Staff Analysis of Proposed Identity Theft and Wireless Telephone Cloning Amendment Options

March 28, 2000

In response to the congressional directive to the Sentencing Commission contained in the "Identity Theft and Assumption Deterrence Act of 1998" ("Identity Theft Act"), the Commission published two proposed Options and six issues for comment in the Federal Register on January 18, 2000. The following analysis of the two published options compares how they differ, particularly with respect to the range of offense conduct that each will punish and the policy implications of the Commission's decisions in this regard. Also included is an analysis of Option Three, which staff presented to the Commission on March 10. Option Three represents an effort to consolidate the interrelated aspects of wireless telephone cloning and identity theft, and to resolve cumbersome drafting issues that have become apparent since Options One and Two were published.

OPTION ONE: IDENTITY THEFT

Policy

The two-level enhancement proposed in Option One is derived from the research conducted by the Commission's staff and reported to the Commission on December 15, 1999. The fundamental observation derived from this research is that identity theft occurs along a continuum. Within this continuum the more aggravated forms of identity theft involve some affirmative activity to generate or "breed" another level of identification means without the knowledge, or ability to know, of the individual victim whose identification means are purloined or misused. This affirmative activity of "breeding" contrasts with the more basic misuse of identification means such as the use of a stolen credit card to purchase merchandise or the forging of a signature to cash a stolen check, conduct that is already punished under existing statutes and guideline provisions.

Structure and Application

Accordingly, the substantial two-level increase in punishment of Option One is based on the assumption that the aggravated conduct of "breeding" identification means of actual individuals will necessarily result in "harm to reputation, inconvenience, and other difficulties" to the individual victims whose identification means are misused. Thus, Option One incorporates into its structure the particular type of harm about which Congress was most concerned in passing the Identity Theft Act. In contrast to Option Two, discussed in detail below, Option One does not require that the government prove the fact and the extent of such harm at the sentencing hearing.

Because it is axiomatic that such harm can only affect actual, as opposed to fictitious, individuals, Option One also makes clear at Application Note 16 that the enhancement will not attach to offense conduct when the misused identification means correspond to fictitious individuals.[1]

Specifically, Option One provides for increased punishment when an individual offender obtains or makes additional identification means about which the "true owner" of the identification means has no control or knowledge and which pass into the exclusive control of the offender and other perpetrators.[2] In anticipation of situations where the government may not be able to establish that the defendant was involved in obtaining or making (*i.e.* "breeding") the new identification means, Option One also provides for the same increase in punishment if the defendant is in possession of five or more such 'bred" identification means or documents.[3]

OPTION TWO: IDENTITY THEFT

Key Distinctions Between Option One and Option Two

Option Two, submitted by the Department of Justice, takes a different approach to increasing punishment for offense conduct involving the misuse of identification means. Option Two differs in five fundamental respects from Option One. First, Option Two does not distinguish among a range of offense conduct along the continuum of identity theft, and does not require that a new level of "bred" identification means be involved for the enhancement to attach.

Second, Option Two can apply to all fraudulent offense conduct, not only to the offense conduct that results from the misuse of identification means. Third, Option Two will apply irrespective of whether the misused identification means corresponds to a fictitious or actual individual. Fourth, a total increase of four levels for offense conduct resulting from the unauthorized use of identification means is possible under the two prongs of Option Two, whereas Option One limits the *direct increase* for such offense conduct to two levels. Finally, one of the two-level increases of Option Two will not attach if there is already an increase under the loss

---

[1] For a textual analysis and discussion of the legislative history of the Identity Theft Act regarding its application to fictitious individuals, see Appendix A.

[2] Option One ensures that this affirmative conduct is necessary for the enhancement to apply by means of the definitional sections in Application Notes 16 and 17.

[3] Fairly typical conspiracies involve the use of "runners" to cash stolen checks by using counterfeit identifications, often obtained or created in the name of the payee on the stolen check with the photograph of the runner. See, for example, Case Nos. 450973 and 456310 in Appendix B. Under Option One, if the "runner" cannot be tied to the offense conduct of breeding the identification means which the runner then uses to cash a stolen check, the runner will not receive an enhancement for his activity. Should the runner be found in possession of five or more such "bred" identification means, however, then the enhancement will apply.

table at §2F1.1(b)(1). Option One, in contrast, will apply its two-level increase for the misuse of identification means *in addition* to the increase that results from the loss table.

Structure and Application

Option Two essentially takes a two-pronged approach. In the first prong, Option Two provides a two-level enhancement whenever there is "more than minimal" 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." Option Two will therefore require the government to prove at the sentencing hearing that there is "more than minimal" harm of this nature, unlike Option One which presumes that such harm has occurred or has been risked in the course of the aggravated offense conduct of "breeding" identification means and documents.

Option Two also has a broader scope than Option One in that it will apply to any fraudulent offense conduct (not just to identity-related offenses) where the government can demonstrate "more than minimal" 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." Accordingly, the enhancement in this first prong of Option Two is not limited to situations where such injury is caused by the misuse of identification means.

The second prong of Option Two increases punishment by two levels whenever the production or transfer of six or more identification documents, false identification documents, or means of identification were involved in the offense conduct, but would not effect such an increase if the defendant is already receiving an increase under the fraud loss table. This second prong of the proposal differs in application from Option One in several notable respects.

First, Option One requires the aggravated offense conduct of "breeding" identification means of another individual for the two-level enhancement to attach while Option Two does not. In contrast, Option Two imposes a two-level enhancement if the offense conduct involves the transfer or production of any six means of identification, *whether false of not*, irrespective of whether these six or more identification means are those *of an individual other than the defendant*, *and* irrespective of whether the means of identification involved in the offense conduct were *unauthorized*. Furthermore, unlike Option One, the misused identification means implicated by Option Two correspond to fictitious as well as actual individuals.

