March 10, 2000

The Honorable Diana E. Murphy
Chair, U.S. Sentencing Commission
One Columbus Circle, NE
Suite 2-500 South
Washington, D.C. 20002-8002

Dear Judge Murphy:

I write to provide Treasury's comments on two amendment proposals that the U.S. Sentencing Commission recently published in the Federal Register for public comment. The first amendment proposal concerns identity theft and responds to a legislative directive in the Identity Theft and Assumption Deterrence Act of 1998, Pub. L. 105-318. The second proposal also responds to a legislative directive, in the Wireless Telephone Protection Act, Pub. L. 105-172, and directs the Commission to provide an "appropriate" penalty for offenses involving the cloning of wireless telephones.

We believe that stronger penalties are warranted for identity theft and the cloning of wireless telephones. The incidence of both crimes is on the rise. The security of private communications and commercial transactions over the Internet is undermined by criminals who exploit this new technology to steal identities, social security numbers, credit card numbers, and other individual means of identification. In addition, criminals increasingly use cloned cell phones to conceal their identities and avoid detection when conducting drug deals, illegal weapons sales, and other serious crimes. Provided below are our more detailed comments addressing each of the amendment proposals separately.

Identity Theft

Our consideration of the guideline amendment options on Identity Theft are guided by two overriding concerns. First, because the length of sentences under the applicable fraud guideline, USSG §2F1.1, is largely dependent upon the monetary loss amount, the guideline does not adequately account for the significant non-monetary harms suffered by victims of identity theft, including loss of reputation, inconvenience, and destroyed credit standing. Second, §2F1.1 fails to provide greater penalties for identity thieves who produce, transfer, or unlawfully possess multiple means of identification. For instance, an individual who illegally obtains 20 social security numbers matched to named individuals, and then uses them to create false driver's licenses, generally should be punished more severely than someone who illegally possesses a single social security number.

We think that Option 2 in the Sentencing Commission’s proposed amendments addresses these concerns in a simple and direct manner. It provides a two-level increase, and a minimum offense level of either 10 or 12, if "the offense involves harm to an individual's reputation or credit standing, inconvenience related to the correction of records or

restoration of an individual's reputation or credit standing, or similar difficulties." Of the two alternatives for minimum offense level, we favor a floor of 12 because it makes more likely that individuals convicted of identity theft will be sentenced to incarceration.

Additionally, we believe the Application Notes should make clear that even where the stolen means of identification is used to defraud an institution or government agency, a court should consider the non-monetary harm caused to the individual to whom the means of identification rightfully belonged. For example, a court should impose a two-level increase in "tax refund scams" where an identity thief files a false tax return using the name and social security of another, in order to obtain a quick tax refund. Although the real owner of the social security number may not suffer any quantifiable financial loss, he suffers significant harm nonetheless. When he files his own legitimate tax return two months later, he will encounter, at the very least, significant inconvenience and personal embarrassment in trying to sort the matter out with the appropriate tax authority.

Option 2 also provides a two-level increase if "the offense involved the production or transfer of 6 or more identification documents, false identification documents, or means of identification . . . ." We think this provision can be improved in two ways: First, by including "unlawful possession" of 6 or more identification documents as a condition triggering the two-level increase; and second, by providing an additional increase, cumulative to the two-level increase, for cases involving specified numbers of identification documents or means of identification. For example, this latter enhancement could provide an additional one-level increase for offenses involving more that 10 means of identification or identification documents; two levels for more than 25; three levels for more than 50; and four levels for more than 100. We believe that providing explicit increases for multiple means of identification is preferable to the other alternative raised by the Commission, i.e., encouraging courts to depart upward in such cases. Upward departures are rare, even when encouraged by the Guidelines, and they may not lead to equal treatment of like conduct among districts.

Addressing the identity theft amendment proposal in Option 1, we support its intent but are concerned with its application. We fully support a two-level increase for offenses involving "the use of any identifying information of an individual victim to obtain or make any unauthorized identification means of that individual victim." This provision is aimed at punishing conduct in which a victim's identifying information is used to create new documents in the individual’s name, such as credit cards, but the victim remains unaware of the violation until well after his reputation or credit rating is destroyed. The victim is more helpless to protect himself than the average victim of credit card fraud, who generally can protect himself from personal financial loss by closely scrutinizing his monthly bill and notifying his financial institution of unauthorized purchases. This type of fraud deserves greater punishment.

