty of a felony and on conviction is subject to imprisonment not exceeding 10 years or a fine not exceeding $10,000 or both; or

(ii) if the aggregate amount of the loss is less than $10,000, is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 5 years or a fine not exceeding $5,000 or both.

(3) A person who violates subsection (c)(4) of this section:

(i) if the aggregate amount of the loss is $50,000 or more, is guilty of a felony and on conviction is subject to imprisonment not exceeding 10 years or a fine not exceeding $25,000 or both; or

(ii) if the aggregate amount of the loss is less than $50,000, is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 5 years or a fine not exceeding $25,000 or both.

(4) A PERSON WHO VIOLATES SUBSECTION (C)(5) OF THIS SECTION IS GUILTY OF A MISDEMEANOR AND ON CONVICTION IS SUBJECT TO IMPRISONMENT NOT EXCEEDING 10 YEARS OR A FINE NOT EXCEEDING $10,000 OR BOTH.

(e) Access achieved in violation of this section under a single scheme or a continuing course of conduct may be considered as one violation.

(f) A court of competent jurisdiction may try a person prosecuted under this section in any county in this State where:

(1) the defendant performed the act; or

(2) the accessed computer is located.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall be construed to apply only prospectively and may not be applied or interpreted to have any effect on or application to any cause of action arising before the effective date of this Act.

SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2020.