Second, Option Two uses the terms "produce" and "transfer" to describe the offense conduct subject to the two-level enhanced punishment. The term "transfer" is part of the new Identity Theft Act as codified at 18 U.S.C. § 1028(a)(7), but it is not defined in the statute. The term "produce" is not used in the Identity Theft Act as codified at 18 U.S.C. § 1028(a)(7), but it is

defined in § 1028(d)(5) as "alter, authenticate or assemble."[4]

The application of Option Two in light of these definitional issues is unclear. For example, if an eighteen-year old student alters the date of birth on his own driver's license in order to gain entrance into an "adults only" bookstore and somehow becomes involved in offense conduct that is punishable under the fraud guideline, this enhancement could arguably apply. Similarly, if a twenty-two year old friend lends the underage student his entire wallet containing numerous means of identification and events transpire as described above, then the older friend could also arguably be covered by this enhancement, given that "transfer" has been construed by case law to mean "sell, pledge, distribute, give, loan" or otherwise relinquish control.[5]

The third distinction occurs between the fundamental premise of Option One and the second prong of Option Two. Option Two does not provide the two-level increase for the production or transfer of identification means *should an increase already attach under the fraud loss table*. Under Option One, the harm and inconvenience caused to the individual victim is accounted for in the two-level increase by defining the offense conduct as the misuse of identification means through the breeding of documents. Should there also be a monetary loss to a financial institution, the government, or an individual that corresponds to an enhancement under the fraud loss table at §2F1.1(b)(1), the defendant would receive both additional enhancements under Option One.

Finally, under Option Two, a four-level increase may occur whenever a defendant (who does not receive an increase under the fraud loss table) has produced or transferred six or more identification means *and* also caused "more than minimal" inconvenience or harm to an individual's reputation or credit standing, irrespective of whether the offense conduct that resulted in the harm was the result of the production or transfer of the identification means. In contrast, under Option One, there is a maximum increase of two levels for offense conduct involving the

---

[4] A review of recent cases prosecuted under 18 U.S.C. § 1028 prior to its amendment by the Identity Theft Act indicates, however, that the type of conduct associated with charges of "producing false identification documents" is typically conduct that can be described as equivalent to "manufacture, fabricate, or create." *See, e.g.*, United States v. Kuka, 129 F. 3d 1435 (11th Cir. 1997); United States v. Marquez, 48 F. 3d 243 (7th Cir. 1997); United States. v. Goris, 159 F. 3d 1349 (2nd Cir. 1998) (Table) (Unpublished Disposition). Offense conduct in which false identification documents are "shown" to an official or institution more nearly conform to the statutory term of "use." *See* United States v. Chandler, 98 F. 3d 711, 717 (2nd. Cir. 1996). Should the Commission adopt this aspect of Option Two, in order to preclude potential litigation over the guidelines' use of "produce" and "transfer" it might be useful to include clarifying definitions that conform to the case law in this regard.

[5] This definition is taken from jury instructions on the meaning of "intent to transfer" in a case alleging the violation of 18 U.S.C. §1028(a)(3). See United States v. Alejandro, 118 F. 3. 1518 (11th Cir. 1997). See Appendix C for a further discussion of the meaning of the term "transfer" in 18 U.S.C. § 1028.

misuse of identity means but monetary loss is treated as a separate offense characteristic.

OPTION THREE: IDENTITY THEFT

Option Three was developed with four objectives in mind. First, to combine the proposed amendments relating to wireless telephone cloning and identity theft because there is a significant amount of overlap in the statutory definitions of each offense. Second, to broaden the scope of the amendment to include unauthorized access devices such as stolen credit cards and ESN/MIN number pairs in wireless cloned phones. Third, to clarify and streamline the terminology used in connection with the two identity theft options published in the Federal Register on January 18, 2000. Fourth, to consolidate aspects of both published identity theft options, to the extent that they are compatible and consistent with the overall structure of the guidelines.

Consolidation of Wireless Telephone Cloning and Identity Theft Enhancements

Option Three consolidates enhancements for wireless telephone cloning with identity theft into one provision in an effort to minimize the risk of double counting that would otherwise occur because of the overlap in statutory definitions between 18 U.S.C. § 1028, as amended by the Identity Theft and Assumption Deterrence Act of 1998, and 18 U.S.C. § 1029. Specifically, wireless cloned telephones and credit cards are encompassed by the broad definitions of "access device" and "telecommunication identifying information" in 18 U.S.C.§ § 1029(e)(1) and (11). In turn, both "access device" and "telecommunication identifying information" are encompassed by the statutory definition of "means of identification" in 18 U.S.C. § 1028(d)(3)(D).[6] To the extent that the same offense conduct may be subject to both the identity theft and the cloning enhancements (particularly if the cloning enhancement encompasses *all access devices* as was proposed in Option Two for cloned wireless telephones), consolidating the covered offense conduct into one enhancement provision, as opposed to separate and cumulative provisions, is intended to eliminate this possibility.

Modifications to Scope of Enhancement

Another modification made by Option Three is to implement more broadly the directive in the Wireless Telephone Protection Act of 1998. Two options were originally published in the Federal Register on February 11, 2000, to address these directives. Option One essentially tracks the statutory definitions of 18 U.S.C. § 1029(a)(9) so that the proposed two-level enhancement applies to offense conduct involving *cloning equipment, cloned telecommunications instruments, and scanners*. Option Two is considerably broader than Option One in that it extends the proposed two-level enhancement to *counterfeit access devices*.

---

[6] See Appendix D for a further discussion of the relationship between identity theft and wireless telephone cloning.

Option Three is even broader than Option Two, in that it proposes in subsection (B) to expand the enhancement for counterfeit access devices to include *unauthorized access devices*, most commonly, stolen credit cards, within the proposed two-level enhancement, thereby incorporating a substantial aspect of the identity theft proposal submitted by the Department of Justice. Essentially, Option Three has modified the second prong of Option Two for identity theft that would increase punishment for the production and transfer of six or more identification means, and has both narrowed and broadened that proposal. Option Three has narrowed Option Two for identity theft by confining the enhancement to *unauthorized access devices* rather than to all identification means, while broadening it by reducing to *one* the minimum number of unauthorized access devices necessary to trigger this enhancement. Finally, Option Three eliminates the provision in Option One that would have expanded the rule of consequential damages to identity theft situations, electing instead to handle situations involving substantial damage to a victim's credit reputation and inconvenience by means of an upward departure.

Underlying Policy

With respect to identity theft, the underlying policy in subsection (C) of Option Three remains unchanged from Option One in that affirmative identity theft or "breeding" remains the central focus of the enhancement. The language of Option Three has been streamlined by eliminating the complicated definitions of Option One and using terms, to the extent possible, that correspond to statutorily defined terms.

