

IDENTITY THEFT
Martin Richey, AFPD, D. Mass.
Martin.Richey@fd.org

October 2010

I. Overview

Identity theft, broadly defined, is the fraudulent use of another person's identifying information ("means of identification") in connection with some underlying crime.

Congress has passed two statutes that criminalize identity theft. In 1998, Congress enacted the Identity Theft and Assumption Deterrence Act, which set forth the substantive offense of identity theft at 18 U.S.C. § 1028(a)(7). That provision prohibits the use of another person's identifying information in connection with any federal crime or any state or local felony. The maximum penalty for violating § 1028(a)(7) is 15 years imprisonment if the value obtained exceeded \$1,000 over a one-year period.

When Congress enacted 18 U.S.C. § 1028(a)(7), it also directed the United States Sentencing Commission to incorporate the crime of identity theft into the Sentencing Guidelines. The Commission's primary response to this directive was to add a two-level enhancement in the fraud and theft guideline (at U.S.S.G. § 2B1.1(b)(10)(C)(I) and (ii)) for cases that involve identity theft in certain circumstances. Thus, fraud and theft offenses involving identity theft may receive an increased punishment by operation of the Sentencing Guidelines, regardless of whether the defendant is charged with a substantive count under 18 U.S.C. § 1028(a)(7).

In 2004, Congress enacted a second identity theft statute: 18 U.S.C. § 1028A, entitled "Aggravated Identity Theft." Section 1028A(a)(1) prohibits identity theft in connection with certain enumerated federal crimes. Section 1028A(a)(2) prohibits identity theft, or the use of a false identification document, in connection with terrorism offenses.

Although Congress entitled § 1028A "Aggravated Identity Theft," the elements of § 1028A(a)(1) are identical to those of § 1028(a)(7), except that § 1028A(a)(1) is triggered by a nominally narrower range of underlying predicate offenses.¹ However, that range of underlying offenses (enumerated at § 1028A(c)) is actually quite broad, and includes many federal fraud and immigration offenses. Therefore § 1028A(a)(1) does not apply to "aggravated" forms of identity theft in any meaningful sense. Rather, the "aggravated" aspect of § 1028A(a)(1) is the prescribed penalty: a **two-year mandatory sentence**, which must be served **consecutively** to the sentence for the underlying offense. See 18 U.S.C. § 1028A(b).

¹

Indeed, the Eleventh Circuit has held that double jeopardy bars prosecution under *both* § 1028(a)(7) and § 1028A(a)(1) where the two counts charge the same underlying predicate offense and the misuse of the same means of identification. See *United States v. Bonilla*, 579 F.3d 1233 (11th Cir. 2009).

Congress has then provided prosecutors with a powerful weapon that may now be used, at the government's discretion, in identity theft cases. Legal challenges to § 1028A prosecutions have proven difficult, with a couple of notable exceptions discussed below. The most effective defense advocacy in § 1028A cases may well be to persuade the prosecutor to dismiss any § 1028A count(s) in return for a plea to the underlying offense, and the more modest sentence enhancement that may apply under the Sentencing Guidelines.

II. 18 U.S.C. § 1028A – “Aggravated Identity Theft”

A. Elements of the offense

18 U.S.C. § 1028A(a)(1) provides:

Whoever, during and in relation to any felony enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

1. “Means of identification of another person” defined

Identity theft is the fraudulent or deceptive use of another person's identifying information. In the language of the statutes (and the Sentencing Guidelines), a person's identifying information is called a “means of identification.” For purposes of both § 1028A and § 1028(a)(7), “means of identification” is defined at 18 U.S.C. § 1028(d)(7) as follows:

the 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)).

The lists in subsections (A) - (D) are illustrative, not exhaustive. The most important part of the statutory definition appears in the first paragraph. Simply put, a “means of identification” is “any name or number that may be used to identify a specific individual.” Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 Cornell J.L. & Pub. Pol’y 661 (Spring 1999).

a. “Person” means real person, but may include deceased persons.

