Cellular Telephone Cloning

Final Report

Economic Crimes Policy Team

United States Sentencing Commission

January 25, 2000

Paula Biderman
Anne Blanchard
Tom Brown
Paula Desio
Jean Gabriel
Greg Gilmore
Christine Kitchens
Linda Maxfield
Rachel Pierce
Mary Rushen
Courtney Semisch
Andy Purdy, Chair

Executive Summary

The Economic Crimes Policy Team was chartered to advance the Commission's work in several areas, including the development of options for implementing the directives contained in the Wireless Telephone Protection Act (Pub. L. No. 105-172; April 24, 1998). Specifically, this act amended 18 U.S.C. § 1029 (Fraud and related activity in connection with access devices) with regard to the cloning of cellular telephones. The report details the background, analysis, findings and policy options identified by the team.

Wireless Telephone Protection Act

Because of increasing financial losses to the telecommunications industry and the growing use of cloned phones in connection with other criminal activity, Congress passed the Wireless Telephone Protection Act (WTPA) in April 1998. The legislative history indicates that, in amending 18 U.S.C. § 1029, Congress was attempting to address two primary concerns presented by law enforcement and the wireless telecommunications industry.[1]

First, law enforcement officials testified at congressional hearings that they were having difficulty proving the "intent to defraud" element of the pre-amendment provision regarding some equipment used to clone phones.[2] Although there is no legitimate reason to possess the equipment unless an individual is employed in the telecommunications industry, the prosecution often could not prove that the equipment was possessed with the intent to defraud.

Second, law enforcement officials often discovered cloning equipment and cloned cellular telephones in the course of investigating other criminal activities, such as drug trafficking and other fraud. The use of cloned phones to facilitate other crimes increases the ability of offenders to escape detection because of the increased mobility and anonymity afforded by the phones. Gangs and foreign terrorist groups are also known to sell or rent cloned phones to finance their illegal activities.

With these concerns in mind, Congress amended section 1029 in 1998. The significant changes to the statute include—

- Elimination of the intent to defraud element with respect to persons who knowingly use, produce, traffic in, have custody or control of, or possess hardware (a "copycat box") or software which has been

[1] Representative Sam Johnson, who introduced the House version of the bill, was victimized by cellular phone fraud. He was billed for over $6,000 in calls made by a cloned phone.

[2] Prior to the 1998 amendment, 18 U.S.C. § 1029 required that the defendant knowingly and with intent to defraud produced, used, possessed or trafficked in hardware (a "copycat box") or software which had been configured for altering or modifying a telecommunications instrument. Scanning receivers do have legitimate purposes.

configured for altering or modifying a telecommunications instrument[3];

- Modification of the current definition of "scanning receiver" to ensure that the term is understood to include a device that can be used to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument; and

- Correction of an error in the current penalty provision of 18 U.S.C. § 1029 that provided two different statutory maximum penalties (ten and 15 years) for the same offense. With respect to cellular phone cloning, the Act makes clear that a person convicted of such an offense without a prior section 1029 conviction is subject to a statutory maximum of 15 years; a person convicted of such an offense after a prior section 1029 conviction is subject to a statutory maximum of 20 years.

In addition to the amendments to section 1029, the Wireless Telephone Protection Act directs the Commission to "review and amend the federal sentencing guidelines and the policy statements of the Commission, and, if appropriate, to provide an appropriate penalty for offenses involving the cloning of wireless telephones. . . ."[4] The Act also directs the Commission to consider eight specific factors:

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

(B) the existing sentences for the offense;

(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;

---

[3] This offense was formerly covered by subsection (a)(8); the legislation created a new subsection (a)(9) for the offense.

[4] Wireless Telephone Protection Act (Pub. L. No. 105-418, April 24, 1998).

(F) the extent to which federal sentencing guidelines for the offense(s) adequately achieve the purposes of sentencing set forth in 18 U.S.C. § 3553(a)(2);

(G) the relationship of the federal sentencing guidelines for these offenses to offenses of comparable seriousness; and

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

How A Phone Is Cloned

The "cloning" of a cellular telephone occurs when the account number of a victim telephone user is stolen and reprogrammed into another cellular telephone. Each cellular phone has a unique pair of identifying numbers: the electronic serial number ("ESN") and the mobile identification number ("MIN"). The ESN/MIN pair can be cloned in a number of ways without the knowledge of the carrier or subscriber through the use of electronic scanning devices. After the ESN/MIN pair is captured, the cloner reprograms or alters the microchip of any wireless phone to create a clone of the wireless phone from which the ESN/MIN pair was stolen. The entire programming process takes ten-15 minutes per phone. After this process is completed, both phones (the legitimate and the clone) are billed to the original, legitimate account.

The cellular telephone industry does not charge legitimate, victimized customers for fraudulent calls; rather the companies absorb the losses themselves. In addition to losses due to fraudulent billing, the cellular companies incur losses due to the fees paid for connections and long-distance charges.

Work of the Economic Crimes Policy Team

The Team reviewed the Wireless Telephone Protection Act and its legislative history; studied various literature and materials available on the cloning of cellular telephones; analyzed cloning cases sentenced in fiscal year 1998; reviewed relevant case law; and, met with representatives of the U.S. Department of Justice, U.S. Treasury Department, U.S. Secret Service, and the Cellular Telecommunications Industry Association (CTIA). In addition to Commission data, the Team also received and analyzed data from CTIA and the U.S. Secret Service.

To address the specific considerations outlined by the WTPA, the Team analyzed a 50 percent random sample of cases sentenced in FY 98 under 18 U.S.C. § 1029. The 50 percent sample of 394 cases yielded 47 cases involving cellular fraud. Because the selection cases was limited to 18 U.S.C. § 1029, the full range of conduct in cloning cases may not be represented. However, the review of this large proportion of cases convicted under section 1029 provided reliable information and yielded several interesting findings. First, the majority of defendants convicted of cloning offenses are manufacturers or distributors of cloned phones. Second, although there is some indication from the sample of cloning cases that cloning behavior occurs with other illegal behavior, the Team could not determine how widespread this conduct is. Third, the determination of loss in cloning offenses is problematic because it appears that loss is not

calculated consistently. Consequently, it is possible that disparate sentences are being imposed on similar cloning offenders.

Policy Considerations

The Team reviewed cloning offenses in the context of each specific factor enumerated in the WTPA. As a result, the Team identified two concerns regarding whether the current guideline for cloning offenses (§2F1.1 Fraud) provides appropriate penalties:

1. The range of conduct covered by the offenses may not adequately be covered by the current guideline; and

2. the determination of loss in cloning cases is not being accomplished in a consistent, appropriate manner.

Both issues are presented below in more detail along with possible options for amendment.

Range of Conduct

Manufacturing and Distributing

Section 1029 covers cloning behavior that ranges from mere possession of a cloned phone to using, producing, or trafficking in cloning equipment. The statutory maximum for these offenses is ten or 15 years, depending upon the conduct, and are sentenced under §2F1.1. This guideline provides different punishment levels based on whether any or all of the following three factors are applicable: (1) the amount of "loss" involved in the offense;[5] (2) the offense involved "more than minimal planning";[6] and (3) the offense involved "sophisticated means."[7] However, the current guideline does not provide distinctions in sentence severity based on whether the defendant was involved in manufacturing or distributing cloned phones. It is possible that without a separate enhancement for manufacturing or distributing, the current fraud guideline does not adequately distinguish between possessing a cloned phone and the more serious conduct of

[5] Section 2F1.1 provides increases in offense level based on loss beginning with loss amounts in excess of $2,000 (add one level, about 12 1/2% increase); for example, a loss in excess of $40,000 would provide for five additional levels, a loss in excess of $800,000 (11 additional levels), and a loss in excess of $10,000,000 (15 additional levels).

[6] If the specific offense characteristic of "more than minimal planning" is applicable, it provides for an increase of two levels (about 25% increase). §2F1.1(b)(2)(A).

[7] If the specific offense characteristic for "sophisticated means" is applicable, it provides for an increase of two levels. §2F1.1(b)(5)(C). Note that the enhancement for "sophisticated means" "requires conduct that is significantly more complex or intricate than the conduct that may form the basis for an enhancement for more than minimal planning under subsection (b)(2)(A). §2F1.1, comment. (n. 15).

manufacturing or distributing. Because the majority of the cloning cases under this guideline involve manufacturing and/or distribution, it is arguable that this common conduct warrants consideration of an amendment to provide a specific offense characteristic for this conduct.

The report presents two possible options to address this problem. The first option adds a specific offense characteristic to cover the actual offense conduct of manufacturing or distributing, or a specific offense characteristic to cover conduct involving the specific equipment prohibited by the statute. This amendment distinguishes between types of cloning offenders and enhances sentences in response to the concern that prompted congressional action. The second option provides a presumptive loss value for offenses involving manufacturing. This alleviates the need to add a specific offense characteristic to the fraud guideline while still ensuring that the sentence reflects the increased seriousness of the use of manufacturing equipment.

Additional Criminal Conduct

The use of a cloned phone to commit other crimes is one of the other top concerns within the scope of the WTPA expressed by Congress, the Treasury Department and the Secret Service. In fact, the Treasury Department recommended that the Commission amend §2F1.1 to "provide an enhancement for offenses in which fraudulently obtained telecommunications services are used to commit other crimes."[8]

The Team attempted to assess the use of cloned phones in other criminal conduct. However, this effort was somewhat hampered because the case review was limited to cases involving a § 1029 conviction. In other words, only cases known to involve a cloned phone (because of the §1029 conviction) were reviewed to assess the existence of additional criminal conduct. In order to accurately assess how widespread the use of cloned phones is in other offenses, the Team would have to do a sample of all offense types and read each case to determine if there was a cloned phone involved. In the sample of cloning cases, there were few cases involving other criminal conduct and no cases in which a clear connection existed between the use of the phone and the commission of the other offenses. The Commission may choose to study this issue further and postpone amendment action on this specific issue until sufficient data is available. However, if through further analysis, the Team finds that cloned phones are being used to commit additional criminal conduct, several policy questions exist:

1. Is an offense committed with the use of a cloned phone more serious than one committed without the use of a cloned phone?; and

[8] Letter dated November 17, 1998, from Treasury Department Under Secretary (Enforcement) James E. Johnson to Sentencing Commission General Counsel John R. Steer.

