House
Legislative
Analysis
Section

House Office Building, 9 South
Lansing, Michigan 48909
Phone: 517/373-6466

COMPUTER CRIMES

House Bill 5184 as enrolled
Public Act 178 of 2000
Sponsor: Rep. Gene DeRossett

House Bill 5185 as enrolled
Public Act 179 of 2000
Sponsor: Rep. William O'Neil

House Bill 5186 as enrolled
Public Act 180 of 2000
Sponsor: Rep. Jim Howell

House Bill 5187 as enrolled
Public Act 181 of 2000
Sponsor: Rep. Ruth Jamnick

Senate Bill 893 as enrolled
Public Act 184 of 2000
Sponsor: Sen. Mike Rogers

Senate Bill 894 as enrolled
Public Act 185 of 2000
Sponsor: Sen. Mike Rogers

Third Analysis (7-12-00)
House Committee: Criminal Law and Corrections
Senate Committee: Judiciary

THE APPARENT PROBLEM:

In 1979, Michigan enacted its first computer fraud statute (Public Act 53) to prohibit persons from gaining access to a computer or computer system or network for fraudulent purposes, and to bar use of a computer to commit various crimes. The act was similar to laws adopted in most other states and provided criminal penalties for various violations (embezzlement, fraudulent disposition of personal property, larceny) that involve use of a computer or computer system. In 1996, Public Act 53 was amended to expand the types of prohibited activities that relate to accessing or using computers or computer systems and to increase the penalties for such crimes.

Under current law, the computer crime act prohibits individuals from accessing a computer, computer program, system or network with the intent to defraud. It also prohibits unauthorized access to or insertion of instructions or a program into a computer, computer program, system or network. The penalties for such a crime are dependent upon the financial loss resulting from the crime.

It is also illegal to use a computer, computer program, system, or network to commit another underlying crime; however, under current law this is only punishable as a misdemeanor with up to one year imprisonment unless there is sufficient financial loss to upgrade the violation.

Since the enactment and subsequent amendment of Public Act 53 of 1979, the use of computers and telecommunications by businesses and individuals has exploded nationwide, and many new types of high-technology equipment have been developed and are being used for collecting, storing, disseminating, and transferring information. As technological advances have occurred, laws governing illegal activities involving computers have not kept pace, and some people estimate billions of dollars are stolen or destroyed nationwide each year because law enforcement officials lack statutory authority to proceed in cases where substantial evidence exists to prove criminal activity. Some people believe Michigan laws governing computer crimes need to be updated both to expand the types of activities that constitute high-technology crimes and to establish more severe penalties--particularly fines--that apply to persons found engaging in them.

THE CONTENT OF THE BILLS:

House Bills 5185-5187 would amend Public Act 53 of 1979 (MCL 752.792 et al.), which prohibits access to computers, computer systems and networks fort certain fraudulent purposes, to add language to include attempts to commit crimes using computers, and to clarify and expand the existing penalties for crimes committed under the act. House Bill 5184 would amend the Code of Criminal Procedure (MCL 760.1 - 777.69) place these penalties in the statutory sentencing guidelines. Senate Bill 893 would amend Chapter 47 of the RJA ("Forfeiture or Seizure of Certain Property") to include violations committed by use of the Internet, a computer, or a computer program, network, or system. Senate Bill 894 would amend the Michigan Penal Code to clarify and expand the existing penalties for crimes committed under the act. House Bill 5184 is tie-barred to the House Bills 5185-5187 and to Senate Bills 893 and 894, House Bills 5185-5187 are tie-barred to one another and to the two Senate bills, and the Senate bills are tie-barred to the House Bills 5185-5187. The bills would take effect 90 days after they were enacted.

Section 6 of Public Act 53 of 1979 prohibits the use of a computer or a computer program, system, or network to commit a crime. House Bill 5185 would expand the prohibitions in section 6 to also prohibit the use of a computer, etc. to attempt, conspire, or solicit another to commit a crime.