Both 18 U.S.C. §§ 1028A(a)(1) and § 1028(a)(7) only reach the fraudulent use of a means of identification that belongs to a real person. See, e.g., United States v. Jimenez, 507 F.3d 13, 20 (1st Cir. 2007). Courts have held that a “real person” includes a deceased person. See United States v. LaFaive, 2010 WL 3239392 (7th Cir. Aug. 18, 2010); United States v. Maciel-Alcala, 598 F.3d 1239 (9th Cir. 2010); United States v. Kowal, 527 F.3d 741 (8th Cir. 2008); United States v. Jimenez, 507 F.3d at 22 (1st Cir. 2007).

b. Does “person” include a business or corporate entity?

At least one district court has held that the term “person” includes a business or corporate entity. See United States v. Hilton, 2010 WL 2926055, slip opinion, at *3 (W.D.N.C. 2010).

c. The means of identification must identify a specific individual.

While the definition at 18 U.S.C. § 1028(d)(7) is broad, it does have limits. In United States v. Mitchell, 518 F.3d 230 (4th Cir. 2008), the court held that the statutory definition “allows for an identifier, taken alone or together with other information, to qualify as a means of identification so long as the sum total of information identifies a specific individual.” Mitchell involved a counterfeit check scheme, wherein the defendant bought merchandise with counterfeit checks, then later returned the merchandise for cash. When paying by check, the defendant presented a false Georgia driver’s license that he created in the name of “Marcus Jackson.” The driver’s license also contained an address and a date of birth. In fact, the Georgia department of motor vehicles had issued licenses to two individuals named Marcus Jackson, one of whom – Marcus Deyone Jackson – lived in the same town (East Point, GA) and had the same year of birth as appeared on the false license. The government claimed that this information was sufficient to identify a specific individual (Marcus Deyone Jackson from East Point, GA).

The Fourth Circuit disagreed. The court emphasized a distinction between “unique identifiers,” such as a government-issued driver’s license number (or social security number, A-number, and the like) and “non-unique” identifiers, such as first and last name, city of residence, and year of birth. A unique identifier “identifies a ‘specific individual for purposes of § 1028A(a)(1).” (The number on the false driver’s license in this case was wholly fictional). See also United States v. Melendrez, 389 F.3d 829, 830 (9th Cir. 2004) (real Social Security numbers used alone or in conjunction with other information constitute a means of identification because they can be used to uniquely identify specific persons). Non-unique identifiers, on the other hand, may be too general to identify a specific person. Such was the case in Mitchell: (1) “Marcus Jackson” was not an exact match with “Marcus Deyone Jackson,” the individual from East Point; (2) though Marcus Deyone

Jackson lived in East Point, he did not live at the address given on the false license; and (3) though Marcus Deyone Jackson had the same year of birth as that on the false license, he had a different month and date of birth.

d. Forged signatures.

In United States v. Blixt, 548 F.3d 882, 887-88 (9th Cir. 2008), the Ninth Circuit held that a forged signature constituted a “means of identification.” The defendant in Blixt forged her supervisor’s name on company checks in the midst of a fraudulent scheme. The court held that the signature was a “name” within the meaning 18 U.S.C. § 1028(d)(7)(A). When considering Blixt it is important to keep in mind that, in context, the signature there identified a specific individual: the supervisor who was otherwise authorized to sign the checks. If, in context, the forged signature did not identify a specific (and real) individual, the signature would not be a “name” within the meaning of 18 U.S.C. § 1028(d)(7)(A).

NOTE: In United States v. Griffiths, 4:10-CR-3 (N.D.Fla. July 1, 2010), the court granted a judgment of acquittal on a count of aggravated identity theft in connection with bank fraud, where the evidence established that stolen checks with forged signatures were deposited into bank accounts, and funds subsequently withdrawn. The court relied on the fact that a “means of identification,” as defined at § 1028(d)(7)(D), includes access devices as defined in 18 U.S.C. § 1029(e). Section 1029(e) specifically excludes from the definition of access device “a transfer originated solely by paper instrument.” The court reasoned that passing bad checks therefore cannot constitute identity theft.

2. The *knowing* transfer, possession, or use of a means of identification of another person

a. Flores-Figueroa: The government must prove that the defendant knew that the means of identification at issue belonged to another person

Although the law requires that the means of identification belong to a real person, a circuit conflict developed regarding whether a defendant had to *know* that it belonged to a real person.

