105TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
2d Session } { 105–418

# WIRELESS TELEPHONE PROTECTION ACT

FEBRUARY 24, 1998.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCOLLUM, from the Committee on the Judiciary, submitted the following

## REPORT

[To accompany H.R. 2460]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 2460) to amend title 18, United States Code, with respect to scanning receivers and similar devices, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS



The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Wireless Telephone Protection Act".

59–006

SEC. 2. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COUNTERFEIT ACCESS DEVICES.

(a) UNLAWFUL ACTS.—Section 1029(a) of title 18, United States Code, is amended—

(1) by redesignating paragraph (9) as paragraph (10); and

(2) by striking paragraph (8) and inserting the following:

"(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

"(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured for altering or modifying a telecommunications instrument so that such instrument may be used to obtain unauthorized access to telecommunications services; or".

(b) PENALTIES.—

(1) GENERALLY.—Section 1029(c) of title 18, United States Code, is amended to read as follows:

"(c) PENALTIES.—The punishment for an offense under subsection (a) of this section is—

"(1) in the case of an offense that does not occur after a conviction for another offense under this section—

"(A) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

"(B) if the offense is under paragraph (4), (5), (8), or (9), of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both; and

"(2) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both.".

(2) ATTEMPTS.—Section 1029(b)(1) of title 18, United States Code, is amended by striking "punished as provided in subsection (c) of this section" and inserting "subject to the same penalties as those prescribed for the offense attempted".

(c) DEFINITIONS.—Section 1029(e)(8) of title 18, United States Code, is amended by inserting before the period "or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument".

(d) APPLICABILITY OF NEW SECTION 1029(a)(9).—

(1) IN GENERAL.—Section 1029 of title 18, United States Code, is amended by adding at the end the following:

"(g) It is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person under contract with, a facilities-based carrier, for the purpose of protecting the property or legal rights of that carrier, to use, produce, have custody or control of, or possess hardware or software configured as described in that subsection (a)(9).".

(2) DEFINITION.—Section 1029(e) of title 18, United States Code is amended—

(A) by striking "and" at the end of paragraph (6);

(B) by striking the period at the end of paragraph (7) and inserting a semicolon; and

(C) by striking the period at the end of paragraph (8) and inserting "; and"; and

(D) by adding at the end the following:

"(9) the term 'facilities-based carrier' means an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934.".

(e) AMENDMENT OF FEDERAL SENTENCING GUIDELINES FOR WIRELESS TELEPHONE CLONING.—

(1) IN GENERAL.—Pursuant to its authority under section 994 of title 28, United States Code, the United States Sentencing Commission shall review and amend the Federal sentencing guidelines and the policy statements of the Commission, if appropriate, to provide an appropriate penalty for offenses involving the cloning of wireless telephones (including offenses involving an attempt or conspiracy to clone a wireless telephone).

(2) FACTORS FOR CONSIDERATION.—In carrying out this subsection, the Commission shall consider, with respect to the offenses described in paragraph (1)—

(A) the range of conduct covered by the offenses;

(B) the existing sentences for the offenses;

(C) the extent to which the value of the loss caused by the offenses (as defined in the Federal sentencing guidelines) is an adequate measure for establishing penalties under the Federal sentencing guidelines;

(D) the extent to which sentencing enhancements within the Federal sentencing guidelines and the court's authority to sentence above the applicable guideline range are adequate to ensure punishment at or near the maximum penalty for the most egregious conduct covered by the offenses;

(E) the extent to which the Federal sentencing guideline sentences for the offenses have been constrained by statutory maximum penalties;

(G) the extent to which Federal sentencing guidelines for the offenses adequately achieve the purposes of sentencing set forth in section 3553(a)(2) of title 18, United States Code;

(H) the relationship of Federal sentencing guidelines for the offenses to the Federal sentencing guidelines for other offenses of comparable seriousness; and

(I) any other factor that the Commission considers to be appropriate.

## PURPOSE AND SUMMARY

H.R. 2460 amends section 1029 of Title 18 of the United States Code, relating to fraud and related activity in connection with access devices. The bill amends subsection (a)(8) of section 1029 by deleting the "intent to defraud" requirement which exists under current law in order to prove a violation of that section. This section relates to persons who knowingly use, produce, traffic in, have custody or control of, or possess hardware or software which has been configured for altering or modifying a telecommunications instrument. As a result of the amendments made by the bill, in order to prove a violation of section 1029, law enforcement officials will no longer have to prove that a defendant possessing such hardware or software did so with the intent to defraud another person.

