FEDERAL PUBLIC DEFENDER
District of Arizona
850 West Adams Street, Suite 201
PHOENIX, ARIZONA 85007

JON M. SANDS
Federal Public Defender

(602) 382-2700
1-800-758-7053
(FAX) 382-2800

March 27, 2009

Honorable Ricardo H. Hinojosa
Acting Chair
United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500, South Lobby
Washington, D.C. 20002-8002

Re: Comments on ID Theft and Computer Crimes

Dear Judge Hinojosa:

With this letter, we provide comments on behalf of the Federal Public and Community Defenders on the proposed amendments and issues for comment relating to the directives set forth in § 209 of the Identity Theft Enforcement and Restitution Act of 2008, Pub. L. 110-326 (Sept. 26, 2008), and other issues related to identity theft and computer crimes, that were published in the Federal Register on January 27, 2009.[1] At the public hearing on March 17, 2009, we submitted written testimony on these matters. A copy of that written testimony, which includes the written comment by Martin Richey submitted on December 8, 2008, is attached and incorporated as part of this public comment.

We do not reiterate here our important arguments regarding deterrence, recidivism, and complexity. We address a few specific issues that were discussed at the public hearing.

A. The Commission Should Not Amend the Guidelines to Account for Individuals Who Do Not Suffer Monetary Loss in Identity Theft Cases.

As we stated in our written testimony, the Commission should not expand the definition of victim under USSG § 2B1.1(b)(2) to account for individuals who did not suffer monetary loss or who were fully reimbursed for their monetary losses, either on the basis of privacy concerns or on time spent resolving problems.

[1] *See* 74 Fed. Reg. 4,802, 4,803-10 (Jan. 27, 2009).

The available data does not show that a substantial number of individuals suffer significant non-monetary harm. Many individuals are not even aware that their identifying information has been misused. According to a survey conducted by the Federal Trade Commission, of those who are aware of the misuse, only about a quarter report, as a primary concern, the emotional toll resulting from an invasion of privacy.[2] A substantial proportion (30%) of those individuals who are aware that their identifying information was misused spent *an hour or less* resolving problems associated with the misuse of their identifying information, with the median reporting only spending four hours.[3] Only ten percent reported spending 55 hours or more resolving problems.[4]

At the hearing, the Department of Justice's *Ex Officio* asked Eric Handy, the representative at the hearing from the Identity Theft Resource Center, if that organization has any empirical evidence indicating the number of individuals suffering non-monetary harm in identity theft cases. Although Mr. Handy indicated that the organization studies that question every year, neither he nor the organization provided evidence that contradicted the information reported by the Federal Trade Commission.

The varying, and often very little, amount of time spent correcting problems caused by identify theft shows why the number of victims alone is a poor measure of harm and why the current invited upward departure provides a more appropriate way of accounting for substantial non-monetary harm. The Commission itself recognized in 1999 that reliance on the number of victims alone "can result in either overstating or understating the harm."[5] To account for circumstances in which the guideline "substantially understates the seriousness of the offense," USSG § 2B1.1, comment. (n.19(A)), the Commission provided for an upward departure where the offense "caused or risked substantial non-monetary harm," such as "psychological harm, or severe emotional trauma or resulted in a substantial invasion of privacy interest," *id.* comment. (n.19(A)(ii)).

Absent data indicating that courts are frequently departing upward to account for those atypical individuals who suffer an unusual amount of non-monetary harm, the Commission should not add unnecessary complexity to § 2B1.1 or increase penalties in a manner that may overstate the harm in many cases.

[2] Federal Trade Commission, *2006 Identity Theft Report*, at 52-53 & fig. 21 (Nov. 2007).

[3] *Id.* at 5-6 & tbl. 2.

[4] *Id.*

[5] USSC, *Identity Theft Final Report*, at 26 (Dec. 15, 1999).

B. Any Amendment to Account for Non-Monetary Harm in Identity Theft Cases Should Be Narrowly Tailored.

We recognize that the Commission may view this issue in identity theft cases as one that requires action in the form of an amendment to § 2B1.1, regardless of whether courts are or are not frequently departing upward. Although the Commission has not published a proposed amendment, we understand that it may act in some manner, perhaps by amending the definition of "loss" at Application Note 3 to count as "victims" those who do not suffer pecuniary harm but who suffer some other form of harm, or by amending the victim table at subsection (b)(2) to capture those individuals whose personal information was misused but who did not ultimately suffer any monetary loss. We continue to believe that such change is unnecessary, and we object to the promulgation of unpublished amendments. However, we offer the following thoughts regarding the scope of any such change.

First, any enhancement should be carefully circumscribed so that it captures only aggravated cases. In our written testimony, we proposed a special rule that would add a one-level enhancement if any person, otherwise not counted as a victim under § 2B1.1(b)(2), reasonably spent 50 hours or more resolving financial problems resulting from the misuse of the identifying information. This would limit the enhancement to capture harm not already captured by the loss table and to count only those individuals who experienced *aggravated* non-monetary harms as opposed to those non-monetary harms intrinsic to identity theft offenses.