2. Does the use of a cloned phone—and its accompanying anonymity—in and of itself warrant an increase in the sentence?

If and when the Commission chooses to address the issue, several options are available. The first option adds an enhancement to §2F1.1, and/or other designated guidelines, (similar to §2K2.1(b)(5))[9] that increases sentences for the use or transfer of a cloned phone in connection with another offense. The second option includes adding a cross-reference to §2F1.1 that punishes offenders possessing cloned phones at the level for the offense with which the phone was used. This option could be implemented by itself, or in combination with the first option. The disadvantage to this second option is that these cross-references could result in the "tail wagging the dog" situation. In other words, a defendant could be convicted of a less serious offense and have his/her sentence increased considerably based on behavior that was proven by a preponderance standard when the more serious behavior could have been (or should have been charged).

Loss as an Adequate Measurement of Seriousness

It is clear from the Team's review that loss is inconsistently determined in cloning cases, thereby diminishing "loss" as an effective and adequate measure for establishing penalties. In particular, there are two concerns:

1) unused ESN/MIN pairs are sometimes disregarded in the determination of loss; and,

(2) varying and disparate methods of estimating actual and intended loss are used.

Inconsistent loss computations contribute to disparate sentences among cloners and offenders committing crimes of comparable seriousness.

This report presents two options for addressing this inconsistency. The first option involves a "minimalist" approach to resolving the issue that proposes several commentary changes to clarify the determination of loss in cloning cases. The second option aimed at increasing the consistency in application involves giving the courts more definitive rules for application.

Option one modifies the commentary to make clear that unused ESM/MIN pairs are to be used in determining intended loss. Providing a method for estimating loss in cloning cases would also standardize application, and reduce disparity among cloning offenders. Using an average is one possible method. This could help to alleviate some of the

[9] Section 2K2.1(b)(5) adds a 4 level enhancement in the firearm trafficking guideline if the defendant "used or possessed any firearm . . . in connection with another felony offense; or possessed or transferred any firearm or ammunition with knowledge, intent, or reason to believe that it would be used or possessed in connection with another felony offense".

disparity in sentences for cloning offenders by increasing consistency in the determination of loss. In addition, it would increase the ability of the loss enhancement to adequately measure the seriousness of the offense. Currently, without the inclusion of intended loss, the full seriousness of the offense is not being taken into consideration in the sentence imposed. However, this would not address how to determine the value of the unused pairs, and, if current practices prevail, varying methods for determining that value will be used. Therefore, some degree of disparity would remain.

The second option would provide a minimum or presumptive value for ESN/MIN pairs similar to the $100 per card minimum provided for credit cards in §2B1.1. The rule provides that loss in credit card cases includes any unauthorized charges made with stolen credit cards, but in no event less than $100.[10] The Treasury Department recommends that the current $100 per card minimum loss rule be expanded to include all access devices, and the minimum be increased to $1,000 per device to more adequately reflect the seriousness of these offenses. However, expanding the current credit card rule to cloning offenses does not resolve all the disparity problems. Because the current rule only addresses a minimum value, in cases in which courts used an amount above the minimum, the varying methods used to estimate the loss could still lead to disparate results.

Expanding the current credit card rule and increasing the minimum to $1,000 per device could be problematic in another way. In cases in which loss for one or more pairs is determined to be less than $1,000, using a $1,000 per pair minimum for other pairs within the same case could be inappropriate. This problem would not likely occur if the current $100 minimum was retained. For those who argue that the $100 amount is too low for access devices, an amount somewhere between $100 and $1,000 might be less problematic.

In light of the Treasury Department's recommendation, the Team reviewed a sample of 228 credit card cases, the most frequently occurring type of access device case, in part to determine if the offenses were sufficiently comparable to warrant application of the current credit card rule to both offenses. Credit cards are also interesting for comparison because the issue of determining intended loss for unused credit cards is similar to the unbilled ESN/MIN pair issue in cloning offenses.

Credit card cases and cloning cases are similar in several ways. The most significant similarity is that the determination of loss in both types of offenses includes unbilled, or unused accounts, and the use of the unbilled accounts in the determination of loss is inconsistent in both offenses.[11] Of the 31 credit card cases known to involve unbilled accounts, only seven (23%) used the unbilled accounts in the loss calculation;

---

[10] §2B1.1, comment.(n.4).

[11] Because many of the cases provided insufficient data, it is possible that the unbilled numbers were not used because it could not be proven by a preponderance of the evidence that the defendant intended to use them.

twenty-four percent of the cloning cases used unbilled ESN/MIN pairs. And, as in cloning cases, several different methods of determining the intended loss for the unbilled accounts were used.

The data suggests that credit card cases and cloning cases vary sufficiently to warrant consideration of different presumptive minimums, however the current $100 minimum may be too low. The Commission's data was insufficient to determine an average loss per cloned phone, however the average credit card loss per card is $3,775. According to the U.S. Treasury, credit card industry data indicates the average fraud loss in 1998 to be $1,040 per credit card.[12] Treasury also cited 1999 Secret Service statistics indicating an average fraud loss per credit card of $2,218 and cloned cellular telephone of $1,606. The Cellular Telecommunications Industry Association average loss per ESN/MIN pair for 1996-98 is $760.

[12] There are a number of reasons that the Commission data produced a greater average amount. The sources of the figures provided by both Treasury and the Secret Service are unknown to the Team. However, it is almost certain that they include both state and federal cases, and may include unprosecuted cases. The figure computed by the Team is based on a sample of 109 federally sentenced credit card fraud cases for which the exact number of credit cards and exact amount of charges were known. A number of agencies have indicated that U.S. Attorney offices have varying dollar amount thresholds for accepting fraud cases for prosecution. Thus, the Commission's figure is likely higher due to the smaller, more selective sample from which the cases were drawn.

Table of Contents

I. Introduction

This is the Final Report of the Economic Crimes Policy Team (hereafter, the "Team") regarding the directives contained in the Wireless Telephone Protection Act (Pub.L. 105-172; April 24, 1998).

The Economic Crimes Policy Team was chartered to advance the Commission's work in several areas including the development of options for implementing the directives contained in the Wireless Telephone Protection Act (WTPA).[13] This Act effectuated amendments to 18 U.S.C. § 1029 (Fraud and related activity in connection with access devices) related to the cloning of cellular telephones. The "cloning" of a cellular telephone occurs when the account number of a victim telephone user is stolen and reprogrammed into another cellular telephone. This report details the mission, background, analysis, and policy options of the Team.[14]

II. The Wireless Telephone Protection Act

Because of the increasing loss to the telecommunications industry from cloned telephones, and the growing use of cloned phones in conjunction with other criminal activity, Congress passed the Wireless Telephone Protection Act in April 1998. The legislative history indicates that in amending 18 U.S.C. § 1029, Congress was attempting to address two concerns presented by law enforcement and the wireless telecommunications industry.[15]

First, law enforcement officials testified at Congressional hearings that they had difficulty proving the "intent to defraud" element of the pre-amendment provision with regard to some equipment used to clone phones.[16] Although there is no legitimate reason to possess the equipment

---

[13] For this report, the team reviewed the Wireless Telephone Protection Act and its legislative history. We studied various literature and materials available on the cloning of cellular telephones. We also analyzed cloning cases, Commission data and case law. Finally, the team met with representatives from the U.S. Department of Justice and the U.S. Secret Service, and the Cellular Telecommunications Industry Association (CTIA). Interestingly, there may be less of a need for persons committing criminal offenses to use cloned phones for anonymity given the fact that persons can now buy inexpensive cellular telephones with prepaid minutes, with complete anonymity.

[14] The following members of the Team were designated to take the lead on issues related to cellular telephone cloning: Jeanneine Gabriel and Courtney Semisch.

[15] Representative Sam Johnson, who introduced the House version of the bill, was victimized by cellular phone fraud. He was billed for over $6,000 in calls made by a cloned phone.

[16] Prior to the 1998 amendment, 18 U.S.C. § 1029 required that the defendant knowingly and with intent to defraud produced, used, possessed or trafficked in hardware (a "copycat box") or software which had been configured for altering or modifying a telecommunications instrument. Scanning receivers do have legitimate purposes.

unless the person works in the telecommunications industry, law enforcement often could not prove that the equipment was possessed with the intent to defraud.

Second, law enforcement officers often find cloning equipment in the course of investigating other criminal activities, such as drug trafficking and certain types of fraud. The use of cloned phones to facilitate other crimes increases the ability of the offenders to escape detection because of the increased mobility and anonymity afforded by cloned phones. Gangs and foreign terrorist groups are also known to sell or rent cloned phones to generate moneys with which to finance their activities.[17]

With these concerns in mind, Congress amended section 1029 in the following ways:

- Eliminated the intent to defraud element with respect to persons who knowingly use, produce, traffic in, have custody or control of, or possess hardware (a "copycat box") or software which has been configured for altering or modifying a telecommunications instrument.[18] Accordingly, the government only has to prove that the defendant used or possessed the hardware or software with the knowledge that it had been configured for modifying a cellular phone so that the phone could be used to obtain unauthorized access to telecommunications services.

- Created an exception to this offense for law enforcement and persons who work in the legitimate telecommunications industry.

- Maintained the intent to defraud element with respect to persons who knowingly use, produce, traffic in, have control or custody of, or possess a scanning receiver.[19] The intent element was retained because a scanning receiver, unlike a copycat box, has a legitimate use when not used to intercept electronic serial numbers.

- Modified the current definition of "scanning receiver" to ensure that the term is understood to include a device that can be used to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument.

