**March**
**2008**
**Volume 56**
**Number 2**

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

Kenneth E. Melson
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

**Managing Editor**
Jim Donovan

**Program Manager**
Nancy Bowman

**Internet Address**
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Program Manager, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201.

# Identity Theft

## In This Issue

# Identity Theft: The Scope of the Problem

*Jonathan J. Rusch*
*Deputy Chief*
*Fraud Section*
*Criminal Division*

## I. Introduction

Identity theft is considered to be one of the most pervasive forms of white-collar crime in the United States. According to an October 2006 survey by Javelin Strategy & Research, more than 8.4 million U.S. adults were victims of identity theft in the preceding year. Rachel Kim et al., *2007 Identity Fraud Survey Report*, JAVELIN STRATEGY & RESEARCH, Feb. 2007, at 1, *abbreviated version available at* http://www.acxiom.com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Report-627200734724.pdf. While this crime takes many forms—from local vehicle break-ins and trash theft (*see, e.g., United States v. Gonzales*, 7:04 CR021-R (N.D. Tex., Oct. 21, 2005), to international Web sites gathering personal data (*see* Press Release, Sophos, The Italian Job: 26 arrested for Poste Italiane phishing attack (July 16, 2007)) (on file with author), *available at* http://www.sophos.com/pressoffice/news/articles/2007/07/italian-phish.html.—"it invariably leaves victims with the task of repairing the damage to their lives." President's Identity Theft Task Force, *Combating Identity Theft: a Strategic Plan,* PRESIDENT'S IDENTITY THEFT TASK FORCE, Apr. 2007, at 1, *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

## II. Types of harm from identity theft

### A. Financial harm

In the aggregate, victims of identity theft suffer substantial losses. Estimates of aggregate losses due to identity theft vary, but the President's Identity Theft Task Force stated that "the data show that annual monetary losses are in the billions of dollars." *Id.* at 11. The 2006 Javelin Research survey found that losses to businesses and others due to identity fraud totaled $56.6 billion. Rubina Johannes et al., *2006 Identity Fraud Survey Report*, JAVELIN STRATEGY & RESEARCH, Jan. 2006, note 1, at 1.

There are many ways in which victims of identity theft may suffer direct financial harms, varying with the types of information that identity thieves obtain and the ways in which that information is used. These include misuse of their existing credit cards and debit card accounts, opening new accounts (including credit or debit card, loan, and utilities) by criminals, issuance of government benefits or services in the victims' names to unqualified individuals, and purchases of motor vehicles and other valuable items with the victims' funds or credit. *See, e.g.,* Federal Trade Comm'n, *Take Charge: Fighting Back Against Identity Theft*, Feb. 2006, *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.

Victims generally are not liable for debts that identity thieves create in their names. If the misuse involves a consumer's existing credit card account, it can be relatively easy for the consumer to remedy the situation by calling the card issuer, reporting the fraudulent transactions, and providing supporting information. If the misuse involves a consumer's existing debit card or checking account, the victim should ultimately be able to have the fraudulently obtained funds restored to the account, pending resolution of the claim by the financial institution. The consumer, however, may be temporarily deprived of access to those funds. In addition, in cases involving creation of new credit card accounts, the victim

may not learn of the identity theft until a creditor or debt collector contacts him or her. That contact may not take place until after the identity thief has already used those accounts and amassed substantial debt in the victim's name.

Unfortunately, victims may have to spend hundreds, if not thousands, of dollars recovering from the crime. Expenses may include notary fees, certified mailings, hiring of counsel, and lost income. Nonfinancial losses, such as lost time spent correcting credit reports, disputing fraudulent accounts, and obtaining new identity documents, also can be substantial, as described below.

Although many cases of identity theft involve smaller amounts of money, ranging from a few dollars to a few hundred dollars, other identity thefts can lead to more substantial losses. The 2006 Javelin Strategy survey found that, while the *median* fraud amount per victim was $750, the *mean* fraud amount per fraud victim was $5,720. Rubina Johannes et al., *2006 Identity Fraud Survey Report*, JAVELIN STRATEGY & RESEARCH, Jan. 2006, at 2. Because the median (the midpoint of the range of losses per victim, where half are below and half above that midpoint) is substantially lower than the mean (the total losses divided by the number of victims), these data indicate that many identity theft victims have lost thousands of dollars, if not more. *See, e.g.,* National Institute of Standards and Technology (NIST)/Sematech, Engineering Statistics Handbook § 1.3.5.1 (July 18, 2006), *available at* http://www.itl.nist.gov/div898/handbook/eda/section3/eda351.htm. While losses of this magnitude can be burdensome for more affluent individuals, they are devastating for persons of more modest means.

Two instances that the President's Identity Theft Task Force cited in its recently-issued Strategic Plan show how substantial a single victim's financial losses can be.

- [I]n July 2001, an identity thief gained control of a retired Army Captain's identity when Army officials at Fort Bragg, North Carolina, issued the thief an active duty military identification card in the retired captain's name and with his Social Security number. The military identification, combined with the victim's then-excellent credit history, allowed the identity thief to go on an unhindered spending spree lasting several months. From July to December 2001, the identity thief acquired goods, services, and cash, in the victim's name, valued at over $260,000. The victim identified more than sixty fraudulent accounts, of all types, that were opened in his name: credit accounts, personal and auto loans, checking and savings accounts, and utility accounts. The identity thief purchased two trucks valued at over $85,000 and a Harley-Davidson motorcycle for $25,000. The thief also rented a house and purchased a time-share in Hilton Head, South Carolina, in the victim's name.

President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan,* PRESIDENT'S IDENTITY THEFT TASK FORCE, Apr. 2007, at 10, *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

- In another instance, an elderly woman suffering from dementia was victimized by her caregivers, who admitted to stealing as much as $200,000 from her before her death. The thieves not only used the victim's existing credit card accounts, but also opened new credit accounts in her name, obtained financing in her name to purchase new vehicles for themselves, and, using a fraudulent power of attorney, removed $176,000 in U.S. Savings Bonds from the victim's safe-deposit boxes.