The amendment to the statute is being made because law enforcement officials occasionally have been thwarted in proving true violations of the statute by the "intent to defraud" requirement. As the hardware and software in question can be used only for the purpose of altering or modifying telecommunications instruments, persons other than those working in the telecommunications industry have no legitimate reason to possess the equipment. Therefore, requiring the government to prove an "intent to defraud" in order to prove a violation of the section for possessing this equipment is not necessary. By eliminating this requirement from existing law this bill will make it easier to obtain convictions against criminals who possess this equipment before they actually use it for illegal purposes.

## BACKGROUND AND NEED FOR THE LEGISLATION

Cellular telephone fraud is a significant criminal activity in the United States. Each year the wireless telephone industry loses hundreds of millions of dollars in revenue as the result of calls made from stolen telephones or cloned telephones. In 1996, the last year for which data is available, the wireless telephone industry has reported that the aggregate loss to the industry was approximately $710 million. While the industry estimates that the losses for 1997 will be less, largely attributable to anti-fraud technologies it has developed and employed, the loss to this industry is still unacceptably high.

As significant as is the loss of revenue to the wireless telephone industry, cellular telephone fraud poses another, more sinister, crime problem. A significant amount of the cellular telephone fraud which occurs in this country is connected with other types of crime. In most cases, criminals used cloned phones in an effort to evade detection for the other crimes they are committing. This phenomenon is most prevalent in drug crimes, where dealers need to be in constant contact with their sources of supply and confederates on the street. These criminals often use several cloned phones in a day, or switch from one cloned phone to another each day, in order to evade detection. Most significantly, this technique thwarts law enforcement's efforts to use wiretaps in order to intercept the criminals' conversations in which they plan their illegal activity.

In 1994, Congress passed the Communications Assistance for Law Enforcement Act (Public Law No. 103–414) which, in part, amended 18 U.S.C. §1029, which concerns fraud and related activity in connection with access devices. That act added a new provision to section 1029 to make it a crime for persons to knowingly, and with intent to defraud, use, produce, traffic in, or have custody or control of, or possess a scanning receiver or hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services.

Law enforcement officials have testified before the Subcommittee on Crime that it is often hard to prove the intent to defraud aspect of this section with respect to the possession of hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services. In the most common case, law enforcement officials will arrest criminals for other crimes and find telephone cloning equipment in the possession of the criminals. Without finding specific evidence that the criminals intended to use this equipment to clone cellular telephones, law enforcement officials often have been thwarted in an effort to prove a violation of this statute. But because there is no legitimate reason why any person not working for wireless telephone industry carriers would possess this equipment, there is no question that these criminals intended to use that equipment to clone cellular telephones. Law enforcement officials have informed the Committee that deleting the "intent to defraud" requirement from section 1029(a)(8) with respect to this equipment would enable the government to punish a person who merely possesses this equipment, as well as those who produce, traffic in, or have custody or control over it.

While the Committee is generally hesitant to criminalize the mere possession of technology without requiring proof of an intent to use it for an improper purpose, the testimony before the Subcommittee of Crime, both by law enforcement agencies and representatives of the wireless telephone industry, confirms that the only use for this type of equipment, other than by persons employed in the wireless telephone industry and law enforcement, is to clone cellular telephones. While wireless telecommunications companies use this equipment to test the operation of legitimate cellular telephones, to test the anti-fraud technologies their companies employ to thwart the use of cloned telephones, and in other

ways to protect their property and legal rights, the equipment has no other legitimate purpose. Thus, there is no legitimate reason for any other person to possess this equipment. In short, the requirement in existing law to prove an intent to use this equipment for an illegal purpose is unnecessary.

The bill H.R. 2460, amends existing law by deleting the intent to defraud requirement currently found in section 1029(a)(8). The bill strikes current subsection (a)(8) of section 1029 and replaces it with two separate subsections. New paragraph (8) restates the language presently found in section 1029(a)(8)(A). New paragraph (9) restates the introductory phrase of existing paragraph (8), but omits the "intent to defraud" requirement and essentially restates the text of existing subparagraph (B) of current paragraph (8).

The bill also clarifies the penalties which may be imposed for violations of section 1029. Under existing law, violations of subsections (a)(5), (6), (7), or (8) are subject to a maximum penalty of 10 years under section 1029(c)(1). However, these same violations are also subject to a maximum penalty of 15 years under subsection (c)(2) of that same section. This unintentional duplication of penalty provisions for these crimes should be corrected. The bill corrects this problem by restating the punishment section of section 1029 to more clearly state the maximum punishment for violations of each paragraph of section 1029(a).