---

[17] See H.R. Rep. 105-418, at 10 (1998).

[18] This offense was formerly covered by subsection (a)(8); the legislation created a new subsection (a)(9) for the offense.

[19] Offense located at 18 U.S.C. § 1029(a)(8); definition of "scanning device" located at 18 U.S.C. § 1029(e).

- Corrected an error in the current penalty provision of 18 U.S.C. § 1029 that provided two different statutory maximum penalties (ten and 15 years) for the same offense. With respect to cellular phone cloning, the Act makes clear that a person convicted of such an offense without a prior section 1029 conviction, is subject to a statutory maximum of 15 years; a person convicted of such an offense after a prior section 1029 conviction is subject to a statutory maximum of 20 years.

- The legislation made clear that a person convicted of attempt is subject to the same penalties as the offense attempted.[20]

III. Congressional Directives

In addition to the amendments to section 1029, the Wireless Telephone Protection Act directs the Commission to ". . .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. . . ."[21] The Act also directs the Commission to consider eight specific factors:

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

(B) the existing sentences for the offense;

(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;

---

[20] The statute is also clear with respect to the penalty for conspiracy offenses. Under subsection (b)(2) of the statute, the maximum term of imprisonment for a conspiracy offense is one-half the maximum imprisonment provided for the substantive offense.

[21] Wireless Telephone Protection Act (Pub. L. No. 105-418, April 24, 1998).

(F) the extent to which Federal sentencing guidelines for the offense adequately achieve the purposes of sentencing set forth in 18 U.S.C. § 3553(a)(2);

(G) the relationship of the Federal sentencing guidelines for these offenses to offenses of comparable seriousness; and

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

IV. Background

The U.S. Secret Service and the wireless telecommunications industry are increasingly concerned about wireless fraud. First, the wireless telecommunication industry asserts that wireless fraud has grown exponentially since its introduction into the market. They estimate that wireless fraud costs the telecommunications industry over $650 million per year. Second, according to the Secret Service cloned phones are the communications medium of choice for criminals because it gives them mobile communications and anonymity. Cloned phones are difficult to detect and trace, and phone numbers can be changed in an instant. Law enforcement reports an increase in the number of cloned phones confiscated during investigations of other offenses, such as drug distribution and credit card fraud.

There are four major types of cellular fraud: counterfeit fraud, subscription fraud, network fraud, and call selling operations. Explanations of each are provided below. These cellular telecommunications violations are similar to other access device violations (*e.g.* credit cards) in that they involve unauthorized use and/or access to individual accounts. The changes in 18 U.S.C. § 1029 are aimed at counterfeit fraud, specifically, the cloning of cellular telephones.

- **Counterfeit Fraud (*cloning*)**: Involves the use of illegally altered cellular phones. Offenders gain access to legitimate account number combinations and reprogram them into other handsets to gain unauthorized access to those accounts.

- **Subscription Fraud**: Includes schemes related to fraudulently obtaining cellular telephone accounts. These may involve employees of the cellular carrier, forgery of application information, or theft of subscriber information.

- **Network Fraud**: This advanced type of fraud includes efforts to exploit weaknesses in phone switch equipment and billing systems. Manipulation of current systems can result in third party billing, use of nonexistent account numbers, or the use of multiple phones on single accounts.

- **Call Selling Operations**: This type of fraud involves using stolen calling card numbers and/or cellular account numbers to sell less expensive cellular long distance (often international) service to others.

A. How Wireless Technology Works

Each cellular phone has a unique pair of identifying numbers: the electronic serial number ("ESN") and the mobile identification number ("MIN"). The ESN is programmed into the wireless phone's microchip by the manufacturer at the time of production. The MIN is a ten-digit phone number that is assigned by the wireless carrier to a customer when an account is opened. The MIN can be changed by the carrier, but the ESN, by law, cannot be altered. When a cellular phone is first turned on, it emits a radio signal that broadcasts these numbers to the nearest cellular tower. The phone will continue to emit these signals at regular intervals, remaining in contact with the nearest cellular tower. These emissions (called autonomous registration) allow computers at the cellular carrier to know how to route incoming calls to that phone, to verify that the account is valid so that outgoing calls can be made, and to provide the foundation for proper billing of calls. This autonomous registration occurs whenever the phone is on, regardless of whether a call is actually in progress.

B. How A Phone Is Cloned

The ESN/MIN pair can be cloned in a number of ways without the knowledge of the carrier or subscriber through the use of electronic scanning devices. Some of these devices such as the Cellphone ESN reader and police scanners, have legitimate uses. Cellphone ESN readers, or blueboxes, are used by cellular technicians to test cell phones and equipment. A reader or bluebox is about the size of a shoebox. Digital Data Interpreters (DDI's) are devices specifically manufactured to intercept ESN/MINs. Cellular thieves can capture ESN/MINs using these devices by simply sitting near busy roads where the volume of cellular traffic is high. Numbers can be recorded by hand, one-by-one, or stored in the box and later downloaded to a computer. ESN/MIN readers can also be used from inside an offender's home, office, or hotel room, increasing the difficulty of detection.

After the ESN/MIN pairs are captured, the cloner reprograms or alters the microchip of any wireless phone to create a clone of the wireless phone from which the ESN/MIN pair was stolen. In order to reprogram a phone, the ESN/MINs are transferred using a computer loaded with specialized software[22], or a "copycat" box, a device whose sole purpose is to clone phones. The devices are connected to the cellular handsets and the new identifying information is entered into the phone. There are also more discreet, concealable devices used to clone cellular phones. Plugs and ES-Pros (also with no legitimate uses), which are about the size of a pager or small calculator, do not require computers or copycat boxes for cloning. The entire programming process takes ten-15 minutes per phone. After this process is completed, both phones (the legitimate and the clone) are billed to the original, legitimate account.

---

[22] Programming software needed to alter the microchip is readily available over the Internet, computer bulletin boards, and elsewhere.

When a phone is cloned, the criminal has free, anonymous access to the cell network until the customer or carrier identifies the offense. Generally a cloned phone is 'good' for about the length of a billing cycle, when the offense is discovered by the legitimate subscriber upon receipt of his cellular phone bill. Some carriers have installed profiling systems that can detect unusual or improbable calling patterns. For example, if one call is placed from New York at 1:00 PM and a second call is charged to the same ESN/MIN account from Miami at 1:30 PM that same day, the profiling system will terminate the second call because the phone has obviously been cloned. These profiling systems also flag dramatic increases in use patterns for individual accounts. These profiling and detection systems have been developed by the cellular carriers specifically to target wireless fraud.

Generally, a cellular account can only be accessed by one caller at a time. If both the legitimate and cloned cellular phones are being used in the same vicinity, both phones can only be used simultaneously if they are accessing a different phone switch. If they are using the same switch and one of the phones is in use, the second phone will not be able to dial out. Incoming calls may be routed to either the legitimate or cloned phone, depending on which one is detected first by the system. However, if the cloned phone is located in another city, any number of clones can access the same account (ESN/MIN) at the same time.

The cellular telephone industry does not charge legitimate, victimized customers for fraudulent calls, rather the companies absorb the losses themselves. In addition to losses due to fraudulent billing, the cellular companies incur losses due to the fees they pay for landline connections. These losses can be especially large when cloned phones are used for long distance calling.

V. Analysis of Cellular Phone Cloning Cases

In order to address the specific considerations outlined by the WTPA, the team analyzed a sample of cases sentenced under 18 U.S.C. § 1029 in fiscal year 1998 (FY98). Cases involving cellular telephones and the equipment used to clone them comprise a small proportion of the "access devices" cases defined in 18 U.S.C. § 1029.[23] To maximize the number of cases involving cellular fraud for close scrutiny, the Team analyzed a 50 percent random sample of all cases with at least one conviction for a violation of 18 U.S.C. § 1029 in FY98.[24] The 50 percent sample of 394 cases yielded 47 cases involving cellular fraud. The findings are discussed below in the context of each specific consideration enumerated in the WTPA.

A. The Range of Conduct for the Offenses

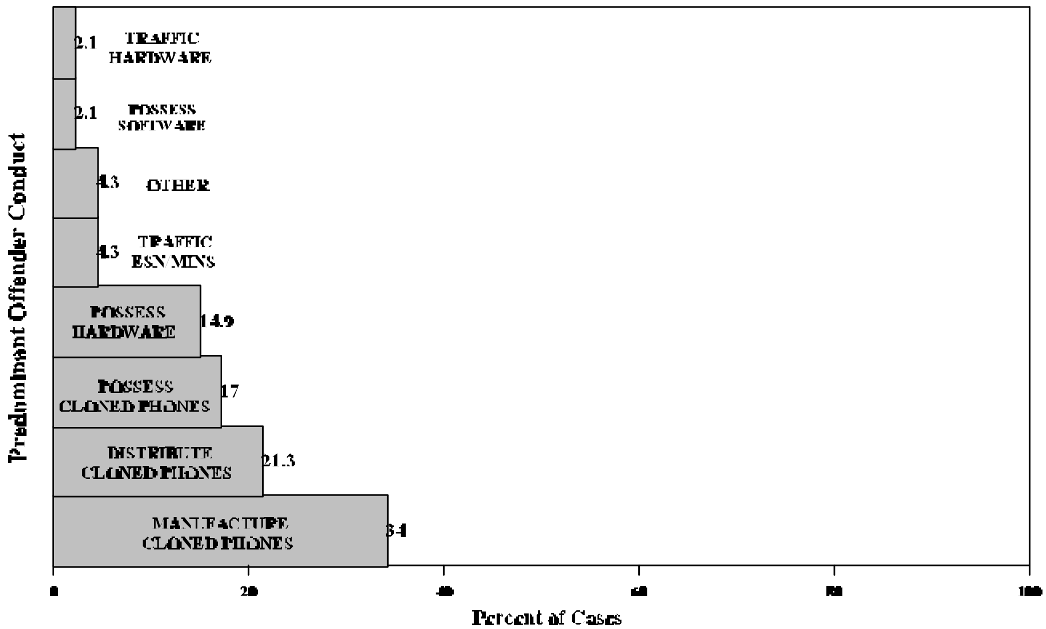
[23] Credit cards are the most commonly used access devices, accounting for the overwhelming majority of the sample of 394 cases. A small minority of the access devices were government benefits cards.