If the Commission chooses to focus instead on the number of individuals who suffer non-monetary harm rather than the extent of the non-monetary harm in a particular case, it should not create a rule that would count each person at the same *rate* as a victim who suffered monetary harm. Instead, the Commission might add a special rule for identity theft offenses that adds a unitary enhancement when the offense involves a very large number of victims who suffer non-monetary harm, leaving the departure provision at Application Note 19 to account for those situations involving individuals who suffer truly unusual non-monetary harm. For example, the Commission might create a special rule for identity theft cases to add one level if the offense involved more than a certain large number of individuals who are not otherwise counted as victims under subsection (b)(2) but whose personal information was misused. Depending on the Commission's data regarding the typical case, the number of individuals should be high enough so that it will limit the enhancement to those identity theft cases in which the number of individuals whose identifying information was actually misused represents the *aggravated* case.

A useful analogy might be drawn from the mass-marketing enhancement at subsection (b)(2)(A)(ii). That two-level increase functions as an alternative method for accounting for large numbers of individuals who may have been affected by an offense but who have not necessarily suffered monetary harm. In 2004, when the Commission broadened that enhancement to apply automatically to conduct described in 18 U.S.C. §

1037 (involving email spam), regardless of whether the person was convicted of § 1037, it explained that it was responding to Congress's concern regarding "offenses that are facilitated by sending large volumes of electronic mail." USSG, App. C, Amend. No. 665 (Nov. 1, 2004). For identity theft offenses involving large volumes of small harms or harms difficult or impossible to measure, similar reasoning might apply.

At least one court has recognized that estimating non-monetary or emotional harm may not be an appropriate measure of harm in cases involving large numbers of affected individuals who experience differing levels of subjective, non-monetary harm. In a case involving a massive email spam operation prosecuted under 18 U.S.C. § 1037, the government asked the court to apply the six-level enhancement for "over 250 victims" under USSG § 2B1.1(b)(2)(C) based on its theory that "hundreds of millions, perhaps billions," of people received the spam, and each had to spend some time deleting the spam or resolving problems resulting from the spam. *See* Gov't Sentencing Mem., at 16, *United States v. Soloway*, No. CR07-187MJP (July 22, 2008). Only sixty-one individuals submitted victim impact statements, however, with some relying on varying methods of calculating their non-monetary or emotional harms.

Regarding the losses claimed by the victims, the judge declined to calculate loss based on individual victims' lost time or emotional damage, stating: "I would never be able to calculate what the loss was. It would be impossible. Because there are so many people and there are so many shades of grey amongst them." Tr. of Sentencing Proceedings, at 3, *United States v. Soloway*, No. CR07-187MJP (July 22, 2008). For similar reasons, the judge declined to apply the enhancement for more than 250 victims, finding that the alternative two-level increase under subsection (b)(2)(A)(ii) for offenses involving mass-marketing was more appropriate in such a case. *Id.* at 5. She explained:

> [C]ounting victims is a very difficult task . . ., trying to define who is truly a victim and who is not. We will have millions of people out there who are harmed but who didn't know where to complain, we have people who complained to entities that couldn't do anything about it. . . .
>
> But the guidelines are also helpful to us there, because they say when this is a mass market event, then you count two points. . . . I can't count victims one-by-one.

Id.

As recognized by the judge there, the alternative mass-marketing enhancement indicates that the Commission concluded that a uniform increase in the offense level is appropriate regardless of whether an offense involved a hundred, a thousand, or a billion emails. Just as in cases involving email spam, counting untold numbers of victims in offenses involving identity theft would risk imprecise and varying measures of harm and could easily overstate the harm in cases involving large numbers of individuals whose information was used. Our proposals would limit the enhancement to obviate these risks.

C. The Commission Should Not Disaggregate Intent to Cause Damage and Intent to Obtain Personal Information in 18 U.S.C. § 1030 Cases.

In our written testimony, we stated that the Commission should not disaggregate a defendant's intent to cause damage and intent to obtain personal information so that they are considered separately from the other factors set forth in § 2B1.1(b)(15) related to offenses under 18 U.S.C. § 1030. We are not aware of any new data indicating that the Commission's stated rationale for structuring the enhancements in an incremental manner to punish incrementally more serious offenses is no longer supported.

In its written testimony for the hearing on March 17th, the Department of Justice asserts that the provision is not functioning in its intended manner, and that it "mandates the same sentence for strikingly dissimilar conduct." As examples, the Department compared the defendant who intended to obtain personal information from a grocery store with a defendant who intended to obtain such information from a "critical infrastructure computer," and a defendant who intentionally damaged a military computer with one who intentionally damaged a computer in someone's home. According to the Department, the first offense in each example is more serious than the second.