In order to ensure that telecommunications companies may continue to use these devices, the bill provides that it is not a violation of new subsection (a)(9) for an officer, employee, or agent of, or person under contract with, a facilities-based carrier to use, produce, have custody or control of, or possess hardware or software as described in that subsection if they are doing so for the purpose of protecting the property of or legal rights of that carrier. Section 1029 presently contains an exception to that section's prohibition for any lawful investigative, protective, or intelligence activities of law enforcement agencies of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States. The bill also defines "facilities-based carrier" in order to make it clear that the exception to new subsection (a)(9) is only available to officers, employees, agents, or contractors of companies that actually own communications transmission facilities, and persons under contract with those companies, because only those persons have a legitimate reason to use this property to test the operation of and perform maintenance on those facilities, or otherwise to protect their property or legal rights of the carriers.

The bill also amends the definition of scanning receiver presently found in subsection (e)(8) of section 1029. Under that definition, a scanning receiver is a device or apparatus "that can be used to intercept a wire or electronic communication in violation of Chapter 119" of Title 18. The bill would add to that definition to ensure that the term "scanning receiver" will be understood to also include devices which intercept electronic serial numbers, mobile identification numbers, or other identifiers of telecommunications service, equipment, or instruments.

Finally, the bill provides direction to the United States Sentencing Commission to review and amend, if appropriate, its guidelines and policy statements so as to provide an appropriate penalty for

offenses involving cloning of wireless telephones. The bill states eight factors which the Commission is to consider in reviewing existing guidelines and policy statements.

## HEARINGS

The Committee's Subcommittee on Crime held a hearing on the subject of cellular telephone fraud on September 11, 1997. The Subcommittee held no hearings on H.R. 2460.

## COMMITTEE CONSIDERATION

On October 9, 1997, the Subcommittee on Crime met in open session and ordered reported favorably the bill, H.R. 2460, by a voice vote, a quorum being present. On October 29, 1997, the Committee met in open session and ordered reported favorably the bill, H.R. 2460, without amendment by voice vote, a quorum being present. At the direction of the Committee, the staff was directed to make technical and conforming changes in the bill which are incorporated in the amendment in the nature of a substitute reported.

## VOTE OF THE COMMITTEE

There were no recorded votes on the bill H.R. 2460.

## COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 2(l)(3)(A) of rule XI of the rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

## COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT FINDINGS

No findings or recommendations of the Committee on Government Reform and Oversight were received as referred to in clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives.

## NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 2(l)(3)(B) of House rule XI is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

## CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 2(l)(3)(C) of rule XI of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 2460, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 403 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
*Washington, DC, October 31, 1997.*

Hon. HENRY J. HYDE,
*Chairman, Committee on the Judiciary, House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2460, the Wireless Telephone Protection Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

JAMES L. BLUM
(For June E. O'Neill, Director).

Enclosure.

*H.R. 2460—Wireless Telephone Protection Act*

CBO estimates that enacting H.R. 2460 will have a small impact on discretionary spending over the next five years. In addition, the bill could lead to increases in both direct spending and receipts, but the amounts involved would be less than $500,000 a year. Because the bill could affect direct spending and receipts, pay-as-you-go procedures would apply. H.R. 2460 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act of 1995 and would impose no costs on state, local, or tribal governments.

H.R. 2460 would make it easier for United States attorneys to prosecute certain fraud offenses involving wireless telephones. The bill also would direct the United States Sentencing Commission to review the federal sentencing guidelines for wireless telephone fraud.

Enacting H.R. 2460 could increase the number of successful prosecutions against perpetrators of wireless telephone fraud. In turn, collections of criminal fines could increase, but we estimate that any increase would be less than $500,000 annually. Criminal fines are deposited in the Crime Victims Fund and spent the following year. Thus, any change in direct spending would match the increase in revenues with a one-year lag.

Any increase in convictions in fraud cases would result in additional federal costs, subject to the availability of appropriations, to accommodate more prisoners. Prison costs would also rise if the U.S. Sentencing Commission elects to enhance prison sentences for wireless telephone fraud, as allowed by the bill. CBO cannot predict the effect of H.R. 2460 on conviction rates or the actions of the U.S. Sentencing Commission, but any increase in discretionary spending over the next five years is likely to be small.

The CBO staff contact for this estimate is Mark Grabowicz. This estimate was approved by Paul N. Van de Water, Assistant Director for Budget Analysis.

## CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to Rule XI, clause 2(l)(4) of the Rules of the House of Representatives, the Committee finds the authority for this legislation in Article I, section 8 of the Constitution.

## SECTION-BY-SECTION ANALYSIS

*Section 1. Short Title.* Section 1 of the bill states the short title of the bill as the "Wireless Telephone Protection Act."

*Section 2. Fraud and Related Activity in Connection with Counterfeit Access Devices.* Section 2 of the bill sets forth the amendments made by the bill to section 1029 of Title 18 of the United States Code.

Section 2(a) of the bill deletes existing paragraph (8) from section 1029(a) and replaces it with two new paragraphs. New paragraph (8) restates in its entirety the text of old paragraph (8)(A). The text of new paragraph (9) is essentially the text of existing paragraph (8)(B), except that the existing requirement that the government show an "intent to defraud" in order to prove a violation has been deleted. Therefore, as section 1029 will be amended, in order to prove a violation of new subsection (a)(9), the government need only prove that the defendant knowingly used, produced, trafficked in, had custody or control of, or possessed hardware or software with the knowledge that it had been configured for altering or modifying a telecommunications instrument so that the instrument could be used to obtain unauthorized access to telecommunications services.

As amended, new subsection (a)(9) does not make it a crime to simply possess a wireless telephone or access device that has been manufactured or modified to obtain unauthorized use of telecommunications services. Under other subsections of section 1029, however, it will continue to be illegal to use, produce, traffic in, have custody or control of, or possess such a telephone or access device if the act was done with the intent to defraud another person. This is current law, and it remains unchanged by the bill.

The statute, as amended, also does not prohibit persons from simply possessing equipment that only intercepts electronic serial numbers or wireless telephone numbers (defined as "scanning receivers" under section 1029, as amended by the bill). For example, companies that produce technology to sell to carriers or state and local governments which ascertains the location of wireless telephones as part of enhanced 911 services do not violate section 1029 by their actions. Under new subsection (a)(8), however, it will continue to be illegal to use, produce, traffic in, have custody or control of, or possess a scanning receiver if such act was done with the intent to defraud another person. This also is current law, and it remains unchanged by the bill.

While not specifically defined in the bill, the Committee intends that the term "telecommunications instrument" as used in new subsection (a)(9) will be construed to mean the type of device which can be used by individuals to transmit or receive wireless telephone calls. The term should be construed to include within its definition the microchip or card which identifies the device or communications transmitted through the device. The term "telecommunication

services" should be given the same meaning as the term "telecommunication service" defined in section 3 of title I of the Communications Act of 1934 (47 U.S.C. §153).

Section 2(b) of the bill amends all of existing subsection (c) of section 1029. Due to a previous amendment to this subsection, an inconsistency exists in current law with respect to the maximum punishment which may be imposed for violations of current subsections (a) (5), (6), (7), or (8). Currently, the maximum punishment for violations of these paragraphs is 10 years under subsection (c)(1) but 15 years under subsection (c)(2). Clearly, it is inappropriate for there to be different maximum punishments which may be imposed for violations of these subsections. Section 2(b) of the bill eliminates this inconsistency by clearly stating the maximum punishments which may be imposed for violations of section 1029.

Section 2(b) of the bill also amends existing subsection (b)(1) of section 1029 to state more clearly the maximum punishment which may be imposed for attempts to commit the crimes described in section 1029. As amended, subsection (b)(1) will provide that convictions for attempts under section 1029 are to be subject to the same penalties as those proscribed for the offense attempted.

Section 2(c) of the bill amends the definition of "scanning receiver" currently found in section 1029(e)(8). The bill adds to the definition of scanning receiver additional language to ensure that the defined term is understood to include a device or apparatus that can be used to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument.

Section 2(d) of the bill creates an exception to the crime described in new subsection (a)(9) for persons who are employed by or under contract with certain telecommunications carriers. The new exception provides that it is not a violation of new subsection (a)(9) for an officer, employee, or agent of a facilities-based carrier, or a person under contract with a facilities-based carrier, to use, produce, have custody or control of, or possess hardware or software configured as described in subsection (a)(9). Thus, these persons legally may continue to possess and manufacture this type of hardware or software. Additionally, these persons legally may send such hardware or software through the mails or send or carry it in interstate commerce.