[24] The sample includes all FY98 cases convicted under subsections (6) and (7) of 18 U.S.C. § 1029 which deal with telecommunications specifically.

The range of conduct associated with cellular offenses varies from simple possession of a cloned handset to manufacturing and distributing cloned phones. To determine the relative frequency of the types of cellular fraud involved in these 47 cases, the Team determined the predominant function of the 47 offenders based on the offense described in the PSRs. Predominant function indicates the single behavior that best describes the offender's conduct. Overall, the most predominant function was the manufacture (cloning) of cellular phones (34%), followed by the distribution of cloned phones (21%) and possession of cloned phones only (17%). Other predominant functions are shown in Figure 1.

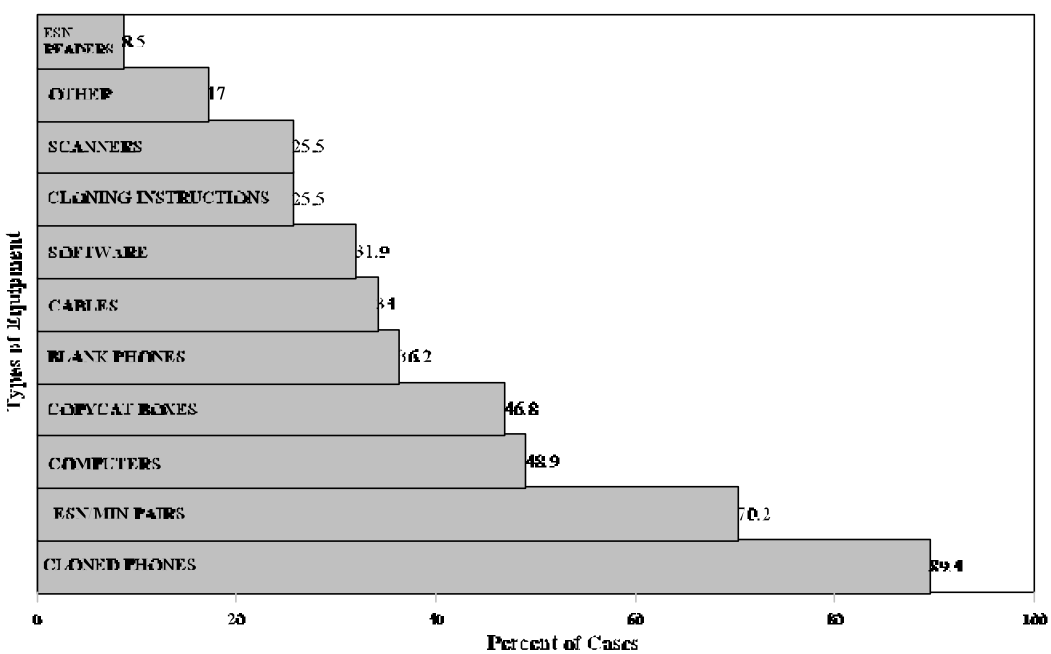
Consistent with the finding that manufacturing is the predominant function of offenders in these cases, approximately half of the cases involved equipment used to clone phones: copycat boxes, computers, and/or ESN/MIN pairs. Twenty-two cases (46.8%) involved copycat boxes, one of the types of equipment with no legitimate uses which the WTPA eliminated the need for proof of intent to defraud. The other type of cloning equipment addressed in the amendment, specialized computer software, was present in 32 percent of the cases. In contrast, a relative minority involved ESN readers and scanners (8.5% and 25.5%, respectively), the equipment necessary to capture the ESN/MIN pairs. Figure 2 displays the distribution of the types of equipment present in the sample.

Figure 1
Predominant Conduct of Cellular Fraud Offenders



Predominant conduct was determined after analysis of the description of each offender's offense conduct, as reported in the PSR. Analysis determined which conduct was most frequently engaged in by each offender.

Figure 2
Types of Equipment Involved in Cellular Fraud



This figure represents the number of cases that involved each type of equipment. Note that many cases involve different types of equipment so that the "percent of cases" sum to more than 100%. The "other" category includes items such as cell locator rings, cell phone batteries, and fraudulent cellular numbers (i.e. made-up).

There was no evidence in the offense conduct sections of the PSRs that large numbers of co-participants were directly involved in these offenses. Most PSRs named only one co-participant, if any, and the largest number of co-participants named in the cellular fraud was five. The entire scope of the cellular fraud offenses was often difficult to determine although some were described as "large scale cloning operations" (*e.g.* the conspiracy had obviously produced and distributed hundreds of cloned phones but they were not traceable or provable for sentencing).

About half (21) of the cases in the sample involved other criminal conduct by the offender or co-participants; thus one of Congress' primary concerns appears to be well founded. However, there were no specific statements in the PSR clearly indicating that the cloned cellular phones were used to further other illicit conduct. For about half of the 21 cases (9), simple *possession* of cloned cellular phones was incidental to the primary offense conduct. For example, one offender was involved in an extensive credit card fraud scheme and a search revealed his possession of a cloned cellular phone. Despite the lack of discussion in the PSR regarding use of that phone, it is reasonable to infer that it was used in conjunction with the credit card fraud. The remaining 12 cases involved the *manufacture and distribution* of cloned cellular phones was the most serious phone cloning conduct that occurred and was in addition to the drug trafficking, credit card and/or check fraud, or counterfeiting that characterized the predominant offense conduct. For example, while one defendant was under surveillance for his participation in a counterfeit currency scheme, he cloned two phones for a co-participant. Table 1 shows the distribution of the primary sentencing guidelines applied for the entire sample of cellular fraud cases. The use of guidelines other than §2F1.1 reflects some of the other types of conduct.

B. Existing Sentences for Cloning Offenses

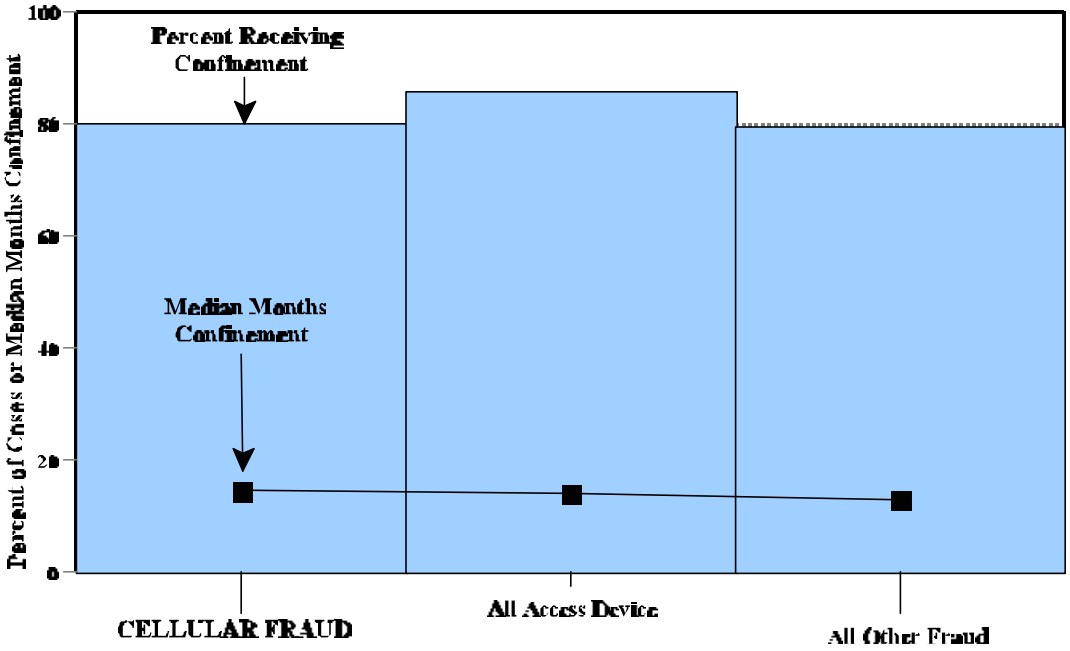
Figure 3 compares the types of confinement rates and lengths for cloning and other offenders. The majority of the cloning offenders (80%) received prison or other confinement sentences with a median length of 15 months.[25] These sentences are comparable to those for similar offenses such as all access device fraud (86% confinement, median 14 months) and all other fraud (80% confinement, median 14 months).

[25] The median represents the midpoint so that half of the cases received sentences shorter than 15 months and the other half received sentences longer than 15 months.

Table 1
Primary Sentencing Guidelines for Cellular Fraud Cases

Primary Sentencing Guideline	Number of Cases	Percent of Cases
Counterfeiting §2B5.1	1	2.1
Drug Trafficking §2D1.1	4	8.5
Racketeering §2E1.1	1	2.1
Fraud §2F1.1	38	80.9
Firearms §2K2.1	1	2.1
Missing Information	1	2.1
Total	47	100.0

Figure 3
Sentencing Outcomes for Cellular, Access Device, and Fraud Cases



C. Loss as an Adequate Measure for Determining Penalties

1. Determination of Loss in the Guidelines

Cellular cloning cases are generally sentenced using the fraud guideline, §2F1.1. That guideline specifies that the loss amount used for sentencing is the actual value of the property, goods, or services taken. In cases in which the intended loss can be determined and is greater than the actual loss, that figure is used instead.[26] For cellular cloning cases, actual loss is generally the amount of fraudulent billing for each cloned ESN/MIN pair. Because the commentary to §2F1.1 indicates that loss need not be determined with precision, the actual loss or average actual loss per ESN/MIN pair (or average loss per victim cellular carrier) would seem sufficient to determine actual loss. Intended loss, the amount that the defendant was attempting to inflict, would technically include the anticipated loss to cloned, but unbilled, ESN/MIN pairs, in addition to those billed.

