Department of Legislative Services

Maryland General Assembly
2019 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 211 (Delegates Barron and W. Fisher)
Judiciary

Criminal Law - Crimes Involving Computers - Ransomware

This bill (1) expands the prohibitions under § 7-302 (c)(4) of the Criminal Law Article; (2) alters the criminal penalties applicable to violations of § 7-302(c)(4); and (3) prohibits a person from knowingly possessing "ransomware" with the intent to use it for specified purposes. The bill also authorizes a person who has suffered a specific and direct injury because of a violation of § 7-302 to bring a civil action in a court of competent jurisdiction, establishes that a conviction for the applicable offense is not a prerequisite for maintenance of the civil action, and authorizes a court in such an action to award actual damages and reasonable attorney's fees and court costs. The bill applies prospectively to any cause of action arising on or after the bill's October 1, 2019 effective date.

Fiscal Summary

State Effect: Minimal decrease in general fund revenues from fines imposed in District Court cases. Minimal increase in general fund expenditures due to the bill's incarceration penalty provisions.

Local Effect: Minimal increase in revenues and expenditures due to the bill's penalty provisions.

Small Business Effect: Meaningful impact on small businesses that are awarded damages in civil actions brought under the bill.

Analysis

Bill Summary: The bill expands § 7-302(c)(4) of the Criminal Law Article to apply the prohibition against engaging in certain computer and technology-related acts with the

intent to interrupt or impair the functioning of specified services and entities to a health care facility, as defined in § 18-338.1 of the Health-General Article. It also makes the penalty applicable to all acts committed in violation of § 7-302(c)(4) more stringent. If the aggregate amount of the loss is $1,000 or more, a violator is guilty of a felony and subject to maximum penalties of 10 years imprisonment and/or a $100,000 fine. If the aggregate loss is valued at less than $1,000, a violator is guilty of a misdemeanor and is subject to maximum penalties of five years imprisonment and/or a $25,000 fine.

The bill establishes a new criminal offense related to the use of ransomware. With the exception of the use of ransomware for research purposes, the bill prohibits a person from knowingly possessing ransomware with the intent to use the ransomware for the purpose of introduction into the computer, computer network, or computer system of another person without the authorization of the other person. Violators are guilty of a misdemeanor, punishable by imprisonment for up to 10 years and/or a $10,000 maximum fine.

"Ransomware" means a computer or data contaminant, encryption, or lock that (1) is placed or introduced without authorization into a computer, a computer network, or a computer system and (2) 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.

Current Law: Under § 7-302 of the Criminal Law Article, a person may not intentionally, willfully, and without authorization, access or attempt to access, cause to be accessed, or exceed the person's authorized access to all or part of a computer or a computer network, language, software, system, service, or database. Also, a person may not intentionally, willfully, and without authorization, copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database that was unlawfully accessed. A violation of these provisions is a misdemeanor, and the violator is subject to maximum penalties of imprisonment for three years and/or a fine of $1,000.

A person may not intentionally, willfully, and without authorization, commit unlawful access or attempted access, as specified, with the intent to (1) cause the malfunction or interruption of any or all parts of a computer, network, language, software, service, or data; (2) alter, damage, or destroy all or any part of data or a program stored, maintained, or produced by a computer, network, software, system, service, or database; or (3) possess, identify, or attempt to identify a valid access code or publicize or distribute a valid access code to an unauthorized person.

If the aggregate amount of the loss is $10,000 or more, the violator is guilty of a felony and is subject to maximum penalties of imprisonment for 10 years and/or a fine of $10,000. If

the aggregate loss is less than $10,000, the violator is guilty of a misdemeanor and is subject to maximum penalties of imprisonment for 5 years and/or a fine of $5,000.

Under § 7-302(c)(4) of the Criminal Law Article, a person may not gain or attempt to gain unauthorized access to computer services with the intent to interrupt or impair the functioning of (1) State government; (2) a service provided in the State by a public service company; or (3) a natural gas or electric service, device, or system provided in the State by a person other than a public service company.

If the aggregate amount of the loss associated with this prohibition is $50,000 or more, a violator is guilty of a felony and subject to maximum penalties of 10 years imprisonment and/or a $25,000 fine. If the aggregate loss is less than $50,000, a violator is guilty of a misdemeanor and is subject to maximum penalties of 5 years imprisonment and/or a $25,000 fine.

Access achieved in a prohibited manner under a single scheme or a continuing course of conduct may be considered one violation. A defendant may be tried in any county in Maryland where the act was performed or the accessed computer was located.

Background: Ransomware attacks are an increasingly popular crime in which individuals, who are often hackers based overseas, use software viruses to assume control of or encrypt computers, data stored in computers, or computer networks and refuse to release control of the computers or data unless a ransom is paid, often through the Internet currency Bitcoin. Unpaid ransoms can result in escalating demands or permanent loss of data. Victims of ransomware attacks include ordinary citizens, small businesses, public libraries, hospitals, local governments, and larger businesses/entities. Because the perpetrators are often based overseas, there is very little local and federal law enforcement can do, especially within the narrow window of time in which victims must pay a ransom.