*Id.* at 10.

It should be noted that identity-theft victims may have to spend more than *de minimis* amounts of money out of their own pockets to resolve their situations with creditors, or administrative or law enforcement agencies. The 2007 Javelin Strategy survey found that the average victim of existing account fraud paid $587 to resolve the problem. The average victim of new account fraud paid

$617 to resolve the problem. Rachel Kim et al., *2007 Identity Fraud Survey Report*, JAVELIN STRATEGY & RESEARCH, Feb. 2007, at 1.

## B. Nonfinancial harms

In addition to direct financial harm, victims of identity theft often suffer nonfinancial harms from which it may take substantially longer to recover. Among other things, victims whose financial accounts have been misused may suffer damage to their credit standing and general reputation in their dealings with legitimate businesses and government agencies.

> One reason that identity theft can be so destructive to its victims, [as the President's Identity Theft Task Force noted,] is the sheer amount of time and energy often required to recover from the offense, including having to correct credit reports, dispute charges with individual creditors, close and reopen bank accounts, and monitor credit reports for future problems arising from the theft.

President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan,* PRESIDENT'S IDENTITY THEFT TASK FORCE, Apr. 2007, at 49, *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf. For example, victims often find it necessary to make multiple telephone calls and write multiple letters to consumer-reporting companies, creditors, and debt collectors. Those calls and letters typically depend on the victim spending still more time to gather the information and documents needed to prove that they are not responsible for the accounts that the criminal has created or transactions that the criminal has conducted in the victim's name.

Moreover, in some cases, when a criminal has used a victim's identity in the commission of a crime, or in identifying himself to law enforcement officers at or before the time of an arrest or first appearance in a criminal prosecution, the identity theft victim may unknowingly have a criminal record incorrectly created under his name. As a result, law enforcement records, such as the National Crime Information Center, may mistakenly list the victim's name as being associated with the criminal acts that the identity thief committed under the victim's name. This, in turn, can lead to mistaken arrests by law enforcement officers who rely, in good faith, on those law enforcement records.

The number of mistaken arrests of identity theft victims is believed to be extremely small in comparison to the estimated numbers of identity theft victims. Nonetheless, the following examples from media reports show how severe and long-lasting the effects of criminal identity theft can be.

*California*: In 2003, the State of California garnished the wages of a resident of the San Francisco Bay area, Jorge Arteaga, for failure to pay speeding tickets. At that time, Arteaga persuaded a judge that he was not the person to whom the tickets were issued, as the tickets pertained to a different car and a different address, and the signature on the ticket was not Arteaga's. Later in 2003, Arteaga was arrested twice on drug-related warrants, but reportedly again persuaded judges that he was not the criminal in both cases. In March 2006, however, Arteaga was arrested on yet another warrant in his name, for allegedly driving on a suspended license. While other records supposedly showed that Arteaga was a parole violator with two auto theft convictions, Arteaga asserted he knew nothing about those crimes. Because of Arteaga's purported status as a parole violator, he was subject to a parole revocation hearing. At the hearing, the presiding commissioner reportedly looked at the mug shot of the actual criminal. Although Arteaga asserted that he was not the person in the photograph, the fingerprints associated with the rap sheet supposedly were Arteaga's. As a result, Arteaga was sent to San Quentin Prison. Arteaga was released from prison only after his attorney reportedly wrote to the warden. A California Department of Corrections employee later described the situation as "a minor clerical error," explaining that "we have two former inmates, both on parole with the same name and we ended up accidentally switching their fingerprints in the files." In January 2007, Arteaga reportedly obtained a judicial exoneration declaring that he

was "factually innocent of the crimes committed by the imposter." *ID Theft Puts Innocent Man In San Quentin*, (KGO-TV broadcast 6 Feb. 20, 2007), *available at* http://abclocal.go.com/kgo/story?section=local&id=5052986.

*California:* In San Francisco, a woman arrested for cocaine possession falsely told court officials that her name was Stancy Nesby, then failed to show up for subsequent court proceedings. A judge reportedly issued multiple warrants for the arrest of Stancy Nesby. Based on the mistaken warrants, from July 2002 to September 2004, the real Stancy Nesby was detained or arrested and jailed seven times by various California law enforcement agencies. Five of the arrests occurred after authorities in Shasta County, where the real Nesby was mistakenly arrested twice, reportedly asked the San Francisco Sheriff's Department to remove the warrants from a state computer system. Nesby eventually sued the City of San Francisco for the failure to remove the warrants from the system. Charlie Goodyear, *A victim who keeps getting arrested -- tangled in a case of identity theft*, SAN FRANCISCO CHRONICLE, Sept. 21, 2004, at A-1, *available at* http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/09/21/MNGET8SAAO1.DTL.

*Wisconsin*: In 1998, a man arrested on drug charges identified himself to police as Malcolm Boyd. A Janesville, Wisconsin resident, Malcolm Boyd, learned of the arrest and went to local police to correct the error. Four months later, after a traffic stop, the real Boyd was arrested and detained on the same pending drug charges. After comparing Boyd's photograph with that of the original individual arrested on drug charges, the police released Boyd. Soon after, Boyd was fired from his part-time job because (according to Boyd) "he was accused of lying about his criminal record." *The darkest side of ID theft*, (MSNBC, Mar. 9, 2003), *available at* http://www.msnbc.msn.com/id/3078488. Some months later, Boyd was laid off from a full-time job, but denied unemployment benefits, because of his criminal record. Boyd was able to get those benefits reinstated, but then had his driver's license suspended for failure to pay traffic fines. The next year, Boyd learned that the man using his name had been arrested in a neighboring county. To establish his innocence of those charges, the real Boyd provided his fingerprints to the local district attorney and later received court documents establishing his innocence. Nonetheless, Boyd was arrested and detained again in 2002 and 2003, but later released. *Id.*