2. Determination of Loss in Practice

The case review revealed inconsistent approaches to the determination of intended loss, specifically as to how this anticipated loss to unbilled pairs is determined, and whether unbilled pairs are considered at all. The data collected by the Commission, as well as federal appellate decisions, demonstrate these variations in the determination of intended loss in cellular fraud cases.

Actual billing losses are obtained from the cellular carriers who gather this information from the legitimate users' billing records. Although billing records make it relatively simple to verify whether an account has been misused, attributing the loss to a single offender can be problematic. Because of the means by which ESN/MIN pairs are stolen (*i.e.* scanning radio frequencies), a single pair could be purloined by more than one person. Additionally, single number pairs can be widely distributed to and used by a number of persons.[27] Therefore, absent additional proof, the court cannot know with certainty that the billed amounts are solely the result of the defendant's criminal conduct.

In many of the cases reviewed by the team little detail was provided as to how loss was calculated; however, in those cases with complete loss information, actual loss billed to the stolen

---

[26] §2F1.1, comment. (n.8).

[27] The Eleventh Circuit, in two cases, has required a greater level of proof for losses in cellular fraud cases. The Court remanded both *United States v. Sepulveda* and *United States v. Cabrera* for resentencing because of the uncertainty that the defendants were the only individuals to unlawfully use the ESN/MINs that they possessed (*i.e.*, multiple users can access the same ESN/MINs and pairs can be provided to multiple users). *United States v. Sepulveda*, 115 F.3d 882 (11th Cir. 1997), and *United States v. Cabrera*, 172 F.3d 1287 (11th Cir. 1999).

ESN/MIN pairs was most typically used.[28] In about half (25) of the 47 cases in the sample the loss calculation included cellular phone cloning conduct alone (*i.e.* there were no losses due to other types of fraud). Of these 25 cases, 19 used the actual loss due to billing.[29]

When a large number of ESN/MIN pairs are used, and obtaining actual loss figures for each pair is burdensome, it may be more practical for the court to use an estimate based on a sample of the used pairs. When large numbers of ESN/MIN pairs are involved, loss is estimated by using an average loss of the random sample of billed numbers, multiplied by the total number of ESN/MINs used.[30] This was the calculation method for three of the cases in the sample.

When stolen ESN/MIN pairs have been identified, but not used, correct guideline application (*i.e.* the greater of actual or intended loss) would require that the court determine the intended loss. The team found that the use of intended loss is problematic for two reasons. First, unused numbers are sometimes disregarded in the loss calculation, and intended loss is not calculated.[31] This can lead to disparate results in sentences of these cloning offenders relative to offenders who are sentenced based on intended loss determined using the unbilled numbers. However, ensuring that intended loss is determined in all cases with identified, but not used, ESN/MIN pairs will not, in itself, reduce the disparity. This is because of the second problem that arises with the calculation of intended loss based upon unbilled numbers. That is, currently neither the case law nor the guidelines provide a standard method for estimating loss in these cases. Specifically, there is no value or calculation method provided for unbilled numbers.[32] As a result, the courts have adopted a variety of methods that, not surprisingly, can also lead to disparate results.[33]

---

[28] The Eighth and Ninth Circuits have affirmed calculations of loss based upon the sum of the loss amounts reported by cell phone companies. *See United States v. Clayton*, 108 F.3d 1114, 1118-19 (9th Cir.), *cert denied*, 118 S. Ct. 233 (1997).

[29] The remaining six cases determined average loss amounts based on samples of used pairs (3), or other presumptive values of the handsets or service (3).

[30] The Ninth Circuit upheld this method of estimating loss based on the average loss from a portion of the ESN/MIN pairs seized multiplied by the total number of seized pairs. See *United States v. Watson*, 118 F.3d 1315, 1317 (9th Cir. 1997).

[31] In some cases, the failure to include unbilled accounts in the determination of loss may be because there was insufficient information 1) to prove that the defendant intended to use the unbilled accounts, 2) to determine the exact intended amount, or 3) to determine whether the intended amount was greater than the actual amount.

[32] By contrast, offenses involving credit cards are governed by a provision providing a minimum loss of $100 per credit card. §2B1.1, comment. (n. 4). The Treasury department has proposed that the designation be expanded to access devices in general and the minimum amount be increased to $1,000.

[33] The Sixth Circuit affirmed the determination of loss based on the average air time consumption of a cell phone customer in Chattanooga, Tennessee, where the offense occurred. The Court multiplied the number of cloned phones that had been seized by the average annual cell phone bill of cell phone customer. *See United*

Despite the fact that so few cases in the cellular fraud sample provided complete information on loss calculations and numbers of ESN/MIN pairs, the few useful cases demonstrate a range of approaches. Fifteen of the cellular fraud cases report enough information to analyze the use of unbilled numbers in loss calculations. The number of ESN/MIN pairs seized in these cases ranged from one to 4,005 (median = 15). The number of fraudulently billed ESN/MINs pairs ranged from one to 940 (median = 13). On average, 40 percent of the ESN/MIN pairs for these cases were unbilled.[34] This variation is meaningful because of the varied calculation methods used. For example, one of these cases involved the seizure of 4,005 ESN/MIN pairs, 940 of which had been used and billed. The loss calculation for this case consisted of the amount billed for those 940 numbers. In contrast, another case involved 915 seized ESN/MIN pairs, 396 of which had been used and billed. The loss calculation for this case began with a random sample of the 396 used ESN/MIN pairs to determine an average loss per number. This average loss ($301) was then applied to the entire group of 915 seized ESN/MIN pairs.

D. Sentencing Enhancements and Departures

In response to the Congressional directive, the Team reviewed the extent to which sentencing enhancements in the 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. In §2F1.1, there are several specific offense characteristics that may apply in cloning offenses. First, the enhancement applies if the offense involved more than $2,000 of loss. This adjustment ranges from one level (for losses of $2,000 to $5,000) to 18 levels (for losses greater than $80,000,000). Thirty-two of the 38 cloning cases (84.2%) sentenced under §2F1.1 received an enhancement for loss. The greatest loss increase applied in the cases reviewed was 11 levels for a loss between $800,001 and $1,500,000. The median increase for loss was a five-level increase for a loss between $40,001 and $70,000.

An additional two levels may be added under §2F1.1(b)(2) if the offense involved more than minimal planning,[35] or a scheme to defraud more than one victim.[36] Alternatively, where the

---

States v. Ashe, 47 F.3d 770 (6th Cir.), *cert. denied*, 516 U.S. 859 (1995). The Seventh Circuit affirmed that the estimate of $1,000 loss per cloned phone to cellular phone providers made by the Cellular Telephone Industry Association was reliable and multiplied that figure by the number of ESN/MIN pairs seized. *See United States v. O'Shield*, 1998 U.S. App. Lexis 4169 (7th Cir. March 6, 1998) (unpublished).

[34] This is likely a low estimate, due to the problem of missing information in the data. Although specific numbers were often not provided, a number of PSRs described hundreds or thousands of ESN/MIN pairs on paper or stored on computers. In these cases not only were there too many ESN/MIN pairs to count, it remained undetermined how many may have been billed.

[35] More than minimal planning is defined as ". . . more planning than is typical for commission of the offense in a simple form. "More than minimal planning" "also exists if significant affirmative steps were taken to conceal the offense . . . . More than minimal planning is deemed present in any case involving repeated acts over a period of time, unless it is clear that each instance was purely opportune." *See* USSG §1B1.1, comment (n. 1(f)).

[36] §2F1.1(b)(2)(B).

offense conduct or concealment of the offense was "especially complex or especially intricate" a two-level, "sophisticated means" enhancement under §2F1.1(b)(5)(C) may be applied in lieu of the enhancement at §2F1.1(b)(2). In the cases reviewed 35 (92.1%) cases received an enhancement for more than minimal planning. The "sophisticated means" enhancement did not go into effect until November 1, 1998; therefore, none of the cases reviewed was eligible for this enhancement. Finally, a two-level increase applies if the offense involved the possession of a dangerous weapon (including a firearm) in connection with the offense. None of the cases reviewed received this enhancement.[37]

If the Commission assumes the most egregious cloning offense is one in which all of the relevant specific offense characteristics apply (*e.g.*, the offense involves a loss of more than $80,000,000 (the top of the loss table), more than minimal planning, and possession of a dangerous weapon, a firearm), the resulting Chapter Two offense level, level 28, would be sufficient to sentence the defendant near the statutory maximum of ten years. An offense level of 28 corresponds to a sentencing range of 78-97 months for a defendant with little or no criminal history. A defendant with a more substantial criminal history could receive a sentence at the ten-year statutory maximum and closer to the 15-year statutory maximum. Likewise, a defendant whose conduct qualified him for a Chapter Three enhancement (obstruction of justice, use of a position of trust/special skill to significantly facilitate the offense or aggravating role in the offense[38]) could also receive a higher sentence.

However, the findings from the 47 cases do not indicate that such a severe case is typical of cellular phone cloning cases. The highest offense level among cloning cases sentenced under the fraud guideline was 18 (including a 3-level reduction for acceptance of responsibility). The loss in this case, $850,987, made a significant contribution to the sentence with an 11-level increase from the loss table. Other enhancements included more than minimal planning (+2) and obstruction of justice (+2) (§3C1.1). At criminal history category I, this offender was sentenced to 33 months prison, the top of the applicable range. In sum, Commission data does not indicate that existing cellular cloning cases incorporate the elements necessary to reach the statutory maximum penalties.