In March 2016, computers at MedStar Health, a prominent health care system in the Maryland/Washington, DC area, were attacked by a virus that blocked some users from logging into its system. MedStar employees reported seeing pop-up screens on their computers demanding payment in Bitcoin. MedStar responded to the attack by shutting down extensive portions of its computer network. In November 2018, two Iranian hackers were charged in federal court in connection with the attack against MedStar and attacks against several other entities, including the cities of Atlanta, Georgia, and Newark, New Jersey; the Colorado Department of Transportation; the Port of San Diego; and other health care companies. The two hackers, who are believed to be in Iran, are alleged to have accessed computer networks remotely, installed ransomware on the networks, and demanded payment from their victims in return for unlocking data. According to prosecutors, their efforts netted $6 million and caused their victims to lose at least $30 million.

The Federal Bureau of Investigation (FBI) estimates that ransomware payments in 2016 totaled $1 billion, a significant increase from the $24 million in estimated payments during 2015. In an attempt to understand the scope of ransomware attacks and develop solutions and approaches to attacks, the FBI issued an alert in September 2016 asking victims to file reports through its Internet Crime Complaint Center. The lucrative nature of the attacks has created a growth industry within criminal networks, with reports of ransomware applications and toolkits being available for purchase and "ransomware as a service," through which individuals can purchase time on a criminal network designed to launch attacks in return for paying the network provider a percentage of the extorted funds.

On January 9, 2019, the Salisbury Police Department was the victim of a ransomware attack. According to news reports, as of January 24, 2019, some data remains inaccessible. However, a backup system prevented the loss of data. The police department is working with the FBI.

State Revenues: General fund revenues decrease minimally from fines imposed in applicable cases due to the shifting of cases from the District Court to the circuit courts as a result of the bill's alteration of existing criminal penalties.

State Expenditures: General fund expenditures for the Department of Public Safety and Correctional Services increase minimally as a result of the bill's incarceration penalties due to more people being committed to State correctional facilities, lengthier incarcerations, and increased payments to counties for reimbursement of inmate costs. The bill creates a new criminal offense, expands an existing criminal offense, and alters existing criminal penalties. The number of people subject to the bill's penalty provisions is expected to be minimal.

Persons serving a sentence longer than 18 months are incarcerated in State correctional facilities. Currently, the average total cost per inmate, including overhead, is estimated at $3,800 per month. Persons serving a sentence of one year or less in a jurisdiction other than Baltimore City are sentenced to local detention facilities. For persons sentenced to a term of between 12 and 18 months, the sentencing judge has the discretion to order that the sentence be served at a local facility or a State correctional facility. The State provides assistance to the counties for locally sentenced inmates and for (1) inmates who are sentenced to and awaiting transfer to the State correctional system; (2) sentenced inmates confined in a local detention center between 12 and 18 months; and (3) inmates who have been sentenced to the custody of the State but are confined in or who receive reentry or other prerelease programming and services from a local facility.

The State does not pay for pretrial detention time in a local correctional facility. Persons sentenced in Baltimore City are generally incarcerated in State correctional facilities. The

Baltimore Pretrial Complex, a State-operated facility, is used primarily for pretrial detentions.

The bill's alteration of existing criminal penalties makes behavior currently classified as a misdemeanor a felony. Changing crimes from misdemeanors to felonies means that (1) such cases are likely to be filed in the circuit courts rather than the District Court and (2) some persons may eventually serve longer incarcerations due to more stringent penalty provisions, applicable to some offenses for prior felony convictions. Accordingly, it is assumed that this bill shifts an unknown number of cases from the District Court to the circuit courts. It is not known whether such a prospective shift may spur more plea bargains and affect actual sentencing practices for this offense.

Local Revenues: Revenues increase minimally as a result of the bill's monetary penalty provisions from cases heard in the circuit courts.

Local Expenditures: Expenditures increase minimally as a result of the bill's incarceration penalties. Counties pay the full cost of incarceration for people in their facilities for the first 12 months of the sentence. Per diem operating costs of local detention facilities have ranged from approximately $40 to $170 per inmate in recent years.

Additional Information

Prior Introductions: None.

Cross File: SB 151 (Senator Lee, *et al.*) - Judicial Proceedings.

Information Source(s): Judiciary (Administrative Office of the Courts); Office of the Public Defender; Federal Bureau of Investigation; *The Baltimore Sun*; *The Washington Post*; Department of Legislative Services

Fiscal Note History: First Reader - January 30, 2019
md/kdm

Analysis by: Amy A. Devadas

Direct Inquiries to:
(410) 946-5510
(301) 970-5510