It should be noted, however, that these actions are only permitted under the exception if these actions were taken for the purpose of protecting the property or legal rights of the facilities-based carrier. The Committee intends that the phrase "for the purpose of protecting the property or legal rights of the carrier" be narrowly construed. Only such actions which might be deemed to part of the ordinary course of business of a telecommunications carrier, such as actions involving maintenance on or modifications to a telecommunications system, or which are designed to test the operation of the system or the system's ability to deter unauthorized usage including the reverse engineering of hardware or software configured as described in new subsection (a)(9), should be deemed to fall within this exception. Acts taken with the intent to defraud another, even if taken by officers, employees, or agents of a facili-

ties-based carrier, or persons under contract with a facilities-based carrier, would still violate the statute.

The Committee takes particular note of the fact that under some circumstances a facilities-based carrier may use this equipment to intercept signals carried on another telecommunications carrier's system for the purpose of testing whether customers of the one carrier may be able to utilize the other carrier's system when those customers initiate or receive calls while inside the other carrier's geographic area of operation. It is the Committee's understanding that, in the past, these types of legitimate interceptions have always occurred with the express consent of the two carriers involved. The Committee believes that this is the appropriate practice. Thus, the exception created by subsection (d) of the bill should only be understood to apply to situations where the other carrier has consented to the use of this equipment on its system.

Section (d) of the bill also adds new paragraph (9) to subsection (e) of section 1029 in order to define the term "facilities-based carrier" as it is used in the exception to new subsection (a)(9). That term is defined to mean an entity that owns communications transmissions facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission. Thus, it does not include so-called "resellers" of wireless telephone air time, companies which buy blocks of air time and resell it to retail customers. The definition also does not include companies which hold nominal title to telecommunications equipment but which have no responsibility for their operations or for performing maintenance on them. Finally, the definition does not include persons or companies which may own and operate tangible telecommunications equipment but which do not hold the appropriate license for that purpose issued by the Federal Communications Commission.

Section 2(e) of the bill directs the United States Sentencing Commission to review and amend its sentencing guidelines and policy statements, if appropriate, to provide an appropriate penalty for offenses involving the cloning of wireless telephones. This section of the bill states a number of factors which the Sentencing Commission is directed to consider during its review. The Committee is concerned that violations of section 1029 are not punished as severely as other, similar, fraud crimes are punished under the Sentencing Commission's sentencing guidelines and, in any event, are not punished as severely as they should be in light of the magnitude of loss resulting from this crime and the fact that this crime is often used to facilitate more serious crimes. This section of the bill directs the Sentencing Commission to consider these and other factors in making to Congress as part of its annual reporting process whatever recommendations it deems appropriate with respect to the guidelines for imposing punishment for violations of section 1029.

## AGENCY VIEWS

No agency views were received with respect to the bill H.R. 2460.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

## SECTION 1029 OF TITLE 18, UNITED STATES CODE

### § 1029. Fraud and related activity in connection with access devices

(a) Whoever—
(1) * * *

* * * * * * *

[(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses—
[(A) a scanning receiver; or
[(B) hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services, or]

*(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;*

*(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured for altering or modifying a telecommunications instrument so that such instrument may be used to obtain unauthorized access to telecommunications services; or*

[(9)] *(10)* without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)(1) Whoever attempts to commit an offense under subsection (a) of this section shall be [punished as provided in subsection (c) of this section] *subject to the same penalties as those prescribed for the offense attempted.*

* * * * * * *

[(c) The punishment for an offense under subsection (a) or (b)(1) of this section is—

[(1) a fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a) (2), (3), (5), (6), (7), (8), or (9) of this section which does not occur after a conviction for another offense under either such subsection, or an attempt to commit an offense punishable under this paragraph;

[(2) a fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment for not more than fifteen years, or both, in the case of an offense under subsection (a) (1), (4), (5), (6), (7), or (8) of this section which does

not occur after a conviction for another offense under either such subsection, or an attempt to commit an offense punishable under this paragraph; and

[(3) a fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this paragraph.]

*(c) PENALTIES.—The punishment for an offense under subsection (a) of this section is—*

*(1) in the case of an offense that does not occur after a conviction for another offense under this section—*

*(A) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and*

*(B) if the offense is under paragraph (4), (5), (8), or (9), of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both; and*

*(2) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both.*

* * * * * * *

(e) As used in this section—

(1) * * *

* * * * * * *

(6) the term "device-making equipment" means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device; [and]

(7) the term "credit card system member" means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system[.];

(8) the term "scanning receiver" means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119[.] *or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument; and*

*(9) the term "facilities-based carrier" means an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934.*

* * * * * * *

*(g) It is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person under contract with, a facilities-based carrier, for the purpose of protecting the property or legal rights of that*

*carrier, to use, produce, have custody or control of, or possess hardware or software configured as described in that subsection (a)(9).*

○