In addition to the grounds for departure listed in Chapter Five, §2F1.1 also indicates that an upward departure may be warranted in cases in which the loss determined under subsection (b)(1) does not fully capture the harmfulness and seriousness of the conduct. Figure 4 shows the departure rates for the 38 cellular fraud offenders sentenced under §2F1.1. The majority (72%) are sentenced within the applicable guideline range. This is slightly higher than the national rate (for all cases sentenced in FY98) of 67.9 percent. Only one of the 38 cloning cases sentenced under §2F1.1 received an upward departure. However, in that case the departure was based on the inadequacy of the defendant's criminal history category in reflecting the actual seriousness of prior conduct, an issue unrelated to the cloning offense conduct. Approximately 24 percent of all

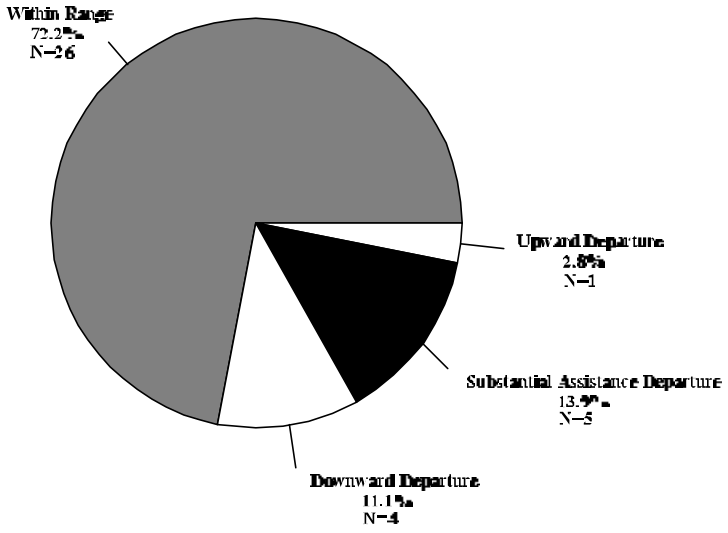
---

[37] §2F1.1(b)(6).

[38] §§3C1.1, 3B1.3, 3B1.1.

cloning cases receive downward departures. Reasons cited for these departures included substantial assistance, family responsibilities, and overstatement of criminal history category.

Figure 4
DEPARTURE RATES FOR CELLULAR FRAUD OFFENDERS SENTENCED UNDER §2F1.1



SOURCE: U.S. Sentencing Commission, 1996 Datafile, USSCFY96.
Of the 38 cellular fraud cases sentenced under §2F1.1, 36 have complete guideline and departure information and are included in this chart.

E. Cloning Sentences in relation to Statutory Maximums

Sentences for cloning offenses have not been constrained by statutory maximum penalties. Depending upon the conduct involved, the statutory maximum penalty in cloning offenses is ten or 15 years. The highest final offense level found in the 47 cases reviewed was level 18. This corresponds to a guideline range of 27-33 months, far short of the statutory maximum. The median imprisonment sentence for these 47 cellular cloning cases is 15 months. Likewise, it appears that the current offense levels leave adequate room for upward departure in these cases.

F. Achieving the Purposes of Sentencing

The WTPA also directs the Commission to review the extent to which Federal sentencing guidelines for the offense adequately achieve the purposes of sentencing set forth in 18 U.S.C. § 3553(a)(2). This section requires

> "the court, in determining the particular sentence to be imposed, shall consider–
> (2) the need for the sentence imposed to--
>
> (A) reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
>
> (B) afford adequate deterrence to criminal conduct;
>
> (C) protect the public from further crimes of the defendant; and
>
> (D) provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner; . . . ."

The Team has several concerns as to whether the current guideline adequately addresses the most serious cloning offenses and provides adequate punishment. Significantly, the guideline punishes mere possessors of cloned phones similarly to manufacturers, especially in cases where the manufacturers have low loss amounts. Because manufacturers and distributors are arguably more culpable than mere possessors, it is possible that without an enhancement for this conduct, the guideline is not adequately punishing important and identifiable cloning conduct. Another significant concern is that the determination of loss appears to be calculated in an inconsistent manner which could cause disparity among similar defendants.

G. Offenses of Comparable Seriousness

Congress directed the Commission to consider the relationship of the guidelines for cellular phone cloning offenses to offenses of comparable seriousness. To address this issue, the Team compared loss calculations for cloning and credit card cases. In general, the data shows that both types of cases involve inconsistent use of unbilled numbers for calculating loss. However, the two groups of cases differ in that cloning cases involve a larger number of access devices and a larger proportion of unbilled numbers compared to credit card cases.

Credit card fraud comprises the majority of the nearly 800 section 1029 cases sentenced in FY98. In its attempt to review offenses of comparable seriousness, the Team reviewed a sample of 228 credit card cases, the most frequently occurring type of access device case. This sample is sufficiently large to provide information regarding the number of credit cards involved, the number of billed and unbilled accounts, the amount of dollars charged and the use of billed and unbilled accounts in loss calculations. Credit cards, are also interesting for comparison because the issue of determining intended loss for unused credit cards is similar to the unbilled ESN/MIN pair issue in cloning offenses.

The review of credit card cases indicated some interesting and useful differences and similarities between these two types of access device frauds. The most significant similarity is the determination of loss in both types of offenses includes unbilled, or unused accounts, and the use of the unbilled accounts in the determination of loss is inconsistent in both offenses.[39] Of the 31 credit card cases known to involve unbilled accounts, only seven (23%) used the unbilled accounts in the loss calculation. And, as in cloning cases, different methods of determining the intended loss for the unbilled accounts were used: $100 minimum as provided in §2B1.1 (2 cases), expected charges based upon charges to cards used in the offense (2 cases) ($2,000), and attempted but incomplete transactions (3 cases) (approximately $8,000 each).

Cloning cases differ from credit card cases in that the median number (7) of credit cards or account numbers seized is lower than for ESN/MIN pairs (15). And, although the number of credit cards involved in these offenses ranged from one to 1,000, the typical case involves a single card or account number. This may be due to the difference in the way in which the two types of access devices are obtained. Scanning devices used to obtain ESN/MIN pairs have the capacity to collect hundreds of numbers at a time and computers can be used to quickly reprogram cellular phones. Therefore, those involved in the manufacturing or distribution of stolen ESN/MIN pairs will conceivably be caught with more numbers. The data indicates that credit cards are not typically stolen in such large volume.

Another somewhat related difference is the prevalence of unbilled numbers in these two types of offenses. The presence of unbilled numbers is much lower for credit cards than for ESN/MIN pairs. The typical credit card cases involves use of all of the illegally obtained

---

[39] Because many of the cases provided insufficient data, it is possible that the unbilled numbers were not used because it could not be proven by a preponderance of the evidence that the defendant intended to use them.

accounts. The proportion of unbilled credit cards in the sample was only 13 percent, compared to 40 percent in the cellular fraud sample. Again, this may be related to the way in which these access devices are obtained. The scanning device will collect multiple numbers, regardless of the number the defendant actually intends to use. Credit cards, which are typically not collected in volume, are more likely to be used when obtained.

In an attempt to estimate average losses for each type of access device, the Commission's data was supplemented by data from other sources. Table 2 uses this compilation of data to compare the average loss per access device for these two types of offenses. The Commission's data was insufficient to determine an average loss per cloned phone, however the average credit card loss per card is $3,775. According to the U.S. Treasury, credit card industry data indicates the average fraud loss in 1998 to be $1,040 per credit card.[40] Treasury also cited 1999 Secret Service statistics indicating an average fraud loss per credit card of $2,218 and cloned cellular telephone of $1,606. The Cellular Telecommunications Industry Association average loss per ESN/MIN pair for 1996-98 is $760.

Figure 5 shows the comparison of loss amounts for cloning, all access device, and all other fraud cases.[41] This figure demonstrates a generally similar trend in loss distribution for the three groups of cases, with the majority clustered at or below the $200,000-350,000 range .

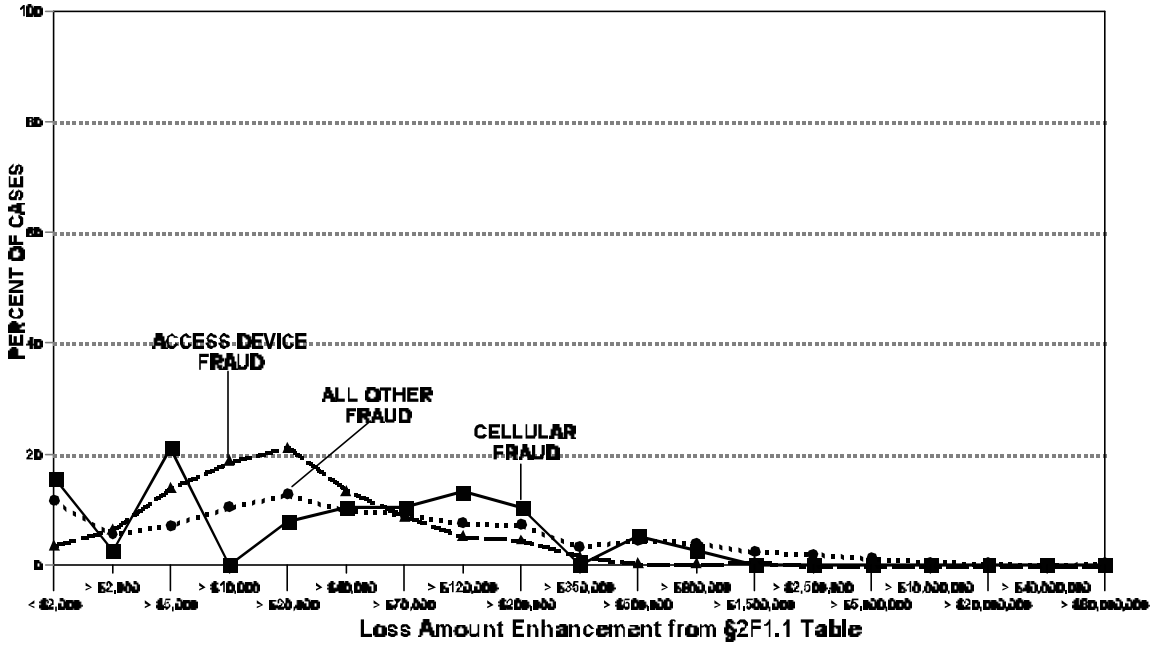
[40] There are a number of reasons that the Commission data produced a greater average amount. The sources of the figures provided by both Treasury and the Secret Service are unknown to the Team. However, it is almost certain that they include both state and federal cases, and may include unprosecuted cases. The figure computed by the Team is based on a sample of 109 federally sentenced credit card fraud cases for which the exact number of credit cards and exact amount of charges were known. A number of agencies have indicated that U.S. Attorney offices have varying dollar amount thresholds for accepting fraud cases for prosecution. Thus, the Commission's figure is likely higher due to the smaller, more selective sample from which the cases were drawn.