Option Three, like Option One, presumes that an individual victim's reputation and credit standing have been compromised (or at least put at great risk) whenever identification means are "bred," and thus builds in a two-level enhancement without overburdening the court with additional evidentiary proof at the sentencing hearing. Option Three also provides an encouraged upward departure if the offense level does not adequately address the seriousness of the offense, as for example, if the offense caused substantial harm to the victim's reputation or credit record.

Minimum Offense Level of Twelve

Option Three provides a minimum offense level of twelve in order to reflect the seriousness of the conduct associated with identity theft. Also, the offense conduct of "breeding" is similar to "sophisticated means" enhancement at §2F1.1(b)(5), and it is likely that much of the offense conduct covered by Option Three may be subject to the sophisticated means enhancement as well. Because the sophisticated means enhancement has a floor of twelve, for the sake of consistency the minimum offense level for identity theft in Option Three should be the same, although it is not intended that the separate two-level increase for "sophisticated means" of §2F1.1(b)(5)(C) apply unless based on other, different conduct.

Minimum Loss Rule

Option Three provides for a minimum loss amount of $500 for unauthorized or counterfeit access devices. However, if the unauthorized access device is a means of telecommunications access (*e.g.*, unused ESN/MIN pairs of numbers) that was not involved in the commission of the offense, then Option Three provides for a minimum loss amount of $100.

ADDITIONAL WIRELESS TELEPHONE CLONING ISSUES

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 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."[7]

The Commission invited comment, generally, regarding whether the use of a cloned wireless telephone in connection with other criminal activity should warrant more serious punishment than the commission of the same offense without the involvement of a cloned telephone. The issue for comment also sought direction regarding whether this additional criminal conduct should be addressed through a Chapter Three adjustment, a specific offense characteristic in one or more Chapter Two guidelines (such as §2D1.1 or §2F1.1), or as a cross reference that would sentence the defendant convicted of an offense involving the use or transfer of a cloned wireless telephone at the level for the offense for which the telephone was used.

The staff has not drafted options to address the issue of additional criminal conduct for several reasons. The question remains as to whether or not an offense committed with the use of a cloned phone is more serious than one committed without the use of a cloned phone. Although the use of a cloned phone to commit additional criminal conduct may hamper law enforcement investigations, it is also possible to achieve the same level of anonymity by using other legal means, such as phone cards and disposable cell phones.

Potential "double-counting" issues also exist with regard to an enhancement for use of cloned phones in connection with another offense. An enhancement in the fraud guideline might overlap with the more than minimal planning enhancement. It could be argued that use of a cloned phone to commit another crime is a significant affirmative step "taken to conceal the offense". Additionally placing this enhancement solely in the fraud guideline would severely limit the number and types of cases in which this enhancement would apply.

This is a particular concern because the use of a cloned phone in drug trafficking and violent offenses probably represent the more egregious cases where the enhancement is desired. The enhancement would have to be placed in other Chapter Two guidelines in order to have broader application to other offenses. However, currently, the Commission has no reliable data regarding the frequency with which this conduct occurs in offenses other than fraud. In addition, an increase in the drug guideline may raise issues regarding the proportionality and severity of drug

---

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

sentences. DEA estimates that 80% of drug cases involve cloned phones. Using that figure, an enhancement in the drug guideline would affect 15,000 cases, increasing sentences an average of 16 months.

Drafting a cross reference in §2F1.1 also raised fairness issues. Although a cross refernce would certainly guarantee that this conduct is addressed in various offenses, the disadvantage to a cross reference 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. In addition, in cases where the more serious behavior is charged, the cross reference would not result in any additional punishment under the guidelines. In such situations it would be an unnecessary determination for the court to make without any actual consequence to the defendant's sentence.

ACTUAL OPTION APPLICATION

In an effort to illustrate further the distinctions and similarities among the proposed options, a chart has been prepared comparing the application of Options One, Two, and Three to eight of the actual cases in Fiscal Year 1999 which had convictions under 18 U.S.C. § 1028(a)(7).[8]

[8]See Appendix E. Note that of the twelve cases containing 18 U.S.C. § 1028(a)(7) as a statute of conviction, two were immigration-related and the immigration guidelines were applied. The remaining two cases involved co-defendants and the same offense conduct as cases which were analyzed.

APPENDIX A:

Issue: ***Does the term "means of identification" in 18 U.S.C. § 1028 (a)(7) include information about a fictitious (as opposed to an actual) individual?***

As discussed in more detail below, the legislative history of The Identity Theft and Assumption Deterrence Act ("Identity Theft Act"), is not definitive on the issue but it indicates that this new statutory section was primarily intended to address harm to actual individuals. Although no reported cases have discussed the new law, the Commission's Monitoring database includes a dozen cases involving prosecutions under Title 18 section 1028(a)(7) since its enactment on October 31, 1998. All but one of the cases involved offenders who were convicted under section 1028(a)(7) for using the "means of identification" of an actual individual.

This memorandum will discuss: (1) the language of the new subsections of section 1028; (2) the relevant legislative history; and (3) the cases with convictions under section 1028(a)(7).

I. Statutory Language

On its face, the new language of the statute does not make clear whether it would cover identifying information that corresponds to a fictitious individual. The new section of the statute does criminalize the knowing and illegal transfer or use of "a means of identification of *another person*," 18 U.S.C. § 1028(a)(7) (emphasis added)[1], and the term at issue is defined as "any name or number that may be used . . . to identify *a specific individual*." 18 U.S.C. § 1028(d)(3) (emphasis added).[2] Although this language could be read to suggest that it is limited to cover only the information of an actual rather than a fictitious person,[3] it does not necessarily exclude

---

[1]Section 1028(a)(7) prohibits the knowing and illegal transfer or use of "a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." 18 U.S.C. §1028(a)(7).

[T]he term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any–

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
(C) unique electronic identification number, address, or routing code; or
(D) telecommunication identifying information or access device (as defined in section 1029(e)).

18 U.S.C. §1028(d)(3).

[3]"Specific" is defined in Webster's Dictionary as "set forth explicitly; definite."

information about "another person" or a "specific individual" who is non-existent. Accordingly, the legislative history was reviewed in an effort to clarify the intent of the language.