*United Kingdom*: An Andover, England resident, Simon Bunce, reportedly entered personal data on a supermarket shopping Web site so that he and his wife could shop online. Thereafter, someone using Bunce's name and address registered for a pornography Web site used by pedophiles. In connection with a United Kingdom law enforcement operation against child pornography, on two occasions in 2004, Bunce was arrested and his house searched. Police later reportedly sent Bunce a letter saying they were not taking any further action in the case because they had not found any evidence of wrongdoing on his computers or media storage devices. The police publicly confirmed that Bunce was not charged with any offense. Dick Bellringer, *Identity theft nightmare*, ANDOVER ADVERTISER, Apr. 4, 2007, at B5, *available at* http://www.andoveradvertiser.co.uk/mostpopular.var.1306843.0.identity_theft_nightmare.php.

Criminals in some instances have even used the identities of deceased persons to conceal their criminal status or activities. For example, in October 2006, Michigan authorities arrested a convicted sex offender on identity theft and forgery charges. He allegedly applied for a birth certificate in the name of an infant who had died in 1972, so that he could move to the State of Oregon without having to register as a sex offender. *See* Press Release, Office of the Attorney General, State of Michigan, UP Sex Offender Arrested in Bizarre Identity Theft Case (Oct. 17, 2006) (on file with author), *available at* http://www.michigan. gov/ag/0,1607,7-164-34739_34811-153805--,00.html.

More recently, in April 2007, a Southern California woman was federally charged with stealing the identities of hundreds of deceased people and using their personal information to file fraudulent federal tax returns that sought more

than $1 million in refunds. *See* Press Release, U.S. Attorney's Office, Central District of California, Hawthorne Woman Charged with Stealing Hundreds of Identities of Dead People to File Bogus Tax Returns that Sought More Than $1 Million in Refunds (Apr. 12, 2007) (on file with author), *available at* http://www.usdoj.gov/usao/cac/news/pr2007/052.html. Such conduct can create significant problems for surviving family members and for executors of the deceased persons' estates in restoring the deceased persons' financial affairs and reputation.

## III. Conclusion

The financial and human toll from identity theft can be devastating. As one of the most pervasive forms of white collar crime in the United States, it warrants focused investigative and prosecutive resources. The perpetrators of identity theft will inevitably grow in number due to the lucrative nature of the offense, and they will likely increase in sophistication as technology evolves. Investigators and prosecutors must do the same to combat the problem.❖

### ABOUT THE AUTHOR

❑**Jonathan J. Rusch** serves as the head of the United States delegation to the United Nations Crime Commission Expert Group on Fraud and the Criminal Misuse of Identity, the United States Co-Chair of the United States-Canada Mass-Marketing Fraud Working Group, and Chair of the national-level Mass Marketing Fraud Working Group. Since 1995, Mr. Rusch has been the Justice Department's coordinator for a series of multinational fraud enforcement operations, including "Operation Global Con" in May 2006 and "Operation Roaming Charge" in October 2004.

Mr. Rusch also serves as Executive Director for Consumer and Benefit Fraud of the Department of Justice's Hurricane Katrina Fraud Task Force. In that capacity, he oversees the Task Force's national enforcement program with respect to charity fraud, disaster-relief assistance fraud, identity theft, and other forms of consumer-related fraud. In addition, since May 2006 he has been serving as a key drafter and editor of the President's Identity Theft Task Force Strategic Plan.

He has been the lead prosecutor in major fraud and public corruption prosecutions by the Department of Justice, including successful prosecutions of a former United States Treasurer, a House Sergeant at Arms, and former Members of Congress, as well as ringleaders of various mass-marketing fraud schemes.

Mr. Rusch received the Attorney General's Award for Fraud Prevention in 2006 for his work on the Hurricane Katrina Fraud Task Force, the Assistant Attorney General's Award for Inter-Agency Cooperation in 2005 for his work in organizing and leading strategic law enforcement initiatives, the Chief Postal Inspector's Award in 2004 for his work in fraud prevention and cross-border fraud initiatives, and the Attorney General's Distinguished Service Award in 1995 for his work in investigating the House Bank scandal. Mr. Rusch also is an Adjunct Professor of Law at Georgetown University Law Center, where he teaches courses on Global Cybercrime Law and Trial Practice, and Lecturer in Law at the University of Virginia Law School, where he teaches Cybercrime.✠

*This article is adapted from a report that Mr. Rusch drafted for the Criminal Process Committee of the American Bar Association Administrative Law and Regulatory Practice Section. The views herein are not necessarily those of the American Bar Association or any of its components.*

# Identity Theft: Applicable Federal Statutes and Charging Decisions

*Sean B. Hoar*
*Assistant United States Attorney*
*District of Oregon*

## I. Identity theft: the nature of the problem

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, and in our digital environment, the possession, transfer, or use of the information often affects interstate commerce. Due in part to the reliance upon the Internet and other electronic mediums to conduct financial transactions and store information, identity information is now more susceptible to theft than ever before. Sensational cases involving millions of victims from electronic database breaches frequent the written and broadcast media, highlighting the vulnerability of the United States' information infrastructure.

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. In order to better understand the nature of the problem, ponder for a moment all the places where identity information is located.