Setting aside the fact that the guidelines no longer "mandate" sentences, the Department's arguments depend on its assumption that § 1030 offenses involving government computers or computers used to operate or maintain critical infrastructures are *always* more serious than offenses involving other computers. Its proposed amendment would increase from two to four levels the enhancement for the individual who intended to obtain personal information from a critical infrastructure computer (as opposed to a grocery store, which would continue to get a two level enhancement), and increase from four to six levels the enhancement for the person who intended to damage a military computer (as opposed to a personal computer not part of any critical infrastructure, which would continue to get a four-level enhancement). In addition, the enhancements for intent to obtain personal information and intentional damage to a protected computer would apply cumulatively to each other and to the enhancement for computers involving a critical infrastructure.

While the Department makes a blanket assertion that critical infrastructure computers "typically contain far more sensitive information, such as medical records and classified information" and that "obtaining personal information from these types of computers clearly warrants more severe punishment," it offers no evidence to support that view. The Commission defines "critical infrastructure" as "systems and assets vital to national defense, economic security, public health or safety or any combination of those matters." USSG § 2B1.1, comment. (n.13(A)). A critical infrastructure can be either privately or publicly owned, and examples include not only systems that may maintain medical records or classified information, but also gas and oil production, storage and delivery systems, water supply systems, telecommunications networks,

electrical power delivery systems, financing and banking systems, and highway and mass transit systems, including airlines and airports. *Id*. Obviously, not all critical infrastructure computers contain "more sensitive information, such as medical records and classified information," as the Department asserts.

Further, all personal information is potentially "sensitive," which is why the guidelines already have a two-level increase to account for the intent to obtain personal information. The Commission defines "personal information" as "sensitive or private information (including such information in the possession of a third party), including (i) medical records; (ii) wills, (iii) diaries, (iv) private correspondence, including email; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information." USSG § 2B1.1, comment. (n.(13(A)). Nothing indicates that some of this information is more sensitive or private than the others. Many people keep highly sensitive information on their personal computers, such as diaries and photographs, which may be far more sensitive than any personal information kept by an electric company or airline. And with the advent of electronic records, many lawyers, doctors, and others keep information on many clients on laptops and other personal computers.

For those cases in which the two-level enhancement for intent to obtain personal information does not adequately capture the seriousness of the offense or the sensitivity of the information, Application Note 19 provides for upward departure if the "offense caused or risked a substantial non-monetary harm," such as "invasion of privacy interest (through, for example, the theft of personal information such as medical, educational, or financial records"). USSG § 2B1.1, comment. (n.19(A)(ii)). It also provides for upward departure for offenses involving stolen information from a protected computer if "the defendant sought the stolen information to further a broader criminal purpose." *Id.* comment. (n.19(A)(v)).

In any event, even if the Commission concludes that intent to obtain personal information from a critical infrastructure computer is more serious than intent to obtain personal information from a personal computer, and that the difference is not adequately reflected by the current structure of § 2B1.1(b)(15)(a), the solution is not necessarily to *increase* the range for intent to obtain personal information from a critical infrastructure computer, but could be to *decrease* the range for offenses involving intent to obtain personal information from a computer that is not used to maintain or operate a critical infrastructure.

With respect to intentional damage under 18 U.S.C. § 1030(a)(5)(A), the Department simply states, again without supporting evidence, that the social harm is greater when a defendant intentionally damages a critical infrastructure computer, as opposed to a personal computer. However, it does not explain why this is necessarily true. To the extent that Congress has criminalized conduct involving intentional damage to a personal computer that does not affect a financial institution or the United States Government, it did not distinguish between those computers and other protected computers for penalty purposes. The aim of § 1030(a)(5)(A) is to punish intentional

damage to any "protected computer." The focus of the current enhancement is to punish the intent to damage, regardless of the type of protected computer. We are unaware of any data indicating how many offenses under § 1030(a)(5)(A) involve personal computers versus military computers, or how courts are treating these two types of offenses. The Department's proposal adds unnecessary complexity to a guideline whose "defects," as far as we know, have not been made apparent by judicial feedback in the form of departures or variances.

As with intent to obtain personal information, even if the Commission concludes that intentional damage to a military computer is more serious than intentional damage to a personal computer, the solution should not necessarily mean that the guidelines must be amended to *increase* the range for damage to military computers. The Commission could *decrease* the range for offenses involving intentional damage only to a personal computer to achieve the desired result.

As always, we very much appreciate the opportunity to submit comments on the proposed amendments. We look forward to continue working with the Commission on these and other matters.

Very truly yours,

JON M. SANDS
Federal Public Defender, District of Arizona
Chair, Federal Defender Sentencing Guidelines Committee

cc: Hon. Ruben Castillo, Vice Chair
Hon. William K. Sessions III, Vice Chair
Commissioner William B. Carr, Jr.
Commissioner Dabney Friedrich
Commissioner Beryl A. Howell
Commissioner *Ex Officio* Edward F. Reilly, Jr.
Commissioner *Ex Officio* Jonathan Wroblewski
Ken Cohen, General Counsel
Judith M. Sheon, Staff Director
Kathleen Grilli
Michael Courlander, Public Affairs Officer