House
Legislative
Analysis
Section

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

COMPUTER CRIMES

House Bill 5184 as passed by the House
Sponsor: Rep. Gene DeRossett

House Bill 5185 as passed by the House
Sponsor: Rep. William O'Neil

House Bill 5186 as passed by the House
Sponsor: Rep. Jim Howell

House Bill 5187 as passed by the House
Sponsor: Rep. Ruth Jamnick

Second Analysis (4-4-00)
Committee: Criminal Law and Corrections

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. [For further description of the current penalty system, see *Background Information*.]

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.

House Bill 5185 would expand the prohibition against using a computer, computer program, system or network to commit a crime by also prohibiting the use of a computer, computer program, system, or network in an *attempt* to commit a crime. In addition, the bill would specify that prosecution for using a computer to commit or attempt to commit a crime would not prevent that person from being charged with, convicted of, or punished for any other violation of law, including the underlying offense. It would further provide that prosecution for using a computer to attempt or commit a crime would not require conviction of 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 clarify that the current penalty language in the act, which sets up a tiered system of penalties depending upon the amount of money involved in the crime, applies to the use of a computer to defraud or otherwise obtain money, property, or services by false pretenses. In addition, the bill would establish specific penalties for unlawfully accessing a computer, computer program, system or network and for using a computer to commit or attempt to commit a crime.

Unlawfully accessing a computer, computer program, system, or network would be a felony punishable by imprisonment for no more than five years and/or a fine of no more than $10,000 for a first offense and punishable by up to ten years imprisonment and/or a fine of up to $50,000 for a subsequent offense.

The penalties for using a computer to commit or attempt to commit a crime would be based upon the underlying crime that was attempted or committed; thus, the violator would have committed both the underlying crime and the crime of using a computer in the commission of the underlying crime. If a person used a computer to commit or attempt to commit a misdemeanor that was punishable by imprisonment for one year or less, the use of the computer in the commission or attempted commission of that crime would be an additional misdemeanor punishable by imprisonment for up to one year and/or a fine of up to $5,000. If a person used a computer to commit a misdemeanor with a maximum term of imprisonment of at least one year but less than two years imprisonment, the use of a computer in the commission or attempted commission of that crime 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 felony with a maximum term of imprisonment of a least two years but less than four years, the use of a computer in the commission or attempted commission of that crime 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 at least four years but less than ten years, the use of a computer in the commission or attempted commission of that crime 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 in the commission or attempted commission of that crime 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 in the commission or attempted commission of that crime 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 in the commission or attempted commission of a crime, the court could order the penalty for using a computer to commit or attempt to commit a crime to be served consecutively and preceding any term of imprisonment that was imposed for the underlying crime.

The bill would also specifically define a "prior conviction" to include violations or attempted violations of the act or of a substantially similar law of the United States, another state, or a political subdivision of another state.

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

for each crime would be the same as 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 C 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 C crime with a statutory maximum of 20 years.

None of the bills would be enacted unless each of the other bills were also enacted. The package would take effect on July 1, 2000.

BACKGROUND INFORMATION:

Under the current law, penalties for violations of the computer crime act are determined under the following system. If the violation involves less than $200, the crime is a misdemeanor punishable by imprisonment for up to 93 days and/or a fine of up to $500 (or three times the aggregate amount of the loss, whichever is greater). If the violation involves an aggregate amount from $200 to $1,000, or is a second violation, it is a misdemeanor punishable by imprisonment for up to one year and/or a fine of up to $2,000 (or three times the aggregate amount of the loss, whichever is greater). If the violation involves an aggregate amount of from $1,000 to $20,000, or a third violation, it is a felony punishable by imprisonment for up to five years and/or a fine of up to $10,000 (or three times the aggregate amount of the loss, whichever is greater). A violation that involved an aggregate amount of $20,000 or more, or a fourth or subsequent violation, is a felony punishable by up to ten years imprisonment and /or a fine of up to three times the aggregate amount.

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)

ARGUMENTS:

For:

The primary purpose of the bills is to revise the current law so that it will apply to certain crimes that the current 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 could 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.

POSITIONS:

The Department of Attorney General supports the bills. (3-30-00)

The Prosecuting Attorneys Association of Michigan supports the bills. (3-30-00)

The Department of State Police supports the bills. (4-4-00)

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.