[41] "[A]ll access device cases" is defined as all cases with a conviction of 18 U.S.C. § 1029. "[A]ll other frauds" is all other cases sentenced under §2F1.1 excluding 18 U.S.C. § 1029 convictions.

Table 2
Comparison of Average Loss in Credit Cards and Cloning

Agency	Average Loss per Credit Card	Average Loss per Cloned Phone
USSC	$3775	Unavailable
Treasury	$1040	N/A
Secret Service	$2218	$1606
CTIA	N/A	$760

Figure 5
COMPARISON OF LOSS AMOUNT DISTRIBUTIONS
FOR CELLULAR FRAUD, ACCESS DEVICES, AND ALL OTHER FRAUDS



SOURCE: U.S. Sentencing Commission, 1995 Database, USSCFY95.
Of the 47 cellular fraud cases, 38 were sentenced under §2F1.1 and have complete guideline information. Of the 785 cases convicted of access device fraud (18 U.S.C. §1029), 656 were sentenced under §2F1.1, contained complete guideline information, and were included in the cellular fraud sample. Of the 5,363 fraud cases sentenced under §2F1.1, 5,156 have complete guideline information and do not have a conviction for access device fraud.

H. Other Factors

1. Criminal History

The majority (60%) of the 47 cellular fraud offenders were assigned Criminal History Category I by the sentencing court. Table 3 displays the distribution of Criminal History Category for the entire sample of cellular fraud offenders. The most common prior convictions were for larceny, fraud, and drug offenses. Four offenders had a prior conviction for cellular fraud. The prior convictions for two of these offenders were federal convictions under 18 U.S.C. § 1029. However, the PSRs for both of these cases indicated that the prior convictions were "related to the current offense conduct" and were not included in the determination of their criminal history categories.

Table 3
Criminal History Category Distribution
for Cellular Fraud Sample

Criminal History Category	Number	Percent
Total	47	100.0
I	28	59.6
II	6	12.8
III	6	12.8
IV	4	8.5
V	1	2.1
VI	2	4.3

2. Data from outside sources

a. Cellular Telecommunications Industry Association (CTIA)

In an effort to supplement the data collected from Commission case files, the Team solicited information from other agencies. The additional data indicate that a large proportion of cellular cloning convictions occur in state and local courts and that the number of cases has risen in recent years.

The Cellular Telecommunications Industry Association (CTIA) is an international organization which represents all elements of wireless communications - cellular, personal communications services, enhanced specialized mobile radio, and mobile satellite services and serves the interests of service providers, manufacturers, and others. CTIA acts as a representative

of its members in communications with the Executive Branch, the Federal Communications Commission, and Congress. In addition, CTIA runs an extensive anti-fraud program involving detection, prevention, investigation, and research. CTIA also is the parent of CIBERNET Corp., a subsidiary that administers the billing and financial accounting systems used by the industry to facilitate cellular roaming across the nation.

CTIA collected data on 137 cloning cases from 1996-1998. The data submitted contain the following information: number of ESN/MIN pairs stolen, number of ESN/MIN pairs fraudulently used, number of cellular carriers affected, total loss amount, and the jurisdiction of the investigative agency at the time of submission to CTIA.

The 137 cases represent only those investigations of cellular phone fraud for which the assistance of CTIA has been enlisted to determine the losses to the cellular carriers. Note that CTIA does not necessarily receive information on all cloning cases that are investigated. In addition, although the jurisdiction of the requesting investigator may be known at the time of the initial request, there is no way to know if a particular case was prosecuted at the same level, or at all. Given these caveats, the CTIA data is summarized in Table 4. The cases that CTIA receives from federal investigators have significantly larger numbers of fraudulently used ESN/MIN pairs and higher loss amounts. The average loss per pair is similar for each jurisdiction.

Table 4
Summary of CTIA Data

	Total Cases	Average ESNs Stolen	Average ESNs Used	Average Loss Amount	Loss Amt Amount per Used ESN
Total	137	894	155	$117,786	$759.91
Federal	89	1248	208	$162,413	$780.83
State/Local	44	240	58	$37,104	$639.72
Carrier	4	220	42	$23,510	$559.76

b. U.S. Secret Service

The Team has received and begun to analyze additional data from the U.S. Secret Service for offenders convicted of wireless fraud between FY 93 and FY 98. Although the analysis is ongoing, some preliminary findings can be reported. First, the data indicate that the number of convicted cellular fraud offenders has increased since 1993. Furthermore, with this increase in overall caseload, the proportion of offenders adjudicated at the federal level has declined. Further analysis will provide information about the distribution of cellular fraud cases across judicial districts.

VI. Policy Considerations

The WTPA directs the Commission to ". . . 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. . . ." Congress also directed the Commission to consider eight specific factors in this review. As a result of the Team's review, two concerns emerged with regard to whether the current guideline for cloning offenses (§2F1.1 (Fraud)) provides appropriate penalties:

> (1) the current guidelines may not be adequate to address the range of conduct covered by cloning offenses; and,
>
> (2) the determination of loss in cloning cases is not being accomplished in a consistent manner.

This section provides options for addressing both issues but each issue could be addressed separately by the Commission. Because the selection of cases reviewed was limited to 18 U.S.C. § 1029, the full range of conduct in cloning cases may not be represented. For example, the case review failed to identify cases involving large cloning organizations with multiple defendants or those involving drug trafficking. The Team expects that such cases involving other serious conduct may not have convictions under section 1029. However, the absence of these cases among section 1029 convictions suggests that to the extent that more serious offense conduct may be present, it likely overshadows cellular phone cloning in charging, convictions, and sentencing.

The review of a large proportion of cases convicted under section 1029 provided reliable information and yielded several interesting findings. First, the majority of defendants convicted of cloning offenses are manufacturers or distributors of cloned phones. Second, although there is some indication from the sample of cloning cases that cloning behavior occurs with other illegal behavior, the Team could not determine how often such conduct was facilitated by the use of cloned phones. Furthermore, the analysis could not indicate how often un-convicted cloning conduct cooccurs with other conduct. In order to make an accurate assessment, a sample of all offense types would need to be reviewed. Third, the determination of loss in cloning offenses is problematic because it appears that loss is not calculated consistently. Consequently, it is possible that disparate sentences are being imposed on similar cloning offenders.

A. The Range of Conduct Covered by the Offenses

1. Manufacturers and Distributors

It is clear from the WTPA that Congress and law enforcement officials are concerned about manufacturers and distributors of cloned phones. The amendment to section 1029 targets offenders who use or possess specific equipment used to capture ESN/MIN pairs and hardware and software used to clone phones. The Wireless Telephone Protection Act, Pub. L. 105-418, included a directive to the Commission to "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. . . ." In November, 1998 the Commission invited public comment on "whether and how [the Commission] should amend the guidelines" for offenses involving cloning of wireless telephones. The Treasury Department recommended that the Commission consider amending the guidelines to provide an increased offense level if the offense involved the use or possession of device-making equipment, including cloning equipment. The Commission's data indicates that manufacturers and distributers are the most common defendants convicted under section 1029. Likewise, the equipment Congress addressed in the amendment to section 1029 (software, copycat boxes) is frequently present in these cases.

Section 1029 covers a range of cloning behavior from mere possession of a cloned phone to using, producing, or trafficking in cloning equipment. The statutory maximum for these offenses is ten or 15 years depending upon the conduct, and are sentenced under §2F1.1. This guideline provides different punishment levels based on the amount of loss, planning or sophistication involved. It is arguable that the current guideline distinctions, however are not adequate to provide appropriate penalties for cloning offenses. Because offenders who manufacture and/or distribute cloned phones or equipment are more culpable, it is arguable that this conduct warrants a specific offense characteristic. Additionally, it is debatable that without a separate enhancement for manufacturing or distributing, the current fraud guideline does not adequately distinguish between possessing a cloned phone and the more serious conduct of manufacturing or distributing.

a. Option 1: Add a Specific Offense Characteristic for Manufacturing or Distributing

This amendment distinguishes between types of cloning offenders and enhances sentences in response to the congressional amendment. This is accomplished by creating a specific offense characteristic to cover the actual offense conduct of manufacturing or distributing, or to cover conduct involving the specific equipment prohibited by the statute.

b. Option 2: Provide a Presumptive Loss Value for Offenses Involving Manufacturing

An alternative approach adds a presumptive loss amount where manufacturing equipment is involved. This would alleviate the need for a specific offense characteristic while still ensuring that the sentence reflects

the increased seriousness of the use of manufacturing equipment. However, this presumably only applies in cases where the actual loss is less than the presumptive loss. In cases where the actual loss exceeds the presumptive loss, defendants using manufacturing equipment do not receive any additional punishment. Consequently, defendants with less loss could receive greater enhancements than those who actually caused more loss.