- What are the contents of a wallet or purse? A driver's license, credit card, debit card, credit or debit card receipts, insurance cards, athletic club membership card, an organizational membership card, business cards, personal and staff emergency home and cellular telephone numbers, and a variety of other items that either alone, or in combination with one another, can provide an identity thief easy and quick access to cash and credit.
- What does a computer contain? A host of digital data that may similarly provide an identity thief access to cash and credit: names, dates of birth, social security numbers, account passwords, financial account information, e-mail addresses and user names.
- What information is found in the home? The remaining documentation of an individual's financial life: bills, financial account statements, insurance statements, birth certificates, and everything else that a person would not want an identity thief to obtain.
- What is in the car? It always contains the registration, but does it periodically contain a wallet, purse, or lap top computer? Is it often used to "store" receipts or other financial documents?
- What is readily available on the Internet? Ever searched for personal identifying information and found it because of coaching a youth sports team and the local organization posted the team information on its Web site? Birth dates are readily accessible on Web sites. Social security numbers and other personal information may be purchased online.
- What about all those data repositories? Where is digital information stored by health care providers, home, auto, and life insurance companies, banks or credit unions, credit card issuer(s), credit bureaus, and "third party affiliates" of insurance companies, banks or credit unions, or credit card issuers to which information is regularly provided or sold.

Does the American public ever give any thought to how much revenue is created by the sale of their identification information by public and private entities?

If an individual or a custodian of personal information gets the least bit careless, identification information will be stolen. Given the ease with which identity theft can be committed, and the lucrative rewards it provides to the thieves, the crime of identity theft is here for the long term. It is one of the most pervasive federal crimes Assistant United States Attorneys (AUSAs) investigate and prosecute. Investigators and prosecutors must be familiar with the various identity theft-related statutes and the resources available to them to pursue identity thieves.

## II. Identity theft: a different type of crime, a different impact upon victims

Identity theft is unique from other crimes, principally in its impact upon victims. Law enforcement often becomes aware that a person is a victim of identity theft before the victim does. During the course of an investigation, law enforcement often finds the identity of a victim in the possession of a criminal. The crime is then reported to the victim, rather than from the victim to law enforcement.

The way in which identity theft occurs may delay discovery by the victim. In most situations, the victim can learn of the theft only after the thief uses the information. This may be months or years after the information is stolen.

- If the theft occurs from a database breach, whether it be by an insider or an intruder into a vulnerable system, 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, which are then activated and the cards sent to third-party addresses, it is 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.

Identity theft is particularly egregious when committed against the vulnerable, such as minors and the elderly. These victims often have little ability to discover the theft, and, as a result, are often harmed far worse than the average victim. When these victims are specifically targeted due to their vulnerability, the loss is often greater because they are such "easy targets" and their response time will likely be much slower than the average victim. A related travesty is when the identity theft is committed by someone in a place of trust, whether it be a friend, a family member, or a financial institution insider. The trusted thief often has access to sufficient financial information to substantially aggravate the amount of harm by stealing a larger amount of money and benefiting from the lapse of time before the harm is detected.

Identity theft often results in a much wider scope of harm to its victims. Not only do they suffer direct financial losses from checking accounts and savings accounts, but they suffer indirect harms such as damage to their credit status, lost economic opportunities, and damage to their reputation. They may also spend substantial time and money to repair damage done, which may involve legal processes to remove civil liens and judgments. In the worst case scenarios, legal processes will be required to dismiss criminal arrest warrants and convictions. One of the

reasons the correction of harm may take substantial time and expense is that the victim may need to "prove the negative."

## III. Identity theft case intakes: the AUSA's reality

The AUSA on duty, or the Identity Theft Point of Contact for the district, will be called when someone is arrested while in possession of multiple social security account number cards, each of which bears the suspect's name, but a different number. The suspect has a long nonfederal criminal history and, at a glance, appears to be a Criminal History Category VI. What does the AUSA advise the arresting officer, agent, or inspector to do? Is the case immediately declined because it is too small (less than ten victims, no known loss, case will likely be prosecuted by state authorities, and the AUSA's plate is already too full)? Does the AUSA tentatively accept the case pending confirmation of certain facts (that the social security numbers [SSNs] belong to actual people, that there may be more victims, that there may be substantial losses, and that further investigation will identify additional evidence—possibly digital evidence that can be forensically examined, among other things)? Or is the case accepted regardless of additional facts or evidence?

Any of these decisions may be appropriate, depending upon the circumstances. If the AUSA decides to at least tentatively accept the case pending the receipt of additional facts or evidence, what steps are taken? What resources exist to create a better case? Can the Office of the Inspector General, Social Security Administration (OIG/SSA) quickly determine that each of the SSNs has been assigned to an actual person other than the suspect? Can the AUSA quickly pull credit reports on the "victim" SSNs to determine recent credit activity? Can the AUSA reach out to identified victims to gather information? Did they know the suspect had their SSN? Are they aware of any unauthorized activity? Do the victims have any idea how the suspect may have obtained their SSN? Does the preliminary investigation indicate compromise of credit or bank accounts? If so, can the prosecutor quickly identify the amount of loss? Is there any digital evidence that can be forensically examined? If a lap top exists, does it show the creation of new SSN account cards in the suspect's name? Does it contain other SSNs? Does it contain other documents used to facilitate identity theft? Is the suspect and her/his attorney amenable to a debriefing—perhaps under Federal Rule of Criminal Procedure 11—in order to determine the scope of the offense and attempt to protect against further use of the victim SSNs?

## IV. Melendrez case study

The author works in a relatively small office in Eugene, Oregon. Although Eugene is often referred to as heaven, it nonetheless is lacking in certain resources—law enforcement. The silver lining is that the lack of resources has helped to facilitate the creation of informal networks involving local, county, state, and federal agencies, and private sector security personnel. As a result of these informal networks, in December of 2001, the author received a call from an officer in a small, rural town—Grants Pass, Oregon—who had attended some financial fraud training that the author coordinated. The officer inquired about whether the United States Attorney's Office (USAO) would take a case involving John Manuel Melendrez, who was a continual thorn in the side of local law enforcement. The author told participants in the training that if they had someone who was involved in identity theft and who created a disproportionately adverse impact in their community, to call the USAO. He explained to them that the primary goal was to make sure a case involving such a person did not fall through the cracks, meaning that he would do what he could to communicate with local and federal authorities to make sure the person was held accountable.

