

**Identity Fraud**  
**Western District Bankruptcy Seminar**  
**May 6, 2016**

**I. Introduction**

Identity Theft is a different type of crime and has a different type of impact on the victims

-If the theft occurs from a database breach, whether it be by an insider or an intruder, the victim will have no means of learning about the theft until informed by some third party

-If it occurs from a simple computer intrusion, the victim will usually learn of the theft only when the thief uses the information.

-If it occurs from the theft of unsolicited mail (such as pre-approved credit card solicitations) difficult to detect because only unsolicited mail is stolen.

-If it occurs from the theft of garbage and recycling material, whether it be residential or commercial ("dumpster diving"), it is difficult to detect unless someone witnesses the theft.

-If it is taken by a pretexter (someone who obtained the information under false pretenses), the victim usually learns of the theft only after the information is used by the thief.

-If identification information is surreptitiously stolen by a skimmer (an electronic device which downloads credit/debit card information), the victim usually learns of the theft only after the information is used by the thief

**II. Identity theft: the nature of the problem**

Identity theft has a huge economic impact upon society. In the United States alone, identity theft results in approximately \$50 billion in annual losses to businesses and consumers. Rachel Kim et al., *2007 Identity Fraud Survey Report*, Javelin Strategy & Research, 1 (Feb. 2007). The primary challenge is that identity information exists everywhere, from wallets to the Internet, to the amorphous digital data repositories on servers around the globe.

Identity theft is simply the theft of information that identifies a specific individual—a name, date of birth, social security number (SSN), driver's license number, or financial account number, among others. It generally becomes a federal crime when the possession, transfer, or use of the information that identifies a specific individual is transported in or otherwise affects interstate commerce.

-in our digital environment, the possession, transfer, or use of the information often affects interstate commerce.

The Social Security Number is a fundamental element of almost every identity theft case. Congress recognized that disclosure of the SSN is a threat to individual privacy and enacted the Privacy Act in 1974 to deal with misuse and unnecessary disclosure of the SSN. Enacted express restrictions on the use of the SSN. Privacy Act, Pub. Law No. 93-579, 88 Stat. 1896 (1974).

-At one time required to have SSN printed on personal checks

Means of identification Includes 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 to identify. 18 U.S.C. § 1028(d)(7).

A signature is a means of identification

-"[A]nother's name in the form of a signature is [included in] the definition of 'means of identification.'" Quoting from *United States v. Blixt*, 548 F.3d 882, 887 (9th Cir. 2008).

- means of identification is equivalent to a signature on a check, whether the signature is a real signature or a forgery. See *United States v. Mello*, 2010 WL 358892 (WD VA 2010).

-“a signature is a form of “name” for purposes of § 1028(d)(7)'s definition of “means of identification.” *United States v. Porter*, 2014 WL 868791 (10th Cir. 2014).

-“Williams argues that, in the absence of record evidence of legibility, no evidence shows that the **signature** identified a specific person. But a copy of the check (attached to the plea agreement) shows a legibly written “Neda D. Stephens” as signatory for “Oral & Maxillofacial Surgical Specialists, P.C.” (R. 513, Plea Agreement at 10.) The employee's signature and place of employment identified her, specifically.” 2014 WL 278432 (6<sup>th</sup> Cir 2014) unpublished

But the name must identify a particular person. *United States v. Mitchell*, 518 F.3d 230, 233-35 (4th Cir. 2008) (reversing a § 1028A conviction because of insufficient evidence that a fake driver's license with the name "Marcus Jackson" identified as specific Marcus Jackson). And while the name must identify a particular person, it can do so "alone or in conjunction with any other information." *Id.*

Several circuits have held that a willingness to "test" the means of identification by submitting it to a verification process is proof of knowledge. See, e.g., *United States v. Foster*, 740 F.3d 1202, 1207 (8th Cir. 2014) (holding that willingness to

use identifying information with lenders is circumstantial proof of knowledge); *United States v. Valerio*, 676 F.3d 237, 244-45 (1st Cir. 2012) (subjecting identifying information to government scrutiny evidence of knowledge); *United States v. Doe*, 661 F.3d 550, 562-64 (11th Cir. 2011) .

### III. Prosecution

#### Identity Fraud (18 USC § 1028)

When Congress enacted the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act), a new offense of identity theft was created. See S. Rep. No. 105-274 (1998). Prior to enactment of the Identity Theft Act, 18 U.S.C. § 1028 addressed only the fraudulent creation, use, or transfer of identification documents and did not address the theft or criminal use of an individual's personal information. With the addition of § 1028(a)(7), Congress intentionally expanded the definition of "means of identification" to include a person's SSN. Congress clearly intended requires proof that a defendant's transfer or use of a means of identification of another person was in or interstate or foreign commerce, or the means of identification was transported in the mail in the course of the transfer or use.

18 U.S.C. § 1028A (Aggravated Identity Theft). Mandatory term of imprisonment of 2 years, consecutively to any other sentence

#### Elements of the Offense

- 1) defendant knowingly possessed or used, without lawful authority, a means of identification of another person and
- 2) that the possession or use of the means of identification of another person was during and in relation to the commission of an enumerated felony
- 3) Enumerated felonies are 18 U.S.C. § 641 (theft of public money); 18 U.S.C. § 656 (theft or embezzlement by bank officer or employee); 18 U.S.C. § 664 (theft from employee benefit plans); 18 U.S.C. § 911 (false impersonation of citizenship); 18 U.S.C. § 922(a)(6) (false statements in connection with the acquisition of a firearm); 18 U.S.C. § 1001 (fraud and false statements); 18 U.S.C. § 1341, 1343, 1344 (mail, wire and bank fraud); 18 U.S.C. § 1542-1546 (nationality and citizenship; passports and visas).