II. Legislative History

The legislative history of the Identity Theft Act does not address whether a misused or stolen information in section 1028(a)(7) can be that of a fictitious individual. While acknowledging that real individuals as well as financial commercial institutions are the victims of identity theft, however, much of the legislative history focused on the need to remedy harms suffered by real people. In their statements, many of the cosponsors of the Act discussed harms suffered by colleagues and constituents as a result of identity theft.

Senator Kyl (R-Az), who introduced identity theft legislation in the Senate, emphasized that the bill was intended to focus on harm to real individuals. See *Identity Fraud: Hearings on S. 512 Before the Subcomm. On Technology, Terrorism and Government of the Senate Judiciary Comm.*, 105th Cong. (May 20,1998) (opening statement of Sen.Kyl). The Senate heard the testimony of an individual victim of identity theft (Senator Kyl's constituent), a victim's rights advocate, and an FTC official, each of whom emphasized that the legislation was intended to address harms to real individuals resulting from identity theft. Id.

Senator Leahy (D-Vt), one of the cosponsors of identity theft legislation stated: "This bill penalizes the theft of personal identification information that results in harm to the person whose identification is stolen and then used for false credit cards, fraudulent loans or for other illegal purposes." 144 CONG. REC. S12604 (daily ed. October 14, 1998) (statement of Sen. Leahy). He went on to say:

> The consequences for the victims of identity theft can be severe. They can have their credit ratings ruined and be unable to get credit cards, student loans, or mortgages. They can be hounded by creditors or collection agencies to repay debts they never incurred, but they were obtained in their name, at their address, with their social security number or diver's license number. It can take months or even years, and agonizing effort, to clear their good names and correct their credit histories. I understand that, in some instances, victims of identity theft have even been arrested for crimes they never committed when the actual perpetrators provided law enforcement officials with assumed names.

144 CONG. REC. S12604 (daily ed. October 14, 1998) (statement of Sen. Leahy).

Senator Hatch (R-Ut), an original cosponsor of the bill, also focused on the harm to real individuals. The bill, according to Senator Hatch, "recognizes not only that it is a crime to steal personal information, and enhances penalties for such crimes, but it also recognizes the person, whose information has been stolen, as the real victim." 144 CONG. REC. S9504 (daily ed. July 30, 1998) (statement of Sen. Hatch). Senator Hatch emphasized that the other fraud statutes

> [Do] little to compensate the victim or address the horror suffered by the individual whose life has been invaded. Often these general criminal statutes treat only affected banks, credit bureaus, and other financial institutions as the victim, leaving the primary victim, the innocent person, without recourse to reclaim his or her life and identity.

Id. Senator Feinstein (D-Ca), another cosponsor of the legislation, stated that the new legislation "does two critical things in the war on identity theft: it gives prosecutors the tools they need, and it recognizes that identity theft victimizes individuals." 144 CONG. REC. S9504 (daily ed. July 30, 1998) (statement of Sen. Feinstein).

Finally, when President Clinton signed the bill into law, he stated: "It can take years for victims of identity theft to restore their credit ratings and their reputations . . . This legislation will enable . . . law enforcement agencies to combat this type of crime, which can financially devastate its victims." Statement by President Upon Signing H.R. 4151, 34 WEEKLY COMP. PRES. DOC. 2203 (November 9, 1998).

It should be noted, however, that the statements and congressional testimony on the Identity Theft Act were not limited to discussions of harm to individuals. For example, testimony provided by officials from Visa USA, Inc. and the American Bankers Association mentions that the legislation would serve to protect financial institutions as well as individuals from frauds that rely on "false" as well as "stolen identity." See *Financial Information Privacy Act: Hearings on H.R. 4321 Before the House Comm. On Banking and Financial Services* , 105th Cong. (July 28, 1998) (statements of Boris Melnikoff, Senior Vice President, Wachovia Corp. on behalf of American Bankers Association and Russell Schrader, Senior Vice President, VISA, U.S.A., Inc.) "[F]raud artists rely on two methods: stealing from valid existing accounts and creating bogus accounts for fraudulent purposes." Id. Nonetheless, the majority of the testimony about the proposed bill and statements by its congressional sponsors focused on the need to criminalize the theft of information about actual individuals.

III. Case Law

There have been no reported cases addressing either the legislative history of subsection 1028(a)(7) or whether it prohibits the use of information about a fictitious person. However, the Commission's Monitoring office has received twelve cases in which defendants were convicted of violations of subsection 1028(a)(7) in fiscal year 1999.[4] Review of those cases reflects that only one involved a conviction based on "means of identification" of a fictitious individual. The defendant in that case used a fictitious name to cash a counterfeit cashier's check. The other 11 cases convicted this past year under subsection § 1028(a)(7), however, clearly involved the misuse of the

---

[4]Cases regarding identification documents are covered by the other sections 18 U.S.C. § 1028 but are not informative on this subject because those parts of the statute were drafted years earlier and clearly addressed "false" as well as authentic identification documents. At least one court recently reviewed the legislative history of the definition section of this statute and concluded that Congress intended to define the term "identification document" broadly. See, e.g., United States v Castellanos, 165 F.3d 1129, 1132 (7th Cir. 1999) (concluding that Congress intended to encompass both complete and incomplete documents within its definition).

identification mean of actual individuals, whether living or deceased, an application that may ultimately be closer to the intent suggested by the legislative history.[5]

[5]*See, generally* Appendix B, which contains a summary of the charges, counts of convictions, offense conduct, and sentences in these 12 cases.

APPENDIX B

CONVICTIONS UNDER 18 U.S.C. § 1028(a)(7)[1]
Fiscal Year 1999

Case No. 448025 (S.D. Miss)

Defendant charged in seven-count indictment:

- 18 U.S.C. §371, Conspiracy to produce false identification (one count)
- 18 U.S.C. § 1028(a)(7), Using false identity with intent to commit a felony (not specified, indictment not available) (one count)
- 18 U.S.C. § 1028(a)(1), Producing a false identification document (four counts)
- 18 U.S.C. § 982, Forfeiture of property

Defendant entered guilty pleas to § 1028(a)(7) and forfeiture.