In addition, the bill specifies that Section 6 would not prohibit a person from being charged with, convicted of, or punished for any other violation committed by that person while violating or attempting, conspiring, or soliciting another person to violate this section, including the underlying offense. The bill also specifies that Section 6 would apply regardless of whether the person was convicted of committing or attempting, conspiring, or soliciting another person to commit the underlying offense.

House Bill 5187 would change the definition of "aggregate amount" (of the value of property lost or stolen), which currently includes only the losses incurred by a single victim. Under the bill, aggregate amount could include the losses of groups of victims. The bill further specifies that the direct or indirect losses incurred in separate incidents that were part of a scheme or course of conduct within any 12-month period could be aggregated to determine the total value of the loss involved in a violation of the act.

House Bill 5186 would specify that the act's existing penalty language, which sets up a tiered system of penalties depending upon the amount of money involved in the crime (described in more detail below), applies to situations where a computer is used to defraud or otherwise obtain money, property, or services by false pretenses. The bill would establish separate penalties for unlawfully accessing a computer, computer program, system or network and for using a computer to attempt, conspire, or solicit another to commit a crime.

Current Penalties. Currently, a violation of Public Act 53 is a misdemeanor punishable by up to 93 days' imprisonment and/or a maximum fine of $500 or three times the aggregate amount, whichever is greater, if the violation involves an aggregate amount of less than $200. If a violation involves an aggregate amount of $200 or more but less than $1,000, or the offender has a prior conviction, the offense is a misdemeanor punishable by up to one year's imprisonment and/or a maximum fine of $2,000 or three times the aggregate amount, whichever is greater.

If a violation of the act involves an aggregate amount of $1,000 or more but less than $20,000, or the offender has two prior convictions, the offense is a felony punishable by up to five years' imprisonment and/or a maximum fine of $10,000 or three times the aggregate amount, whichever is greater. If a violation involves an aggregate amount of $20,000 or more, or the offender has three or more prior convictions, the offense is a felony punishable by up to 10 years' imprisonment and/or a maximum fine of three times the aggregate amount.

Access in Order to Defraud or Steal. Under the bill, the penalties described above would apply only to a violation of Section 4 of the act, which prohibits a person from intentionally gaining access or causing access to be made to a computer or a computer program, system, or network "to devise or execute a scheme or artifice with the intent to defraud or to obtain money, property, or a service by a false or fraudulent pretense, representation, or promise".

Access in Order to Alter, Damage, or Delete. Section 5 of the act prohibits a person from doing either of the following intentionally and without authorization, or by exceeding valid authorization:

-- Gaining access or causing access to be made to a computer or computer program, system, or network to acquire, alter, damage, delete, or destroy property or otherwise use the service of the computer or computer program, system, or network.

-- Inserting or attaching or knowingly creating the opportunity for an unknowing and unwanted insertion or attachment of a set of instructions or a computer program into a computer or computer program, system, or network, that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of a computer or computer program, system, or network.

Under the bill, a violation of Section 5 would be a felony punishable by up to five years' imprisonment and/or a maximum fine of $10,000. If the offender had a prior conviction, the felony would be punishable by up to 10 years' imprisonment and/or a maximum fine of $50,000.

("Prior conviction" would be specifically defined to include a violation or attempted violation of the Michigan Penal Code's prohibition against using the Internet or a computer for the crimes described in Senate Bill 894; Public Act 53; or a substantially similar law of the United States, another state, or a political subdivision of another state.)

Computer Use to Commit Crime. The bill would also establish penalties for a violation of Section 6 (described in House Bill 5185, above) based upon the maximum term of imprisonment for the underlying crime.