The statutes penalize anyone who “knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person.” The issue was whether “knowingly” applies just to the transfer, possession, or use; or to the transfer, possession, or use of a means of identification; or to the transfer, possession, or use of a means of identification of another person. In Flores-Figueroa v. United States, 129 S.Ct. 1886 (2009), the Supreme Court held that an ordinary reading of the text showed that the word “knowingly” extends to all the subsequently listed elements of the crime, and therefore that “§ 1028A(a)(1) requires the government to show that the defendant knew that the means of identification at issue belonged to another person.” Id. at 1894.

The defendant in Flores-Figueroa began working in 2000 under a false name, social security number, and A number. The social security and A numbers were wholly fictional and had been assigned to no one. In 2006, the defendant presented his employer with a social security card and a green card in his true name, with different social security and A numbers than he had used before. The employer reported the defendant to ICE, who determined that the social security and A numbers had in fact been issued to real people.

In its discussion, the Supreme Court addressed the government's argument regarding the practical difficulty in proving beyond a reasonable doubt that a defendant had the requisite knowledge. The Court posited an example similar to the facts at bar: an illegal immigrant offers an employer identification documents that in fact belong to others. The Court said that in such a case, the government may be able to prove the defendant knew the identification was real, but perhaps not because in fact the defendant did not care whether the papers were real or counterfeit. While recognizing the difficulty proving knowledge may pose in such circumstances, the Court found the concern insufficient to overcome the ordinary meaning of the statute. The Court emphasized that intent is generally not difficult to prove in a "classic case of identity theft," which the Court characterized as follows:

For example, where a defendant has used another person's identification information to get access to that person's bank account, the Government can prove knowledge with little difficulty. The same is true when the defendant has gone through someone else's trash to find discarded credit card and bank statements, or pretends to be from the victim's bank and requests personal identifying information. Indeed, the examples of identity theft in the legislative history (dumpster diving, computer hacking, and the like) are all examples of the types of classic identity theft where intent should be relatively easy to prove, and there will be no practical enforcement problem.

Flores-Figueroa, 129 S.Ct. at 1893. The Court further said that "to the extent that Congress may have been concerned about criminalizing the conduct of a broader class of individuals, the concerns about practical enforceability are insufficient to outweigh the clarity of the text." Id.

b. Cases involving the "knowledge" element post-Flores-Figueroa

In United States v. Grajeda-Gutierrez, 372 Fed.Appx. 890 (10th Cir. 2010) (unpublished), the defendant presented a false name and social security number, and falsely claimed to be a lawful permanent resident, in completing an I-9 form. (In support, the defendant presented her employer with a fake green card and license). While upholding her conviction for making a false statement on the I-9 form (a violation of 18 U.S.C. § 1546(a)), the Tenth Circuit, applying Flores-Figueroa and with the government's concession, found the evidence insufficient to prove that the defendant knew the name and social security number she used belonged to a real person.

A troubling trend is developing in the Eleventh Circuit, where the court has held that subjecting identification to government scrutiny (e.g., to the registry of motor vehicles to obtain a license or identification, or to the State Department to obtain a passport) and/or presenting identification to obtain a line of credit is sufficient circumstantial evidence to establish that the defendant knew the identity belonged to a real person. See United States v. Gomez-Castro, 605 F.3d 1245 (11th Cir. 2010); United States v. Holmes, 595 F.3d 1255 (11th Cir. 2010).²

3. The knowing transfer, possession, or use of a means of identification of another person *without lawful authority*

What if the defendant claims that he or she had permission to use the other individual's means of identification?

As a general matter, the Eleventh Circuit has held that the government does not have to prove that the means of identification was actually *stolen* in order to establish that it was used "without lawful authority." See United States v. Hurtado, 508 F.3d 603, 607-08 (11th Cir. 2007). In Hurtado, the defendant used another person's birth certificate and driver's license in applying for a U.S. passport. Relying upon the legislative history and title § 1028A ("Aggravated identity *theft*"), the defendant argued that the statute was aimed at individuals who stole identities, not to those who commit simple passport fraud, and that in order to establish that the identification was used without lawful authority, the government had to prove that the identification was stolen by the defendant. Without defining the full scope of the term "without lawful authority," the court said:

For sure, stealing and then using another person's identification would fall within the meaning of "without lawful authority." However, there are other ways someone could possess or use another person's identification, yet not have "lawful authority" to do so. There is no dispute here that Hurtado did not have any authority, much less lawful authority, to use Colon's identification. We need not attempt to define every situation where transfer, possession, or use of a means of identification would be "without lawful authority." It is clear that the plain language of this phrase indicates Congress's intent to prohibit more than just the defendant's transfer, possession, or use of identification that was obtained by theft by that defendant.