2. Additional Criminal Conduct

The use of a cloned phone to commit other crimes is one of the top concerns expressed by Congress, the Treasury Department and the Secret Service. In fact, the Department recommended that the Commission amend §2F1.1 to "provide an enhancement for offenses in which fraudulently-obtained telecommunications services are used to commit other crimes."[42]

The Team attempted to assess the use of cloned phones in other criminal conduct. However, this effort was somewhat hampered because the case review was limited to cases involving a section 1029 conviction. In other words, only cases known to involve a cloned phone (because of the section1029 conviction) were reviewed to assess the existence of additional criminal conduct. In order to accurately assess how widespread the use of cloned phones is in other offenses, the Team would have to sample cases from offense types to determine if there was a cloned phone involved. In the sample of cloning cases, there were few cases involving other criminal conduct and no cases in which a clear connection existed between the use of the phone and the commission of the other offenses. The Commission may choose to study this issue further and postpone amendment action on this specific issue until sufficient data is available. However, if through further analysis the Team were to find that cloned phones are being used to commit additional criminal conduct, several policy questions exist:

1) Is an offense committed with the use of a cloned phone more serious than one committed without the use of a cloned phone; and

2) Does the use of a cloned phone—and its accompanying anonymity—in and of itself warrant an increase in the sentence?

If and when the Commission chooses to address the issue, several options are available. The first option adds an enhancement to §2F1.1, and/or other designated guidelines, (similar to §2K2.1(b)(5))[43] that increases sentences for the use or transfer of a cloned phone in connection with another offense. The second option adds a cross-reference to §2F1.1 that punishes offenders

---

[42] Letter dated November 17, 1998, from Treasury Department Under Secretary (Enforcement) James E. Johnson to Sentencing Commission General Counsel John R. Steer.

[43] Section 2K2.1(b)(5) adds a 4 level enhancement in the firearm trafficking guideline if the defendant "used or possessed any firearm . . . in connection with another felony offense; or possessed or transferred any firearm or ammunition with knowledge, intent, or reason to believe that it would be used or possessed in connection with another felony offense".

possessing cloned phones at the level for the offense with which the phone was used. This option could be implemented by itself, or in combination with the first option. The disadvantage to this second option is that these cross-references could result in the "tail wagging the dog" situation. In other words, a defendant could be convicted of a less serious offense and have his/her sentence increased considerably based on behavior that was proven by a preponderance standard when the more serious behavior could have been (or should have been charged).

a. Option 1: Add an Enhancement for Use of a Cloned Phone in Connection with Another Crime

At a minimum §2F1.1 could be amended to include an enhancement (similar to §2K2.1(b)(5)) which would increase sentences under §2F1.1 for the use or transfer of a cloned phone in connection of another offense. However, placing this enhancement solely in the fraud guideline would severely limit the number and types of cases in which this enhancement would apply. In order to address a wider range of cases a similar enhancement could be added to other Chapter Two guidelines where the commission felt that the use of a cloned phone was particularly egregious (*e.g.*, crimes of violence or drug distribution). An even broader application of the enhancement could be accomplished by including it as a Chapter Three adjustment so that it could be considered in all cases.

b. Option 2: Add a Cross Reference

The use of a cross-reference in §2F1.1 could be implemented by itself, or in conjunction with Option 1 above. This cross-reference punishes offenders possessing cloned phones at the level for the offense with which the phone was used. However, this only applies for offenses in §2F1.1. In order for it to have broader application to other offenses, the cross-reference would have to be added to the relevant Chapter Two guidelines. Although this would certainly guarantee that this conduct is addressed in various offenses, it raises fairness issues, as described above.

B. Loss as an Adequate Measurement of Seriousness

Congress specifically directed the Commission to examine ". . . 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." The team found that the use of intended loss is problematic for two reasons. First, unused numbers are sometimes disregarded in the loss calculation, and intended loss is not calculated.[44] This can lead to disparate results in sentences of cloning offenders. However, ensuring that intended loss is determined in all cases with identified, but not used, ESN/MIN pairs will not, in itself, reduce the disparity because currently neither the case law nor the guidelines provide a standard method for estimating loss in these cases. Specifically, there is no value or calculation method provided for

[44] In some cases, the failure to included unbilled accounts in the determination of loss may be because there was insufficient information to prove that the defendant intended to use the unbilled accounts.

unbilled numbers. As a result, the courts have adopted a variety of methods that can also lead to disparate results.[45]

Inconsistent loss computations contribute to disparate sentences among cloners and offenders committing crimes of comparable seriousness. Therefore, with regard to Congress's specific directives to the Commission, the inconsistent determination of loss prohibits the current guideline from adequately achieving the purposes of sentencing. In particular, "the need for the sentence imposed to reflect the seriousness of the offense, . . . and to provide just punishment for the offense. . ." is jeopardized when loss is being determined inaccurately.

The Commission has two options for addressing this inconsistency. These options are described in the following paragraphs. The first option is a "minimalist" approach to resolving the issue. It suggests several commentary changes to clarify the determination of loss in cloning cases. The second option, aimed at increasing the consistency in application, involves giving the courts more definitive rules for application.

a. Option 1: Clarifying the Use of ESN/MIN Pairs in the Determination of Loss

The first concern can easily be addressed by modifying the commentary to make clear that unused ESN/MIN pairs are to be used in determining intended loss. This alleviates some of the disparity in sentences for cloning offenders by increasing consistency in the determination of loss. In addition, it increases the ability of the loss enhancement to adequately measure the seriousness of the offense. Currently, without the inclusion of intended loss, the full seriousness of the offense is not being taken into consideration in the sentence imposed. However, this does not address how to determine the value of the unused pairs, and, if current practices prevail, varying methods for determining that value will be used. Therefore, some degree of disparity would remain.

Providing a method for estimating loss in cloning cases would also standardize application, and, consequently, reduce disparity among cloning offenders. Using an average is one possible method. For example, in the case where there are both used and unused ESN/MIN pairs, loss for the unused pairs would be determined by taking of the average amount of loss for a sample of the used pairs multiplied by the number of unused pairs. Likewise, in cases where the number of used pairs is so large that determining actual loss is prohibitive, an estimate of loss could be accomplished by taking an average from a sample of the used pairs and extrapolating for the entire set of used pairs. Although this seems to be workable solution for cases involving used pairs, the courts would still be without guidance in cases where none of the ESN/MIN pairs have been used, therefore there would still be the potential for disparity.

b. Option 2: Provide a Minimum or Presumptive Value for ESN/MIN Pairs

[45] See Note 21.

On November 30, 1998, the Commission invited public comment on "whether and how [the Commission] should amend the guidelines" for offenses involving cloning of wireless telephones. Because the current guidelines provide a "special rule" for credit cards, the Commission requested comment on whether to expand the current rule for credit cards to all access devices, including ESN/MIN pairs. The current rule, provides that loss in credit card cases includes any unauthorized charges made with stolen credit cards, but in no event less than $100.[46]

In 1999, the Treasury Department responded to this proposal and recommended that the $100 minimum loss amount in the current rule be raised to $1,000 per card or access device.[47] In support of this recommendation, Treasury cited credit card industry data that showed the average fraud loss in 1998 to be $1,040.59 per credit card. Treasury also cited 1999 Secret Service statistics indicating an average fraud loss per credit card of $2,218 and cloned cellular telephone of $1,606. The Commission's data was insufficient to determine an average loss per cloned phone, however the average credit card loss per card is $3775.[48]

Expanding the current credit card rule to all access devices in and of itself is not problematic but it does not resolve all the disparity problems. Because the current rule only addresses a minimum value, in cases where courts used an amount above the minimum, the varying methods used to estimate the loss could still lead to disparate results.

Increasing the current minimum from a $100 to a $1,000 minimum value may be problematic in another way. For example, in cases where loss for some pairs is determined to be less than $1,000, using a $1,000 per card minimum for other pairs within the same case could be inappropriate.[49] This problem would not likely occur if the current $100 minimum was retained. For those who argue that the $100 amount is too low for access devices, an amount somewhere in between $100 and $1,000 might be less problematic. It is also possible that a different figure is

---

[46] §2B1.1, comment. (n.4).

[47] Letter dated March 26, 1999, from Treasury Department Under Secretary (Enforcement) James E. Johnson to Sentencing Commission Interim Staff Director Timothy B. McGrath.

[48] As stated previously, there are a number of reasons that the Commission data produced a greater average amount. The sources of the figures provided by both Treasury and the Secret Service are unknown to the Team, however, it is almost certain that they include both state and federal cases, and may include unprosecuted cases. The figure computed by the Team is based on a sample of 109 federally sentenced credit card fraud cases for which the exact number of credit cards and exact amount of charges were known. A number of agencies have indicated that U.S. Attorney offices have varying dollar amount thresholds for accepting fraud cases for prosecution. Thus, the Commission's figure is likely higher due to the more selective criteria used to select the cases.

[49] CTIA data indicates industry average loss per cloned phone is closer to $800.

necessary for ESN/MIN pairs and credit cards to adequately reflect the seriousness of each offense.[50]

An alternative to expanding the current minimum rule for credit cards is assigning presumptive values to ESN/MIN pairs and other access devices. A presumptive value would be used in any situation in which the loss is not be reasonably ascertainable, because either the ESN/MIN pairs were not used and the court is determining intended loss, or determining actual loss is difficult. In these situations the "presumptions" would be used unless the government or defense provides sufficient information for a more accurate assessment of the loss. This option differs from the current credit card rule in that it leaves to the court the discretion to determine the loss using actual figures when able to do so, and provides a solid alternative (not just a minimum) in cases where a more accurate assessment can not be made. Much of the disparity in these cases results from the latter, when an accurate assessment cannot be made. In such cases, unused ESN/MIN pairs are ignored, or varying methods are used to determine their value. A presumptive value would alleviate this problem, thereby reducing disparity.

Arriving at an acceptable presumptive value for ESN/MIN pair may be difficult. Currently, the Commission's data is insufficient to establish an average figure. However[16], the Team has requested supplementary data from the U.S. Secret Service. With this supplementary data, and the Commission's own data, the Team will be better equipped to suggest a presumptive value with confidence. Without this supplementary data, the Commission would have to rely on an average derived from industry statistics.

[50] Although Treasury Department and U.S. Secret Service data suggests that for cloning cases loss typically exceeds $1,000 per phone, CTIA industry average data indicates loss is only $760 per phone.