John Manuel Melendrez appeared to be the typical criminal who created a disproportionately adverse impact in his community. He had a lengthy criminal history, and every time he was arrested, he was in possession of false identification. Although he had a long criminal

history (ten prior felonies, a few of which were violent robberies), the state criminal justice system did little to deter his criminal activity. Although his case was perhaps one of the "smallest" the author had seen, the commitment to review the case was honored.

The preliminary facts were very simple. When arrested, Melendrez was in possession of a social security card in a name similar to his own, but which contained a number that did not appear to be his. A second, similar social security card was found when he was lodged in jail. Was it worth further inquiry?

During the initial call from the officer, the AUSA inquired about whether other evidence existed that could be reviewed to determine whether Melendrez had created other documents. The purpose of the question was to determine whether the "breeder document" enhancement now found at U.S.S.G. § 2B1.1(b)(10)(C)(i) and (ii) could be used. If so, this enhancement would provide an offense level "floor" of 12, regardless of loss. If his Criminal History Category was in fact VI, his sentencing guideline range would be 30 to 37 months imprisonment—even if there were no loss. In attempting to determine whether any other evidence existed, the AUSA asked the officer to review any communication Melendrez had with anyone after he was placed in jail. The officer was also asked to focus on developing probable cause to search wherever Melendrez lived prior to his arrest, and on finding a computer or whatever else was used to create the social security cards found in Melendrez's possession.

The prosecutor told the officer that if additional evidence was developed which showed that SSNs of actual people were used by Melendrez to create false documents, then he would likely be able to pursue the case, regardless of loss, due to the disproportionately adverse impact Melendrez had in his community (utilizing the "breeder document" enhancement). The AUSA told him that he preferred to have at least ten victims from multiple jurisdictions, but that they could discuss it further depending upon the evidence.

## A. Case development: investigative chronology

On December 1, 2001, Melendrez was arrested on a probation violation by the Grants Pass, Oregon Police Department (GPPD). At the time of his arrest, he identified himself as Juan Miguel Melendrez and provided a temporary Colorado driver's license and a social security card bearing the number xxx-xx-8897, in the name of Juan Melendrez. While in custody, a second social security card bearing the same number in the name of Juan Melendrez was seized from him.

On December 12, 2001, in response to the prosecutor's request to gather additional evidence, GPPD detectives obtained information including photographs from the Colorado and Oregon Departments of Motor Vehicles which showed that Melendrez had obtained an Oregon driver's license in the name of Timothy Allen Cooper, with a date of birth of November 7, 1960, and a Colorado driver's license in the name of Juan Miguel Melendrez with a date of birth of May 15, 1955. On December 21, 2001, GPPD detectives obtained a search warrant for Melendrez's home and seized a computer, printers, electronic credit card equipment, and other equipment and material which was apparently used to manufacture identification documents.

On December 28, 2001, in reviewing jail records, GPPD detectives learned that Melendrez had contacted Paul Wickey shortly after being incarcerated. They later learned that Melendrez instructed Mr. Wickey to go to Melendrez's home and remove certain items before the GPPD detectives served the search warrant. The GPPD detectives learned that Mr. Wickey had removed several bags of items from Melendrez's home and stored them at his residence in Merlin, Oregon.

On December 31, 2001, GPPD detectives met with Mr. Wickey, at which time he admitted that Melendrez had contacted him and requested that he go to Melendrez's home and remove incriminating evidence. He said that he then went to Melendrez's home and removed a number of items, although he was unable to remove the computer equipment due to a recent surgery. Mr.

Wickey then provided the items that he had removed from the Melendrez's home to the GPPD detectives. These items included blank and completed birth certificates, blank and completed Department of Defense Report of Separation forms (DD Forms 214), blank and completed identification cards, and other material which was apparently used to manufacture identification documents. The various documents used six social security numbers which a Special Agent with OIG/SSA determined had been assigned to actual persons other than Melendrez.

A forensic analysis of the computer and diskettes seized from Melendrez's home revealed graphic images of social security cards, DD Forms 214, birth certificates, identification cards, and other identification documents. The various images matched the documents which were previously seized and which used six social security numbers assigned to actual persons other than Melendrez.

## B. Investigative outcome

The investigation determined that during the months of September, October, and November 2001, Melendrez used his computer equipment to produce at least nine identification documents, using six social security numbers assigned to actual persons other than Melendrez. No known loss resulted from the offense, but due to Melendrez's extensive criminal history, the case was taken federally.

## C. Federal prosecution

Melendrez rejected a plea agreement, believing he could do better with a straight guilty plea under the sentencing guidelines. The conditions of the plea agreement would have resulted in an applicable sentencing guideline range of 30 to 37 months. He ultimately pled guilty to unlawfully producing more than five identification documents in violation of 18 U.S.C. § 1028(a)(1), (b)(1)(A)(i) and (ii), (b)(1)(B).

## D. Sentencing

The presentence report (PSR) found that Melendrez had possessed five or more means of identification that unlawfully were produced from, or obtained by the use of, another means of identification, including social security cards, birth certificates, driver's licenses, and DD Forms 214. It therefore recommended that the offense level be increased to a level 12 pursuant to U.S.S.G. § 2B1.1(b)(9)(C) (2002) (the predecessor to U.S.S.G. § 2B1.1(b)(10)(C)(i) and (ii) (2007)). Melendrez objected to this offense level increase, claiming that U.S.S.G. § 2B1.1, cmt. n.7 (2007), limited the application of U.S.S.G. § 2B1.1(b)(9)(C) (2007) when a means of identification is used to produce a "fictitious" document. The PSR also recommended that the offense level be increased two-levels pursuant to U.S.S.G. § 3C1.1 (2007) for his obstruction of justice in attempting to conceal or destroy evidence, resulting in an adjusted offense level of 14. Finally, the PSR recommended a two-level reduction for Melendrez's acceptance of responsibility, resulting in a total offense level of 12. Since the Criminal History Category was VI, the applicable Sentencing Guidelines range was found to be 30 to 37 months.