Offense Conduct: In large fraud operation, several people were solicited to cash fictitious counterfeit cashier's checks and instructed to have passport photos made which were later given back to "runners" on valid Texas-issued driver's licenses. At various gambling casinos, various runners displayed state driver's license with their photo and another's name, gave a cashier's check as a deposit, then left soon and obtained cash refund of balance of the amount of the check deposited with the casino; cashier's check later discovered to be fraudulent. No individual victims identified, casinos are victims of the counterfeit check fraud, and loss amount of fraud calculated into sentence. Since the checks were counterfeit, it is unlikely the names on the fictitious driver's licenses corresponded to actual individuals.

Sentence:	**Criminal History Category:**
Eighteen months incarceration Actual and intended loss $149,500 Restitution ordered $101,100	III

[1]U.S. Sentencing Commission, 1999 Datafile, USSCFY99.

Case No. 450585 (D.D.C.)

One count of 18 U.S.C. §1028(a)(7) charged (noted on charging documents as " misdemeanor fraud and related activity in connection with identification documents and information.")

Defendant entered guilty plea.

Offense Conduct: Defendant's friend applied for passport, filling out an official DSP-11 application form in name of another actual individual; friend presented a Pennsylvania birth certificate, Virginia driver's license and Virginia ID document, all in the name of another *actual* individual; that individual was ultimately determined to be living in a half-way house, and said her documents were lost or stolen; however, witness stated that defendant had apparently paid the "victim" $100 for her identification papers. Because defendant also signed the DSP-11 application form as a witness attesting to her friend's false name and identity, defendant was charged with a misdemeanor violation.

The immigration guideline at §**2L2.2(a)** with a BOL of 8 was applied at sentencing.

Sentence:	**Criminal History Category:**
One year probation No loss No restitution	I

Case No. 450973 and 456310 (S.D. Tex.)

Sole count of 18 U.S.C. § 1028(a)(7) charged and guilty plea entered.

Offense Conduct: As part of large scheme that involved stealing and cashing U.S. Treasury checks in major cities, defendant was recruited to cash checks using counterfeit ID documents, and was instructed to have his photo taken and given counterfeit IDs in the names of the *actual individuals whose names appeared on Treasury checks.*

Sentence:		**Criminal History Category:**
450977	14 months incarceration Intended loss $2,263 No restitution	IV
456310	6 months plus two days Intended loss $ 2,263 No restitution	I

Case No. 452399 (M.D. Fla.)

Defendant charged in two-count indictment:

- 18 U.S.C. § 911, False impersonation of U.S. Citizen
- 18 U.S.C. § 1028(a)(7), Use of SSN assigned to another to commit unlawful act, *e.g.*, to elude inspection or examination by immigration officials in violation of 18 U.S.C. § 1325.

Defendant entered guilty plea to both counts.

Offense Conduct: Defendant falsely represented himself on employment application to be a U.S. citizen and used social security of *another actual individual*; defendant also in possession of State of Florida ID card and credit cards of that other real individual but information in PSI insufficient to determine whether defendant "bred" those documents or whether they originated with lawful owner and were stolen from him.
PSI indicates no victim, although clearly the misused SSN belonged an actual person.

The immigration guideline §**2L2.2(a)** with a BOL of 8 was applied at sentencing**.**

Sentence:	**Criminal History Category:**
Three months incarceration No loss No restitution	I

Case No. 452892 (D.D.C.)

Defendant was charged in a two count indictment

- 18 U.S.C. § 1029, Unauthorized use of access devices
- 18 U.S.C. § 1028(a)(7), Identity Theft

Defendant entered guilty plea to both counts.

Offense Conduct: Defendant obtained social security numbers and identification information of several employees where he worked, as well as CEO's spouse; opened First USA Bank credit cards via telephone in three names, and was also discovered, during the investigation, to have committed similar activity in name of deceased individual several years ago in another jurisdiction. Defendant also passed bad checks on his own account. No discussion of harm to *actual* individuals contained in the PSI.

Sentence:	**Criminal History Category:**
Eighteen months incarceration Loss $113,971.18 Restitution ordered $110,041.23	III

Case No. 455457 and 463647 (S.D. Tex.)

Defendants charged in three-count indictment

- 18 U.S.C. § 1028(a)(1), Possession of false identification documents
- 18 U.S.C. § 1028(a)(7), Use of false identification documents
- 18 U.S.C. § 1001, False statement to postal officials (form to receive mail)

Defendants entered guilty plea to all counts.

Offense Conduct: Two customers of Monex had ordered gold coins and paid with personal checks; checks were subsequently stolen, and addresses altered; the delivery of the coins was diverted to perpetrators' address at Commercial Mailboxes; defendant presented two forms of identification (driver's licenses and other IDs in connection with Postal Service form in order to rent a box at Commercial Mailboxes) the names on which corresponded to the *actual individuals whose checks were stolen*. The defendants were also found to have VISA credit cards in the victim's names, but it is unclear from the PSI whether the defendants "bred" these additional ID means, or whether they were actual cards issued to the victims originally and stolen from them; no discussion of individual victim impact in the PSI.

Sentence:		**Criminal History Category:**
455457	Twelve months plus 1 day incarceration Intended loss $134,202 No restitution ordered	I
463647	Twelve months plus 1 day incarceration Intended loss $134,202 No restitution	I

Case No. 456825 (D.Nev.)

Defendant charged in thirteen-count indictment

- 18 U.S.C. § 1028(a)(7), Uttering forged securities by means of false identification (three counts)
- 18 U.S.C. §§1028(a)(7) and 1344, Use of another's identification to commit bank fraud (one count)
- 18 U.S.C. § 513(a), Uttering forged securities (five counts)
- 18 U.S.C. § 1344, Scheme to defraud federally insured financial institution (three counts)

Defendant entered guilty plea to one count each of 18 U.S.C. §§ 1028(a)(7), 1344, and 513(a).

Offense Conduct: Defendant used driver's license of an individual whose purse had been stolen by an accomplice; defendant and accomplice also involved in stealing mail, opening fraudulent accounts in aliases, altering and negotiating stolen checks.