Id. at 607.

2

See also United States v. Iyamu, 2010 WL 3279156, *6 (11th Cir. Aug. 20, 2010) (unpublished)(citing Holmes and holding evidence of knowledge sufficient where defendant submitted names and correctly corresponding social security numbers to obtain credit cards); United States v. Ehrlich, 2010 WL 2508898, *3 (11th Cir. June 23, 2010) (unpublished) (affirming conviction where defendant "used his victim's identification to obtain fairly large amounts of credit on various occasions.").

Similarly, in United States v. Abdelshafi, 592 F.3d 602 (4th Cir. 2010), the Fourth Circuit held that the means of identification need not have been “misappropriated.” The defendant in Abdelshafi provided transport for medicaid patients. He received a daily trip log, which contained patients’ identifying information including Medicaid identification numbers. The defendant used these numbers to submit fraudulent claims for non-existent trips, or trips with inflated mileage. He was charged with health care fraud and aggravated identity theft.

Against the defendant’s argument that because he had been given the Medicaid numbers, he did not act “without lawful authority,” the court said that “‘nothing in the plain language of the statute requires that the means of identification’ at issue ‘must have been stolen;’– or as Abdelshafi characterizes the point ‘misappropriated’– ‘for a § 1028A(a)(1) violation to occur.’” Abdelshafi, 592 F.3d at 607 (quoting Hurtado, 508 F.3d at 607). Put simply, “The statute prohibits an individual’s knowing use of another person’s identifying information without a form of authorization recognized by law.” Abdelshafi, 592F.3d at 609. See also United States v. Mobley, 2010 WL3340364, *6 (6th Cir. August 25, 2010)(“That a defendant’s use of any social security number . . . to submit a fraudulent credit card application must be ‘without lawful authority’ is obvious”); United States v. Hines, 472 F.3d 1038, 1039-40 (8th Cir. 2007)(defendant who provided false name and social security number at arrest acted “without lawful authority,” even though he testified that he had traded drugs and money for permission to use the information).

4. During and in relation to any felony enumerated in subsection (c)

In order to violate 1028A(a)(1), the identity theft must have occurred “during and in relation to any felony violation enumerated in subsection (c),” which provides a laundry list of predicate federal offenses.

There is little case law interpreting the phrase “during and in relation to” in the context of 18 U.S.C. § 1028A(a)(1). However, upon the government’s concession, the Fifth Circuit has reversed a conviction under this provision. In United States v. Ekwuruke, 372 Fed.Appx. 521 (5th Cir. April 7, 2010) (unpublished), the defendant was a temporary employee of Bank of America, which had contracted to receive and process tax payments on behalf of the IRS. The defendant stole checks during his employment and was charged with theft of bank funds and theft of government funds. He was also charged with aggravated identity theft – the predicate offense being the theft of bank funds – in connection with his altering and depositing one of the stolen checks. Because the check deposit occurred after his employment with Bank of America had ended, the government conceded on appeal that the identity theft was not “during and in relation to” the theft of bank funds.³

One district court has interpreted the phrase “during and in relation to” quite broadly. In United States v. Guillen-Perez, 2007 WL1455823 (N.D. Fla. May16, 2007), an alien defendant was arrested by local police for a battery offense. During his arrest, the defendant gave a false name that corresponded to a fraudulent social security card he was carrying. In a subsequent federal prosecution for illegal re-entry and aggravated identity theft, the defendant challenged § 1028A(a)(1) on the

3

These facts are gleaned from the appellate briefs.

grounds that the phrase “in relation to” is too vague. The court rejected the challenge, and in doing so said that the defendant’s possession of the fraudulent social security card was “in relation to” the crime of re-entry, since the defendant gave the name on the social security card at his arrest to avoid being correctly identified. (The defendant was subsequently acquitted by a jury of the aggravated identity theft charge).