The sentencing court agreed with the recommendations contained in the PSR and Melendrez was sentenced to serve a 30-month term of imprisonment.

## E. Appeal

Melendrez appealed the district court's sentence, alleging that an SSN is not a means of identification for purposes of U.S.S.G. § 2B1.1(b)(9)(C)(i) and (ii) (2002), when it is used in a fictitious document. The government's position was that when an SSN has been issued to an actual person, the SSN is always a means of identification, regardless of whether it is used in a fictitious document. The Court of Appeals for the Ninth Circuit affirmed the district court decision. *United States v. Melendrez*, 389 F.3d 829, 834 (9th Cir. 2005). Melendrez served a 30-month term of imprisonment.

## F. Melendrez case outcome

Was the Melendrez case worth federal prosecution? Although it was a very small case—there were only six SSNs used without authorization and there was no known loss—due

to Melendrez's serious criminal history and his use of SSNs to create other means of identification, he was sentenced to, and served, a 30-month term of imprisonment. If the guidelines range would have been based solely on loss, Melendrez would have had to steal over $30,000 in order to merit such a sentence. *See* U.S.S.G. § 2B1.1(b)(1)(D) (2007).

The Melendrez case was a win/win situation for all agencies involved. The local agency did all the leg work and helped to remove a prolific criminal from their community. The federal agency did minimal work—the case agent confirmed that the SSNs were issued to actual people other than Melendrez, she presented a criminal complaint to the magistrate judge, and she appeared before a federal grand jury. The USAO did what it said it would do. It assisted the local agency, and it helped to hold the identity thief accountable. The process helped foster confidence in the network of law enforcement agencies created to work on identity theft offenses.

How was the result in Melendrez obtained?

- monetary threshold was waived;
- further investigation was encouraged;
- AUSA "brainstormed" with investigators about possible leads;
- AUSA followed through on commitments;
- the most relevant subsections under 18 U.S.C. § 1028(a) and (6) were utilized, and
- all available enhancements under the sentencing guidelines were used.

## V. Role of monetary thresholds

What role should monetary thresholds play in investigative and prosecutive guidelines for identity theft cases? While monetary thresholds are often necessary to properly allocate investigative and prosecutive resources, they often cause the premature termination of identity theft investigations. Most identity theft investigations begin with the discovery of relatively nominal losses to individual victims—yet when such investigations are pursued, a substantial increase is usually found in the amount of loss and the number of victims. When an investigation is terminated before its potential is developed, identity thieves who would otherwise warrant federal prosecution become exempt from liability.

Even if monetary thresholds are necessary as a case screening device, they should be reduced or waived in at least certain types of identity theft cases. As an example, in conventional identity theft cases involving violations of 18 U.S.C. § 1028(a)(7), but no identifiable monetary loss, a minimum offense level of 12 is established when an offender transfers or uses a victim's means of identification to obtain other means of identification. U.S.S.G. § 2B1.1(b)(10)(C)(i) (2007). Likewise, in cases involving no identifiable monetary loss, a minimum offense level of 12 is established when an offender possesses five or more means of identification that were unlawfully produced from another means of identification or obtained by the use of another means of identification. U.S.S.G. § 2B1.1(b)(10)(C)(ii) (2007).

For most fraud offenses, the loss would have to be more than $30,000 for the resulting offense level to be level 12. This minimum offense level accounts for the fact that the means of identification that were "bred" (produced or obtained) often are within the defendant's exclusive control, making it difficult for the individual victim to detect that his or her identity has been stolen. Generally, the victim does not become aware of the offense until certain harms have already occurred (a damaged credit rating or an inability to obtain a loan). The minimum offense level also accounts for the nonmonetary harm associated with these types of offenses, much of which may be difficult or impossible to quantify ( 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 indicates that Congress was especially concerned with providing increased punishment for this type of harm. U.S.S.G. § 2B1.1, cmt. background. To the extent investigative or prosecutive guidelines include monetary thresholds to ensure resources bring the "biggest bang for the buck," such thresholds are not

necessary in identity theft cases where the Sentencing Guidelines impose the equivalent of a $30,000 loss for certain specific offense characteristics.

An even better example of why monetary thresholds should be reduced or waived involves aggravated identity theft, which carries a 2-year minimum mandatory sentence. 18 U.S.C. § 1028A(a)(1). For most fraud offenses, the loss would have to be more than $120,000 to approximate a 24-month term of imprisonment.

## VI. Federal identity theft statutes

This article primarily concerns the conventional identity theft statute, 18 U.S.C. § 1028(a)(7), and the aggravated identity theft statute, 18 U.S.C. § 1028A. It is important to understand, however, that § 1028(a) proscribes a variety of document fraud which may be related to identity theft. Section 1028(a)(1)-(6) and (8) proscribe the fraudulent creation, use, or transfer of identification *documents* and *features*, while § 1028(a)(7) proscribes the criminal transfer, possession, or use of identification *information*.

### A. Section 1028

Section 1028 is a deceptively complex statute. It contains a number of possible jurisdictional components, at least one of which must be pleaded and proven for any § 1028 violation. It also contains a number of penalty components, each of which carries a different statutory maximum penalty. The facts underlying the different statutory maximum penalties must also be pleaded and proven to establish the maximum penalty for any § 1028 violation.