Sentence:	**Criminal History Category:**
6 months incarceration	II
Actual and intended loss $14,353	
Restitution ordered $10,583	

Case No. 459294 (W.D. Wis.)

Defendant charged in five-count indictment

- 18 U.S.C. § 1028(a)(7), Use of name of a real individual to commit theft of property, activity that constitutes a felony under Wisconsin state law (one count)
- 42 U.S.C. § 408(a)(7)(B), False use of a Social Security number (one count)
- 18 U.S.C. § 1001, False statements (three counts)

Defendant entered guilty plea to Count One, 18 U.S.C. § 1028(a)(7)

Offense conduct: Defendant used alias to obtain a job in the Supreme Court as a custodian and then stole computer equipment valued at $65,000, name and social security number misused to obtain the employment were those of *another actual individual* who said he did not know defendant; Defendant applied for at least two jobs in the name of the victim individual, as well as obtained a social security card, a Wisconsin state identification card, and checking and savings accounts, and applied for credit in the victim's name using the victim's personal identification means; defendant also submitted a false W-4 tax form using the victim's name and social security number; Additional conduct includes false claim in defendant's own name to the Social Security Administration to claim benefits to which he was not entitled.

No discussion of impact to actual victim whose identify means were misused.

Sentence:	**Criminal History Category:**
Twenty-one months incarceration Actual loss $62,849.43 Restitution ordered $62,849.43	IV

Case No. 460458 (N.D. Tex.)

Defendant charged in eight- count indictment:

- 42 U.S.C. § 408(a)(7)(B), Fraudulent use of social security number (six counts)
- 18 U.S.C. § 1028 (a)(7), False use of identification (one count)
- 18 U.S.C. § 1029(a)(2), Unauthorized use of access device (one count)

Defendant entered guilty plea to one count of 18 U.S.C. § 1028(a)(7)

Offense Conduct: Defendant opened bank account in name of organization, providing Articles of Incorporation (not indicated whether these were genuine or counterfeit) which showed her to be the president and *also used a social security number that was not her own*; Defendant also subscribed to phone service and then paid with counterfeit checks; apparently defendant made counterfeit checks on a computer using the name and account number (slightly altered) of an actual legitimate company; evidence included blank checks, scanners, and testimony from an "employee" who saw the checks being printed; additional relevant conduct included assuming the identity of her sister to purchase a home and obtain a mortgage loan valued at $193,000; as part of the supporting documentation to obtain the mortgage loan, defendant fabricated a tax return and forged the signature of her sister and also *included a tax preparer's name with a fabricated EIN that was not actually assigned to that tax preparer*, defendant also *used sister's name, and a variation of her sister's social security number* and other identification (not specified) to open a bank account, and deposited worthless checks. Defendant held liable for $375,000 loss.

Sentence:	**Criminal History Category:**
Twenty-four months incarceration Intended and actual loss $375,000 Restitution ordered $154,669	IV

Case No. 460527 (E.D. N.C.)

Defendant charged in fourteen count indictment

- 18 U.S.C. § 371, Conspiracy to steel mail in violation of 1708, to produce false identification documents in violation of § 1028, and to commit bank fraud in violation of § 1344 (one count)
- 18 U.S.C. § 1708, Steal and take mail from a letterbox (three counts)
- 18 U.S.C. § 1028(9)(1) & (2), Produce false identification documents (a false NC driver's containing defendant's photograph, and different false names) (five counts)
- 18 U.S.C. § 1344, Aiding and abetting others to use identification of another without lawful authority with the intent to commit bank fraud (five counts)

Defendant entered guilty plea to all counts except conspiracy.

Offense Conduct: Defendant and others engaged in stealing checks from 37 residential mail boxes and producing counterfeit checks based on those stolen checks, then negotiating the counterfeit checks use false identifications (counterfeit state driver's licenses bearing defendants' photos and names of *actual individual victims* whose checks had been stolen from mail).

Sentence:	**Criminal History Category:**
Sixty-three months incarceration Actual loss $117,472.63 Restitution ordered $117,472.63	III

Includes upward departure of two additional offense levels because § 2F1.1 does not adequately take into consideration non-monetary harm and emotional trauma to 37 individual victims.

APPENDIX C:

Issue: ***How is the term "transfer" interpreted in the context of 18 U.S.C. § 1028?***

While there is no clear case law on point, the use of the word "transfer" would appear to be akin to "distribution" and not to "use." The False Identification Crime Control Act of 1982, 18 U.S.C. § 1028, prohibits four separate activities: production, use, transfer and possession with the intent to use or transfer. *See* United States v. Rohn, 964 F.2d 310, 312 (4th Cir. 1992). Section 1028(a)(2) prohibits the knowing transfer of illegal identification documents and section 1028(a)(3) prohibits the knowing possession of 5 or more illegal identification documents with the intent to unlawfully use or transfer them. Because Congress used both the terms "use" and "transfer," fundamental principles of statutory construction would assume that they are not intended to be synonymous.

A review of the case law indicates that "transfer" has generally been used in cases of distribution. In United States v. Alejandro, 118 F.3d 1518 (11th Cir. 1997), the defendant was stopped at the Miami airport by custom and immigration authorities. The defendant was found to have 108 counterfeit birth certificates loosely inserted into the pages of a rolled-up newspaper. The defendant was charged and convicted at jury trial of possession with the intent to transfer five or more false identification documents in violation of 18 U.S.C. §1028(a)(3). On appeal, the defendant challenged the sufficiency of the evidence that he possessed the documents "with the willful intent to transfer" them unlawfully. The Eleventh Circuit noted there was substantial circumstantial evidence of guilt. The number of documents, together with the fact they were hidden, refuted the argument that they were for personal or professional use. The documents also had a potential "street" value of $32,400.

Congress did not criminalize the mere possession of false identification, but requires that an individual possess the identification documents with the intent to use or transfer. 18 U.S.C. 1028(a)(3). In United States v. Rohn, 964 F.2d 310, 313 (4th Cir. 1992), the appellate court reversed the defendant's conviction because the government failed to prove that the defendant possessed more than seventy pieces of false identification with the intent use or transfer them unlawfully. The seventy pieces of identification included Social Security cards, driver's licensces and identification cards in thirteen separate names, but all with the defendant's picture.