B. Penalties

1. Statutory provisions

The statutory penalty for violating 18 U.S.C. § 1028A(a)(1) is a two-year mandatory sentence that must be served **consecutively** to the sentence for the underlying offense. Moreover, the statute expressly prohibits a reduction in the sentence for the underlying offense “to compensate for, or otherwise take into account” the harsh effect of the mandatory penalty. 18 U.S.C. § 1028A(b)(3). See, e.g., United States v. Omole, 523 F.3d 691, 699 (7th Cir. 2008). Note, however, that a court is not precluded from taking § 1028A’s mandatory sentence into account in sentencing a defendant on other counts of conviction charged in the same indictment that are not predicate felonies underlying the § 1028A conviction. United States v. Vidal-Reyes, 562 F.3d 43 (1st Cir. 2009).

Sentences for *multiple* counts under § 1028A(a)(1) may be imposed to run concurrently with each other. See 18 U.S.C. § 1028A(b)(4). The court is instructed to consult the Sentencing Guidelines when determining whether to impose multiple § 1028A sentences consecutively or concurrently with one another. *Id.*; see also U.S.S.G. § 5G1.2, comment. (n.2(B)) (enumerating factors court should consider when imposing sentence for multiple counts of conviction under 18 U.S.C. § 1028A).

2. Sentencing Guidelines

The Sentencing Commission created a new guideline – U.S.S.G. § 2B1.6 – for counts brought under the aggravated identity theft statute. Under U.S.S.G. § 2B1.6, the sentence is the two-year mandatory, which is to be applied consecutively to the sentence for the underlying offense. Application Note 2 to U.S.S.G. § 2B1.6 directs that if a sentence for § 1028A is imposed in conjunction with a sentence for an underlying offense, the guideline identity theft enhancement at U.S.S.G. § 2B1.1(b)(10)(C)(I) and (ii) (see below) is not applied to the underlying offense.

III. The Sentencing Guideline Enhancement For Identity Theft in Non- § 1028A Prosecutions: U.S.S.G. § 2B1.1(b)(10)(C)(I) and (ii)

If a defendant is not charged under the Aggravated Identity Theft section (18 U.S.C. § 1028A), but the underlying facts of the case include conduct that constitutes identity theft, the defendant may be subject to the identity theft enhancement set forth at U.S.S.G. § 2B1.1(b)(10)(C)(I) and (ii).

A. The concept of “affirmative identity theft,” or “breeding” documents

Identity theft can be committed in very simple form. For example, if a defendant steals a credit card and uses it to pay for goods and services, she has committed “identity theft”: she has used a means of identification (the credit card account number and/or the cardholder’s name) in connection with the crime of credit card fraud.

A more complicated form of identity theft is committed when a defendant takes a means of identification and “breeds” it, *i.e.*, creates another means of identification from the first means of identification. Assume, for example, that the above defendant uses the information from the credit card (for example, the credit card account number) to apply for an additional credit card. The defendant has committed affirmative identity theft; she has “bred” a new means of identification (the new credit card account number) from the old means of identification (the stolen credit card account number). This aggravated form of identity theft arguably causes more harm: new lines of credit may be opened in a victim’s name, affecting her credit report without her knowledge.

When faced with the directive to incorporate the crime of identity theft into the Guidelines, the Sentencing Commission chose to focus on this more aggravated form of identity theft rather than on the simpler form:

Subsection (b)(10)(I) implements the directive to the Commission in section 4 of the Identity Theft and Assumption Deterrence Act of 1998, Public Law 105- 318. This subsection focuses principally on an aggravated form of identity theft known as “affirmative identity theft” or “breeding,” in which a defendant uses another individual’s name, social security number, or some other form of identification (the “means of identification”) to “breed” (*i.e.*, produce or obtain) new or additional forms of identification. Because 18 U.S.C. § 1028(d) broadly defines “means of identification,” the new or additional forms of identification can include items such as a driver’s license, a credit card, or a bank loan. This subsection provides a minimum offense level of level 12, in part because of the seriousness of the offense. The minimum offense level accounts for the fact that the means of identification that were “bred” (*i.e.*, produced or obtained) often are within the defendant’s exclusive control, making it difficult for the individual victim to detect that the victim’s identity has been “stolen.” Generally, the victim does not become aware of

the offense until certain harms have already occurred (e.g., a damaged credit rating or an inability to obtain a loan). The minimum offense level also accounts for the non-monetary harm associated with these types of offenses, much of which may be difficult or impossible to quantify (e.g., harm to the individual's reputation or credit rating, inconvenience, and other difficulties resulting from the offense). The legislative history of the Identity Theft and Assumption Deterrence Act of 1998 indicates that Congress was especially concerned with providing increased punishment for this type of harm.