Section 1028 was created to confront criminal conduct involving false identification documents. On December 31, 1982, as part of the False Identification Crime Control Act of 1982, § 1028(a)(1)-(6) was enacted to prohibit the fraudulent creation, use, and transfer of identification documents. *See* Pub. L. No. 97-398, § 2, 96 Stat. 2009 (Dec. 31, 1982). On October 30, 1998, as part of the Identity Theft and Assumption Deterrence Act, § 1028(a)(7) was enacted to prohibit the theft and unlawful use of personal identifying information, whether or not the information was contained in, or used in, fraudulently created documents. Congress perceived that § 1028(a)(7) was needed because 18 U.S.C. § 1028(a)(1)-(6) addressed only the fraudulent creation, use, or transfer of identification documents, and not the theft or criminal use of the underlying personal information. *See* Pub. L. No. 105-318, § 3(a) to (g), (h)(1), 112 Stat. 3007 to 3009 (Oct. 30, 1998).

On April 30, 2003, as part of the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 (PROTECT Act), the Secure Authentication Feature and Enhanced Identification Defense Act of 2003 (SAFE ID Act) added § 1028(a)(8) to prohibit trafficking in false authentication features which would otherwise be used in false identification documents. *See* Pub. L. No. 108-21, Title VI, § 607(b), 117 Stat. 689 (Apr. 30, 2003). Since that time, a number of amendments have been made to various aspects of § 1028. *See* Pub. L. No. 108-275, § 2(c), 3, 118 Stat. 832 (July 15, 2004), (Identity Theft Penalty Enhancement Act—created "aggravated" identity theft statute at § 1028A); Pub. L. No. 108-458, Title VII, § 7216, 118 Stat. 3833 (Dec. 17, 2004), (Intelligence Reform and Terrorism Prevention Act of 2004); Pub. L. No.109-13, Div. B, Title II, § 203(a), 119 Stat. 315 (May 11, 2005) (Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005); and Pub. L. No. 109-177, Title VI, § 603, 120 Stat. 253 (Mar. 9, 2006) (USA PATRIOT Improvement and Reauthorization Act of 2005).

Section 1028(a) proscribes eight different types of conduct involving fraudulent identification documents or the unlawful use of identification information. It provides that a federal crime is committed when jurisdictional facts referenced in § 1028(c) exist, and a person

> (1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;
>
> (2) knowingly transfers an identification document, authentication feature, or a

false identification document knowing that such document or feature was stolen or produced without lawful authority;

(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;

(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;

(5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;

(6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;

(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or

(8) knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification.

18 U.S.C. § 1028(a).

**Section 1028 jurisdictional component**. All § 1028 offenses must have facts that create federal jurisdiction. All § 1028 offenses must derive from *"a circumstance described in subsection (c)"* of § 1028. This commonly overlooked but critical jurisdictional phrase requires that:

(1) the identification document, authentication feature, or false identification document *is or appears to be issued by or under the authority of the United States* or a sponsoring entity of an event designated as a special event of national significance or the document-making implement is designed or suited for making such a document or feature;

(2) the offense is an offense under § 1028(a)(4) (*the document is possessed with intent to defraud the United States)*; or

(3) either—

(A) the prohibited production, transfer, possession, or use is in or affects interstate or foreign commerce, including the transfer of a document by electronic means; or

(B) the means of identification, document, or document-making implement *is transported in the mail* in the course of the prohibited production, transfer, possession, or use.

18 U.S.C. § 1028(c) (emphasis added).

Congress intended to provide broad federal jurisdiction over violations of § 1028 by requiring that only a minimal nexus with interstate or foreign commerce be shown. H.R. Rep. No. 97-802, at 14 (1982), *as reprinted in* 1982 U.S.C.C.A.N. 3519, 3532-33; *United States v.*

*Pearce*, 65 F.3d 22, 25 (4th Cir. 1995). The minimal nexus requirement will be satisfied if it is proven beyond a reasonable doubt that the defendant had an intent to do acts which, if completed, would have affected interstate commerce. *United States v. Villarreal*, 253 F.3d 831, 839 (5th Cir. 2001).

**Section 1028 penalties.** In *Apprendi v. New Jersey*, 530 U.S. 466 (2000), the Supreme Court held that "[o]ther than the fact of a prior conviction, any fact that increases the penalty for a crime beyond the prescribed statutory maximum must be submitted to a jury, and proved beyond a reasonable doubt." *Id.* at 490. Section 1028 contains a number of penalty element options, each of which is based upon a different set of facts and carries a different statutory maximum penalty. It is critical that facts relied upon for imposition of a penalty which is higher than the baseline statutory maximum penalty for the offense be pleaded and proven beyond a reasonable doubt. This includes having the jury instructed on the facts and having it return an appropriate finding or verdict form on the facts. *Id*. Once the fact which increases the maximum statutory penalty is pleaded and proven, however, other factors which may enhance a sentence up to the maximum statutory penalty are within the discretion of the court to find in rendering a reasonable sentence. *United States v. Booker/Fanfan*, 543 U.S. 220 (2005). Depending upon the facts pled and proved, § 1028(b) provides penalties of between 1 and 30 years of imprisonment for violations of § 1028(a).

Section 1028(b) provides that the punishment for a § 1028(a) violation is:

> (1) a $250,000 fine or imprisonment for not more than 15 years, or both, if the offense is—
>
> > (A) the production or transfer of an identification document, authentication feature, or false identification document that is or appears to be—
> >
> > > (i) an identification document or authentication feature issued by or under the authority of the United States; or
> >
> > > (ii) a birth certificate, or a driver's license or personal identification card;
> >
> > (B) the production or transfer of more than five identification documents, authentication features, or false identification documents;
> >
> > (C) an offense under § 1028(a)(5) (a document-making implement or authentication feature is knowingly produced, transferred, or possessed with the intent that it will be used in the production of a false identification document or another document-making implement or authentication feature);
> >
> > (D) an offense under (a)(7) that involves the transfer or use of one (1) or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any one (1) year period;
>
> (2) a $250,000 fine or imprisonment for not more than five (5) years, or both, if the offense is—
>
> > (A) any other *production, transfer, or use* (not mere possession) of a means of identification, an identification document, authentication feature, or a false identification document; or
> >
> > (B) an offense under § 1028(a)(3) (possession with intent to use or transfer unlawfully five or more identification documents) or

§ 1028(a)(7) (the transfer, possession or use of means of identification of another person with intent to commit a federal crime or state felony);

(3) a $250,000 fine or imprisonment for not more than 20 years, or both, if the offense is committed—

(A) to facilitate a drug trafficking crime (as defined in § 929(a)(2)—any felony federal drug crime);

(B) in connection with a crime of violence (as defined in § 924(c)(3)—a felony offense that has as an element the use or attempted use of physical force, or that by its nature involves a substantial risk of physical force being used during the offense); or

(C) after a prior conviction under § 1028 becomes final;

(4) a $250,000 fine or imprisonment for not more than 30 years, or both, if the offense is committed to facilitate an act of domestic terrorism (as defined under § 2331(5)) or an act of international terrorism (as defined in § 2331(1)).