If the underlying crime was a misdemeanor or a felony that was punishable by imprisonment for one year or less, the use of the computer would be an additional misdemeanor punishable by imprisonment for up to one year and/or a fine of up to $5,000. If the underlying crime was a misdemeanor or felony with a maximum term of imprisonment of more than one year but less than two years imprisonment, the use of a computer would be a felony punishable by imprisonment for up to two years and or a fine of up to $5,000, or both. If the underlying crime was a misdemeanor or felony with a maximum term of imprisonment of a least two years but less than four years, the use of a computer would be a felony punishable by imprisonment for up to four years and/or a fine of up to $5,000. If the underlying crime was a felony with a maximum term of imprisonment of four years or more but less than ten years, the use of a computer would be a felony punishable by imprisonment for up to seven years, a fine of up to $5,000, or both. If the underlying crime was a felony punishable by a maximum term of at least 10 years but less than 20 years imprisonment, the use of a computer would be a felony punishable by imprisonment for up to 10 years, a fine of up to $10,000, or both. If the underlying crime was a felony punishable by a maximum term of imprisonment for at least 20 years or for life, the use of a computer would be a felony punishable by imprisonment for up to 20 years, and/or a fine of up to $20,000.

In any case involving the use of a computer to commit, attempt, conspire, or solicit another to commit a crime, the court could order that a term of imprisonment imposed for a violation of Section 6 be served consecutively to any term of imprisonment that was imposed for the underlying offense.

Law Enforcement Reimbursement. The bill would authorize the sentencing court to order a person convicted of a Public Act 53 violation to reimburse the state or a local unit for expenses incurred in relation to the investigation and prosecution of the violation.

House Bill 5184 would amend the Code of Criminal Procedure (MCL 760.1 - 777.69) to place the new penalties in the statutory sentencing guidelines.

Unlawfully accessing a computer, computer system, or computer program would be a categorized as a property crime, with a first offense being a class E crime with a five-year statutory maximum, and subsequent offenses would be class D crimes with a ten-year statutory maximum.

Using a computer to commit a crime would be based on the tiered system listed above and the offense category, offense variable level, and prior record level for each

crime would be the same as for the underlying offense.

• Using a computer to commit a crime that was punishable by more than one year but less than two years imprisonment would be class G crime with a statutory maximum of two years.

• Using a computer to commit a crime punishable by more than two years but less than four years imprisonment would be a Class F crime with a statutory maximum of four years.

• Using a computer to commit a crime punishable by more than four years but less than ten years imprisonment would be a Class D crime with a statutory maximum of seven years.

• Using a computer to commit a crime that was punishable by more than 10 years but less than 20 years imprisonment would be a Class D crime with a statutory maximum of 10 years.

• Using a computer to commit a crime that was punishable by imprisonment for 20 years or more or for life would be a Class D crime with a statutory maximum of 20 years.

Senate Bill 893 would amend Chapter 47 of the RJA ("Forfeiture or Seizure of Certain Property") to include violations committed by use of the Internet, a computer, or a computer program, network, or system in the list of offenses for which seizure and forfeiture proceedings may apply to property used in or obtained through the commission of a crime. (The Penal Code offense that would be added to the definition of "crime" in Chapter 47 would be amended by Senate Bill 894, as described below.)

In addition, forfeiture currently is allowed for committing or conspiring to commit any of the offenses listed in Chapter 47 of the RJA. The bill also would allow forfeiture proceedings for attempting or soliciting another to commit any of the listed offenses.

Senate Bill 894 would amend the Michigan Penal Code to revise offenses and penalties for certain crimes involving use of the Internet or a computer, and provide for reimbursement to the state or a local unit for investigation and prosecution of those crimes.

The penal code prohibits use of the Internet, a computer, or a computer program, network, or system to communicate with any person for the purpose of committing, attempting to commit, conspiring to commit, or soliciting another to commit any of the following:

-- Involvement in child sexually abusive activity or material, kidnaping, first-, second-, third-, or fourth-degree criminal sexual conduct (CSC), or assault with intent to commit CSC, when the victim or intended victim is a minor.

-- Solicitation of a child for immoral purposes, recruitment or inducement of a minor to commit a felony, kidnaping of a child under the age of 14, or stalking or aggravated stalking.