U.S.S.G. § 2B1.1, comment.(backg'd).

Thus, the Guidelines provide the following enhancement in the fraud and theft guideline at § 2B1.1(b)(10)(C):

(10) If the offense involved . . . (C)(I) the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification, or (ii) the possession of 5 or more means of identification that unlawfully were produced from, or obtained by the use of, another means of identification, **increase by 2 levels**. If the resulting offense level is less than level 12, **increase to level 12**.

This enhancement applies where the defendant bred the original means of identification to obtain additional means of identification, or possessed 5 or more bred means of identification. The enhancement does not apply to the most basic forms of identity theft (for example, using a stolen credit card or forging a signature on a stolen check).

As with the substantive offense of identity theft itself, the means of identification must belong to a real person (see U.S.S.G. § 2B1.1, comment. (n.9(A)), and the burden is on the government to establish proof of that fact. See, e.g., United States v. Hines, 449 F.3d 808 (7th Cir. 2006) (district court's application of enhancement reversed where prosecution failed to offer evidence that Social Security number had been issued to a real person).

Note, however, that the means of identification subsequently obtained need not be in the victim's name. See United States v. Melendrez, 389 F.3d 829, 830 (9th Cir. 2004) (enhancement properly applied where the defendant created false social security cards and army forms using stolen social security numbers but fake names: "Those nine digits tied the victims to the identification documents, regardless of the names with which the Social Security numbers were paired.").

IV. Miscellaneous Sentencing Guideline Issues

Practitioners should be aware of the following additional sentencing guideline issues. These issues may arise in non- § 1028A cases, or in the guideline calculation for an underlying offense charged in conjunction with § 1028A.

A. Upward departure encouraged in egregious cases: U.S.S.G. § 2B1.1, Application Note 19(A)(vi)

At Application Note 19 to U.S.S.G. § 2B1.1, the Commission notes that an upward departure may be warranted in an identity theft case where:

- substantial harm was done to the victim's reputation or credit record, or the victim suffered substantial inconvenience related to repairing reputation or credit record;
- the victim was erroneously arrested, or denied a job based on an erroneous arrest record; or
- the defendant obtained numerous means of identification with respect to one individual, and essentially assumed that individual's identity.

This departure language was added prior to the enactment of 18U.S.C. § 1028A. One should argue that if the government proceeds under § 1028A, the consecutive mandatory provides sufficient punishment, and an upward departure with respect to any underlying offense is unwarranted.

B. Enhancement for abuse of position of trust

If the defendant obtained access to the means of identification by exceeding or abusing the authority of his or her employment position, the "abuse of position of trust" enhancement may apply to guideline calculation of the underlying offense. See U.S.S.G. § 3B1.1, comment. (n.2(B)).

C. Enhancement for number of victims

Under U.S.S.G. § 2B1.1(b)(2), enhancements are prescribed if the offense involved 10 or more victims (2-level enhancement), 50 or more victims (4-level enhancement), or 250 or more victims (6-level enhancement).

Application Note 4(E) to U.S.S.G. § 2B1.1 now explicitly provides that in cases involving means of identification, the definition of "victim" includes "any individual whose means of identification was used unlawfully or without authority." Note 4(E) was added by amendment effective November 1, 2009.

Prior to this amendment, courts were divided on whether an individual whose means of identification was taken and used but who was reimbursed by a third party (e.g., a bank or credit card company) was a victim for purposes of § 2B1.1(b)(2). See United States v. Kennedy, 554 F.3d 415

(3d Cir. 2009) (discussing cases).⁴

V. Restitution

Title 18 U.S.C. § 3663(b)(6) permits restitution for time spent by the victim to remediate the harm resulting from the offense (e.g., to repair damage done to a credit report).

4

Prior to the amendment, a “victim” was defined as someone who suffered actual loss. See Application Note 1 (“Definitions”) to U.S.S.G. § 2B1.1. Actual loss is defined as reasonably foreseeable pecuniary harm. U.S.S.G. § 2B1.1, comment. (n.3(A)(I)). Pecuniary harm is defined as monetary harm, and does not include emotional distress, harm to reputation, or other non-economic harm. U.S.S.G. § 2B1.1, comment. (n.3(A)(iii)).