However, while supporting its intent, we are concerned that Option 1, as drafted, may be overly confusing in application. For instance, the new term "unauthorized identification means" is defined as "any identifying information that has been obtained or made from any

other identifying information without the authorization of the individual victim whose identifying information appears on, or as a part of, that unauthorized identification means." This definition is confusing, and we are concerned that courts may have difficulty distinguishing the meaning of this new Guideline term ("unauthorized identification means") from the statutory term "means of identification."

That said, we would support an attempt to work this provision into Option 2 if it could be simplified and clarified. Specifically, it could serve as an alternative basis for applying Option 2's existing two-level increase for harm to an individual's reputation or credit standing. In other words, we suggest that Option 2's two-level increase apply if the offense involved either: (1) harm to an individual's reputation or credit standing, or inconvenience related to the correction of records or restoration of reputation; or (2) the use of an individual's identifying information to create new identification documents or means of identification without the victim's knowledge or permission. We are willing to assist the Commission in determining whether this combination of Option 1 and 2 is workable.

Telephone Cloning

We have two principal concerns with the current guideline applicable to telephone cloning offenses (USSG §2F1.1). First, the guideline's sentence enhancements are overly weighted toward proof of actual financial loss, and therefore do not adequately account for the fact that financial loss is often very difficult to determine in cases involving the use or possession of cloned telephones and cloning equipment. Second, the guideline does not provide sentence enhancements for the use or possession of cloning equipment and other device making equipment.

This latter concern seems to have been shared by the Commission in earlier versions of the Guidelines. Prior to November 1, 1993, Application Note 11 to §2F1.1 encouraged courts to enhance the sentences for "the use or possession of device making equipment . . . in a manner similar to the treatment of analogous counterfeiting offenses under Part B of this Chapter." Counterfeiting offenses involving the possession of counterfeiting devices or manufacturing equipment receive a six-level sentence enhancement, to an adjusted offense level of 15. USSG §2B5.1(b)(2). As of November 1, 1993, however, Application Note 11 was amended to delete any reference to device making equipment. Little or no explanation was given for this significant deletion.[1] We think an important principle was lost.

Of the two options, we feel that Option 2 more fully restores this principle and better addresses our concerns generally. Option 2 provides a two-level enhancement for offenses involving any "device-making equipment," and broadens the statutory definition of device-

[1]The only written explanation for the amendment was the Commission's accompanying statement that it was "clarifying Application Note 11 and conforming the phraseology in this application note to that used elsewhere in the guidelines." USSG App. C, Amendment 482.

making equipment (found in 18 U.S.C. §1029(e)(6)) to include the cloning hardware and software described in 18 U.S.C. §1029(a)(9). We favor the two-level increase over the "presumptive loss amount" alternative because it will guarantee a set increase in offense level across the full range of loss amounts.

Neither Option 1 nor Option 2, however, address our concern that the sentences provided in §2F1.1 are too heavily contingent upon proof of actual financial loss, particularly in regard to offenses involving the use and possession of cloned phones. We therefore urge the Commission to adopt a specific offense characteristic that would assign an alternative minimum loss amount not just for stolen or fraudulent credit cards, see §2B1.1 (minimum loss amount of $100 per credit card), but for cloned phones and certain other access devices (e.g., mobile phone identification numbers) as well.

The current $100 minimum loss amount for credit cards in §2B1.1 is, in our view, simply inadequate. Based on the investigative records and experience of the U.S. Secret Service, the average loss caused by fraudulent credit cards and cloned cellular telephones in most cases exceeds $1,000. We therefore recommend that the Commission provide a minimum loss amount of at least $1,000 per access device. Thus, in fraud cases where the actual loss is difficult to ascertain or is less than $1,000 per credit card or cloned phone, courts would instead assign a minimum loss amount of $1,000 per access device when determining sentence enhancements under the monetary loss table in §2F1.1.

In addition, we encourage the Commission to provide for increased penalties when a cloned wireless telephone is used in connection with other criminal activity. In our view, use of a cloned phone represents a degree of sophistication and additional planning (i.e., to conceal identity) that warrants greater punishment. Thus, we support a two-level enhancement for this type of conduct in §2F1.1.

* * * *

In conclusion, we strongly support changes to the fraud guideline that provide stronger sentences for offenses involving identity theft and the cloning of wireless telephones. Treasury's law enforcement bureaus, in particular the United States Secret Service and IRS Criminal Investigations, give high priority to these crimes and devote substantial resources to their investigation and prosecution. Their efforts will be aided by changes to the Sentencing Guidelines that ensure appropriate penalties for these crimes. We hope that our comments on the individual amendment proposals will aid the Commission in its future deliberations.

Sincerely,

James E. Johnson
Under Secretary for Enforcement

cc: Eric Holder
Deputy Attorney General