APPENDIX D:

Issues: **I.** ***Can a cloned phone be considered an "identity means" under 18 U.S.C. § 1028*****?**

II. ***What is included within the concepts of "access device" and "counterfeit access device" as used in 18 U.S.C. § 1029?***

I. Can a cloned phone be considered an "identity means" under 18 U.S.C. § 1028?

Title U.S.C. § 1028(d)(3)(D) provides that "means of identification" include "tele-communication identifying information or access device [s] (as defined in section 1029(e))." Section 1029 (e)(1) defines "access device" to include" . . . any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number or other telecommunications . . . identifier . . . that can be used . . . to obtain . . . services or any thing of value." Section 1029(e)(11) defines "telecommunication identifying information" as an "electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account . . . ."

Given the breadth of these definitions and assuming, as seems reasonable, that the courts will view "identity means" and "means of identification" as synonymous, a cloned phone will be considered as an "identity means" under 18 U.S.C. § 1028(d)(3)(D), as augmented by 18 U.S.C. § 1029(e)(1) and (11).

For purposes of Option One, "means of identification" as defined in 18 U.S.C. § 1028(d)(3) will be co-extensive with "identifying information" as used in Option One. For purposes of Option Two, "fraudulent identification documents" are co-extensive with the definitions of "means of identification" and "access devices" in 18 U.S.C. §§ 1028 and 1029. Thus, a cloned phone will also be considered an "identity means" under either Option One or Option Two.

II. What is included within the concepts of "access device" and "counterfeit access device" as used in 18 U.S.C. § 1029?

The term "access device" is broadly defined at 18 U.S.C. §1029(e)(1) to include "any card, plate, code, account number, electronic serial number, mobile identification number, or other telecommunications service, equipment or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." Based on this expansive language, cloned phones, credit cards, debit cards, ESN-MIN pairs, credit card numbers, debit card numbers, social security numbers, health insurance account numbers, driver's license numbers, "PIN" numbers, bank account numbers, brokerage account numbers and other such types of identifying information constitute "access devices" as that phrase is used in 18 U.S.C. § 1029. *See*, *e.g.*, United States v. Bailey, 41 F.3d 413 (9th Cir. 1994) (falsified electronic serial numbers for cell phones); United States v. Taylor, 945 F.2d 1050 (8th Cir. 1991) (American Express account number); and United States v. Dabbs, 134 F.3d 1071 (11th Cir. 1998) (merchant's bank account number).

The term "counterfeit access device" is defined at 18 U.S.C. § 1029(e)(2) as "any access device that is counterfeit, fictitious, altered or forged, or an identifiable component of an access device or a counterfeit access device." Thus, "counterfeit access device" includes any of the indicia of identification mentioned in the paragraph above as long as it differs in some respect from the device after which it was patterned, constitutes identifying data of another person, or constitutes identifying data of a non-existent person.

With respect to the question regarding "valid but unissued credit card numbers," they do not, in my opinion, constitute "counterfeit access devices." They do, however, constitute an "unauthorized access device" in terms of 18 U.S.C. § 1029(e)(3) and, as such, their use to obtain anything of value in excess of $1,000 within one year is prohibited.

Appendix E
POSSIBLE RE-SENTENCING OUTCOMES FOR SELECTED IDENTITY THEFT CASES[1]

Case Description	Current Months Prison[2]	Option I Months Prison	Option I Elements	Option II Months Prison	Option II Elements	Option III Months Prison	Option III Elements
Used fictitious driver's licenses to cash counterfeit cashier's checks at casinos. 448025	18	18	none	18	none[3] (loss)	21	prod. cntrft. acc.dev.
Cashed stolen Treasury checks with counterfeit IDs bearing payees names. 450973	14	18	use ID to obtain ID	14	none (loss)	21	use ID to obtain ID, floor
Opened credit card accounts with stolen SSNs, negotiated counterfeit and NSF checks. 452892	18	21	use ID to obtain ID	18	none (loss)	21	prod cntrft. acc. dev., use ID to obtain ID
Negotiated altered checks using counterfeit ID with names of true account holders. 455457	12 [+1 day]	15	use ID to obtain ID	12 [+1 day]	none (loss)	15	prod. cntrft. acc. dev., use ID to obtain ID
Negotiated altered checks from stolen mail, opened accounts using aliases. 456825	6	6	none	6	none (loss)	10	prod. cntrft. acc. dev.
Created, negotiated counterfeit checks and used sister's ID to secure loans, accounts. 460458	24	30	use ID to obtain ID	24	none (loss)	30	equip, prod. cntrft. acc. dev.
Obtained employment, IDs, accounts, arrested using another's SSN and name. 459294	21	24	use ID to obtain ID	24	harm (loss)	24	use ID to obtain ID
Negotiated checks stolen from mail using IDs bearing account holders names, manufactured driver's licenses. 460527	63	78	use ID to obtain ID	63	harm (loss)	78	equip, prod. unauth. acc. dev., use ID to obtain ID

[1]Of the 12 cases that were convicted of 18 U.S.C. § 1028(a)(7), in fiscal year 1999, eight that were sentenced under the fraud guideline (§2F1.1) are included in this table. Two were excluded because they were sentenced under immigration guidelines and two were excluded because they were co-defendants in the same conduct.

[2]Cases were "re-sentenced" at the same point in the guideline range as their original sentences and the application of the Acceptance of Responsibility reduction was adjusted to -3 when offense level totals reached level 16.

[3]In most cases the extent of the harm to individual victims is difficult or impossible to know. Therefore, estimates of when this enhancement would apply *may* undercount actual occurrences. In only two cases did the harm enhancement very obviously apply. Indications of *none (loss)* and *(loss)* mean that conduct described under the second prong would apply but because a loss adjustment was already added, the +2 doesn't apply.

