Economic Crimes Policy Team

Cellular Telephone Cloning

EXECUTIVE SUMMARY

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 configured for altering or modifying a telecommunications

[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.

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;

(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. §

---

[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).

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 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.

---

[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).

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

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

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

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 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.

---

[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".

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; 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

---

[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.

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.