Means of Identification, includes: Name; SSN; DOB; Driver's license; Alien registration number; Passport number; Employer or taxpayer identification number; Unique biometric data; Unique electronic identification number; Address, or routing code; or telecommunication identifying information or access device (e.g., credit card or financial account number). 18 U.S.C. § 1028(d)(7)

The government can establish that the defendant acted “without lawful authority” in violation of 18 U.S.C. § 1028A(a)(1) in any number of ways; the element does not require the government to prove specifically that the means of identification was stolen, misappropriated, or misrepresented by the defendant. Thus, even though the defendant had lawful authority to use Medicaid patients' identifying information for proper billing purposes, his use of the patients' information to submit fraudulent billing claims was without legal authority. *United States v. Abdelshafi*, 592 F.3d 602 (4th Cir. 2010), cert. denied, 131 S. Ct. 182 (2010).

-However the Supreme Court ruled that a violation of 18 USC Section 1028 requires that the Government show that the Defendant knew that the means of identification belonged to another person *Flores-Figueroa v. United States*, 556 U.S. 646 (2009)

-deceased persons can be victims

#### **IV. An Ever Expanding Frontier-Stolen Identity Refund Fraud Cases (SIRF)**

-use stolen SSN to file false tax return for refund

SIRF schemes generally exploit two aspects of the tax system:

1. The IRS does not receive information on tax withholdings until later in the year, allowing fraudsters to create fictitious W-2 forms with fake tax withholdings.

2. "Refundable" credits, such as the earned income tax credit, education credits or fuel credits do not require persons to have had taxes withheld before they can receive a tax refund.

Department of Justice has streamlined the review process for SIRF cases

#### **V. The Practical Effect and Elder Fraud**

American Association of Retired Persons (AARP) highlighted characteristics of people older than 50 that make them easy targets for financial abuse.

-In general: expect honesty in the marketplace, are less likely to take action when defrauded, and are less knowledgeable about their rights in an increasingly complex marketplace.

-more likely to be home than their younger neighbors, they are often within easy reach of devious telemarketers and home solicitors.

Scammers target elders that they perceive to be vulnerable -- those that are isolated, lonely, physically or mentally disabled, unfamiliar with handling their own finances, or have recently lost a spouse.

-pose as trustworthy helpers

- May obtained paperwork that appears to give them legal authority to act -- including powers of attorney, authorizing signature cards, and vehicle pink slips.
- Some work at a bank or other financial institution and have intricate ways of hiding their tracks by manipulating electronic records and such.

Many elderly victims do not report fraud because they feel ashamed, or they fear others will think they cannot care for themselves, which may trigger placement in a nursing home or long-term care facility. Significantly, many victims are not aware of support resources or do not know how to access them. In the case of financial exploitation, many victims have close ties to the offender and may feel protective. They may want to stop the exploitation and recover their assets, but not want the offender punished. In addition, many victims believe they are at least partially to blame. *United States v. Martin*, 455 F.3d 1227, 1240 (11<sup>th</sup> Cir. 2006)

## **VI. Court Filings**

In 2009 E-Government Act of 2002 (P.L. 107-347, Title II, § 205) requires all federal courts to make their electronic filings available to the general public online.

Provision applies to virtually all documents filed in federal court — greatly increasing the risk that sensitive information is inadvertently published.

To safeguard against the publication of individuals' sensitive information, the E-Government Act broadly directed the federal judiciary to adopt uniform rules to protect sensitive information contained in court filings. Effective December 1, 2007, to the Federal Rules of Appellate Procedure (Rule 25), Civil Procedure (Rule 5.2), Criminal Procedure (Rule 49.1), and new Bankruptcy Rule 9037 require parties to redact specific categories of information from all filings, including Social Security and taxpayer identification numbers (except for the last four digits), all names of minor children (except for initials), all financial account numbers (except for the last four digits), all dates of births for persons (except for the year of birth), and in criminal cases, all home addresses (except for the city and state).

Weakness of safeguard depends solely on the conscientiousness of whomever is filing the documents to identify, and then redact, the sensitive information.

- whether an attorney or layperson with no legal background.

- not only parties effected, but non-parties as well

## VII. What To Do

- Do not give out SSN
- Check credit reports
- Observe unusual activity when using cards
- Create strong passwords that mix 10 or more letters, numbers and special characters.
  - Don't use the same password for more than one account.
  - Use anti-virus software, anti-spyware software, and a firewall on your computer.
- If asked for ID information and do not know personally know the person say **GOODBYE**
- Review accounts routinely
- If traveling take care of mail and paper to avoid leaving ID docs
  - tell credit card company and bank
  - stop mail or have some pick it up from the mail box each day
- Save Facebook, Twitter, etc postings to general public until return

If believe identity stolen

- Contact law enforcement (important to know the how and when) including Internal Revenue Service, Federal Trade Commission, Department of Motor Vehicles, Federal Bureau of Investigation, United Postal Service, United States Postal Service, local Police Department
- Contact financial institution
- Federal Court can order restitution "to the victims of the offense" (18 USC § 3572)
  - based upon the actual loss incurred by the victim

Theft Enforcement and Restitution Act, Pub. Law 110-326, 122 Stat. 3560 (signed into law September 26, 2008)

Provides that restitution orders for identity theft cases may include an amount equal to the value of the victim's time spent remediating the actual or intended harm of the identity theft or aggravated Identity theft offense