Identity Theft Guideline Options: Applicability to Selected FY99 18 U.S.C. § 1028 (a)(7) Cases

Case Description	Option I	Option II	Option III
448025 In large fraud operation, several people were solicited to cash fictitious counterfeit cashier's checks and instructed to have passport photos made which were later given back to "runners" on valid Texas-issued driver's licenses. At various gambling casinos, various runners displayed state driver's license with their photo and another's name, gave a cashier's check as a deposit, then left soon and obtained cash refund of balance of the amount of the check deposited with the casino; cashier's check later discovered to be fraudulent. No individual victims identified, casinos are victims of the counterfeit check fraud, and loss amount of fraud calculated into sentence. Since the checks were counterfeit, it is unlikely the names on the fictitious driver's licenses corresponded to actual individuals.	n/a	Increase for loss applied, so (b)(8) is n/a for production or transfer of 6 or more ID means.	+2 (b)(5)(B) for producing counterfeit access devices.
450973 As part of large scheme that involved stealing and cashing U.S. Treasury checks in major cities, defendant was recruited to cash checks using counterfeit ID documents, and was instructed to have his photo taken and given counterfeit IDs in the names of the *actual individuals whose names appeared on Treasury checks*.	+2 (b)(6)(A) for use of identifying information to obtain or make unauthorized ID means.	Increase for loss applied, so (b)(8) is n/a for production or transfer of 6 or more ID means.	+2 and floor (b)(5)(C) for the unauthorized use of any means of ID to produce/obtain any other means of ID.
452892 Defendant obtained social security numbers and identification information of several employees where he worked, as well as CEO's spouse; opened First USA Bank credit cards via telephone in three names, and was also discovered, during the investigation, to have committed similar activity in name of deceased individual several years ago in another jurisdiction. Defendant also passed bad checks on his own account. No discussion of harm to *actual* individuals contained in the PSI.	+2 (b)(6)(A) for use of identifying information to obtain or make unauthorized ID means.	Increase for loss applied, so (b)(8) is n/a for production or transfer of 6 or more ID means.	+2 (b)(5)(B) for producing counterfeit access devices OR (b)(5)(C) for the unauthorized use of any means of ID to produce/obtain any other means of ID.

Identity Theft Guideline Options: Applicability to Selected FY99 18 U.S.C. § 1028 (a)(7) Cases

Case Description	Option I	Option II	Option III
455457 Two customers of Monex had ordered gold coins and paid with personal checks; checks were subsequently stolen, and addresses altered; the delivery of the coins was diverted to perpetrators' address at Commercial Mailboxes; defendant presented two forms of identification (driver's licenses and other IDs in connection with Postal Service form in order to rent a box at Commercial Mailboxes) the names on which corresponded to the *actual individuals whose checks were stolen*. The defendants were also found to have VISA credit cards in the victim's names, but it is unclear from the PSI whether the defendants "bred" these additional ID means, or whether they were actual cards issued to the victims originally and stolen from them; no discussion of individual victim impact in the PSI.	+2 (b)(6)(A) for use of identifying information to obtain or make unauthorized ID means.	Increase for loss applied, so (b)(8) is n/a for production or transfer of 6 or more ID means.	+2 (b)(5)(B) for producing counterfeit access devices OR (b)(5)(C) for the unauthorized use of any means of ID to produce/obtain any other means of ID.
456825 Defendant used driver's license of an individual whose purse had been stolen by an accomplice; defendant and accomplice also involved in stealing mail, opening fraudulent accounts in aliases, altering and negotiating stolen checks.	n/a	Increase for loss applied, so (b)(8) is n/a for production or transfer of 6 or more ID means.	+2 (b)(5)(B) for producing counterfeit access devices.
460458 Defendant opened bank account in name of organization, providing Articles of Incorporation (not indicated whether these were genuine or counterfeit) which showed her to be the president and *also used a social security number that was not her own*; Defendant also subscribed to phone service and then paid with counterfeit checks; apparently defendant made counterfeit checks on a computer using the name and account number (slightly altered) of an actual legitimate company; evidence included blank checks, scanners, and testimony from an "employee" who saw the checks being printed; additional relevant conduct included assuming the identity of her sister to purchase a home and obtain a mortgage loan valued at $193,000; as part of the supporting documentation to obtain the mortgage loan, defendant fabricated a tax return and forged the signature of her sister and also *included a tax preparer's name with a fabricated EIN that was not actually assigned to that tax preparer*, defendant also *used sister's name, and a variation of her sister's social security number* and other identification (not specified) to open a bank account, and deposited worthless checks. Defendant held liable for $375,000 loss.	+2 (b)(6)(A) for use of identifying information to obtain or make unauthorized ID means.	Increase for loss applied, so (b)(8) is n/a for production or transfer of 6 or more ID means.	+2 (b)(5)(A) for possession of device making equipment OR (b)(5)(B) for producing counterfeit access devices.

Identity Theft Guideline Options: Applicability to Selected FY99 18 U.S.C. § 1028 (a)(7) Cases

Case Description	Option I	Option II	Option III
459294 Defendant used alias to obtain a job in the Supreme Court as a custodian and then stole computer equipment valued at $65,000, name and social security number misused to obtain the employment were those of *another actual individual* who said he did not know defendant; Defendant applied for at least two jobs in the name of the victim individual, as well as obtained a social security card, a Wisconsin state identification card, and checking and savings accounts, and applied for credit in the victim's name using the victim's personal identification means; defendant also submitted a false W-4 tax form using the victim's name and social security number; Additional conduct includes false claim in defendant's own name to the Social Security Administration to claim benefits to which he was not entitled.	+2 (b)(6)(A) for use of identifying information to obtain or make unauthorized ID means.	+2 (b)(7)(A) and (B) for harm to an individual...that was more than minimal. Increase for loss applied, so (b)(8) is n/a for production or transfer of 6 or more ID means.	+2 (b)(5)(C) for the unauthorized use of any means of ID to produce/ obtain any other means of ID.
460527 Defendant and others engaged in stealing checks from 37 residential mail boxes and producing counterfeit checks based on those stolen checks, then negotiating the counterfeit checks use false identifications (counterfeit state driver's licenses bearing defendants' photos and names of *actual individual victims* whose checks had been stolen from mail).	+2 (b)(6)(A) for use of identifying information to obtain or make unauthorized ID means.	+2 (b)(7)(A) and (B) for harm to an individual...that was more than minimal. Increase for loss applied, so (b)(8) is n/a for production or transfer of 6 or more ID means.	+2 (b)(5)(A) for possession of device making equipment OR (b)(5)(B) for producing counterfeit access devices OR (b)(5)(C)(i) for unauthorized use of any means of identification to produce/obtain any other means of ID.