-- An explosives offense listed in Chapter 33 of the code, causing a death by explosives, selling explosives to a minor, or intentionally reporting a crime relating to a bombing, attempted bombing, or threat to bomb, knowing that the report is false.

-- Various gambling or gaming offenses prohibited by the Penal Code or the Michigan Gaming Control and Revenue Act.

The bill would delete the gambling and gaming offenses from this provision and specify that the use of the Internet or a computer to commit any of the remaining crimes (except stalking, aggravated stalking, and the explosives offenses) would be a violation where the victim or intended victim was a minor or the person who committed the crime believed that the victim was a minor.

The bill would also restructure the penalties for these crimes. Under the bill, the penalty would vary based on the penalty for the underlying crime, see Table 1. (Table provided by the Senate Fiscal Agency)

Table 1

Underlying Crime	Offense Level	Maximum Imprison-ment	Maximum Fine
Less than 1 year	mis-demeanor	1 year	$5,000
1-2 years	felony	2 years	$5,000
2-4 years	felony	4 years	$5,000
4-10 years	felony	10 years	$5,000
10-15 years	felony	15 years	$10,000
15 years - life	felony	20 years	$20,000

In addition, under the bill, a person convicted of an Internet or computer offense described above could be ordered to reimburse the state or a local unit of government for expenses incurred in relation to the investigation and prosecution of the violation.

FISCAL IMPLICATIONS:

According to the House Fiscal Agency, to the extent that the bills increased the numbers of offenders receiving state or local criminal sanctions, or increased the length of those sanctions, the bills would increase state and/or local costs. To the extent that these changes increased collections of fines for violation of state penal laws, there would be a corresponding increase the amounts of these revenues going to local libraries. (2-16-00)

According to the Senate Fiscal Agency, the bills would have an indeterminate impact on state and local government. (3-17-00)

ARGUMENTS:

For:

Unfortunately, insofar as legitimate uses for computers are increasing on a daily basis, illegitimate uses are increasing just as quickly. Thus, the primary purpose of the bills is to revise the current law so that it will apply to a number of crimes that the existing law fails to deal with or for which it provides inadequate punishments. In particular, because current punishments are based upon the amount of financial loss that occurred, they limit the punishment in cases where no financial loss occurred. The ever-increasing scope and influence of the Internet and computers on daily life and commerce makes criminal acts that involve them potentially more devastating every day. By establishing more severe penalties it is hoped that certain offenders will be deterred from committing crimes. In particular, the bills target some younger people who might engage in interference types of crimes on a lark (juvenile "hackers" who might unlawfully access a computer, or a computer system or network simply to see if they can do it). Furthermore, by allowing prosecutors to aggregate not only the amount from crimes that took place over a series of months, but also amounts taken from groups of victims, the bills will assure that people who run large-scale scams that affect large numbers of people are severely punished.

Against:

The bills fail to address some of the problems with the current act that were concerns at the time amendments were added in 1996. For example, the act creates a rebuttable presumption, with certain exceptions, that someone was either not authorized or had exceeded authorization from the owner or operator of a computer system to gain access to that system. This means people could be "surfing the Net" (i.e., browsing for information on the Internet) and inadvertently find themselves inside a closed system due to some coincidental sequence of commands they made, and--before they were aware of this and could exit the system--find themselves facing a criminal charge that *presumed* they were doing something illegally. The onus would then be on the individual to rebut the presumption that he or she had acted illegally; this could be both difficult and costly for that individual. The act also prohibits someone from "knowingly creating the opportunity for an unknowing and unwanted insertion or attachment" of computer-related instructions. Arguably this could allow the prosecution of someone who wrote or produced a publication that specialized in providing computer users "inside information" about how computer systems operate, simply because it made it possible for someone else to use information intended to be used for good purposes for a criminal use. While these are not flaws in the bills themselves, they are flaws in that act that could and should be addressed as part of this cleanup package.

Analyst: W. Flory

■This analysis was prepared by nonpartisan House staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.