18 U.S.C. §§ 1028(b) and 3571(b)(3).

## B. Section 1028(a)(7)

Section 1028(a)(7) is the "conventional" identity theft subsection. As referenced above, it provides that when federal jurisdiction exists (the transfer, possession or use was in or affected interstate or foreign commerce, or involved the mail), it is a federal crime to knowingly transfer, possess, or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law. The federal, state, or local law that is facilitated by the identity theft must also be proven.

**Section 1028(a)(7) penalties**. As set forth above, depending upon the facts pled and proven, § 1028(b) provides a penalty of between 5 and 30 years of imprisonment for violations of § 1028(a)(7). The most common maximum statutory penalty for a § 1028(a)(7) offense will likely be a $250,000 fine or imprisonment for not more than 15 years, or both, because most federal identity theft offenses will involve the transfer or use of at least one or more means of identification which results in the perpetrator obtaining $1,000 or more during any one year period of time. 18 U.S.C. § 1028(b)(1)(D). If, for whatever reason, these facts are not pled or proven, the statutory maximum penalties for a § 1028(a) offense will always be at least a $250,000 fine or imprisonment for not more than 5 years, or both. 18 U.S.C. §§ 1028(b)(2)(B) and 3571(b)(3). Note that any person who attempts or conspires to commit any offense under § 1028 is subject to the same penalties as those prescribed for the substantive offense under § 1028, the commission of which was the object of the attempt or conspiracy. 18 U.S.C. § 1028(f). This ensures that the applicable maximum penalty is commensurate with the offense.

**Section 1028 forfeiture**. Every § 1028 charging instrument should have a forfeiture count, and every § 1028 plea agreement should have a forfeiture or abandonment provision. The forfeiture or abandonment should involve all instrumentalities, proceeds, and contraband, associated with identity theft. Regarding the forfeiture of instrumentalities of identity theft, § 1028(b)(5) provides that any personal property used or intended to be used to commit a violation of § 1028(a) is subject to forfeiture. The forfeiture of property under § 1028, including any seizure and disposition of the property and any related judicial or administrative proceeding, is governed by the provisions of 21 U.S.C. § 853. 18 U.S.C. § 1028(g).

Regarding the forfeiture of proceeds of identity theft, 18 U.S.C. § 982(a)(2)(B) provides that the court, in imposing sentence on a person convicted of a § 1028 violation, shall order the forfeiture of any property constituting, or derived from, proceeds the person obtained directly or indirectly as a result of the violation. All forfeited proceeds should be remitted to victims through

utilization of the restoration process. Note that there must be an intermediary overseeing the remission of proceeds to victims which is why it is necessary that AUSAs work with their respective forfeiture counsel to utilize the restoration process to remit the proceeds to victims.

Regarding the forfeiture of identity theft contraband, § 1028(h) provides that when any person is convicted of a violation of § 1028(a), the court shall order, in addition to the penalty prescribed, the forfeiture and destruction or other disposition of all illicit authentication features, identification documents, document-making implements, or means of identification. The directive of § 1028(h) should be included in any plea agreement. Whether the case is resolved by plea or trial, however, any illicit authentication features, identification documents, document-making implements, or means of identification, should be identified for the court so that § 1028(h) can be enforced.

Monetary thresholds exist for the federal forfeiture of property, and the monetary value of computer equipment used to commit identification document fraud or identity theft will often not meet those thresholds. Monetary thresholds, however, should never impede the divestment of a defendant's instrumentalities, proceeds, or contraband. If a threshold is not met, the defendant can be required to abandon any interest in the equipment as part of any resolution prior to trial of the matter. If the matter is not resolved prior to trial, the AUSA should seek an exemption from the monetary threshold.

If the equipment does not constitute the proceeds of fraud, or if ample proceeds otherwise exist to remit to victims for purposes of restitution, once the equipment is either abandoned or forfeited, it can be put into use by law enforcement agencies. When an investigation is assisted by a local agency, the forfeited or abandoned computer equipment can be provided to that agency for use in future investigations. This tends to foster positive interagency relationships and long-term cooperation in identity theft investigations. It also serves as an incentive for local agencies to participate in identity theft working groups or task forces.

AUSAs should always consult with their district forfeiture counsel on forfeiture matters. They should also consult with the respective investigative agency to determine whether an administrative action has been commenced against the forfeitable property to ensure that criminal forfeiture is necessary. To accomplish criminal forfeiture, a separate count must be alleged against the specified property, setting forth the basis for forfeiture. It must then be proven at trial by a preponderance of the evidence or consented to as part of a guilty plea. *See, e.g., United States v. Garcia-Guizar*, 160 F.3d 511, 518 (9th Cir. 1998) (preponderance standard is constitutional because criminal forfeiture is not a separate offense, but only an additional penalty for an offense that was established beyond a reasonable doubt). Notice of the forfeiture must thereafter be published to ensure there are no third parties who desire to make a claim to the property. 21 U.S.C. § 853(n)(1). When property is abandoned, the abandonment agreement can be enforced only against the defendant entering into the agreement, because it is not published, and third parties who might otherwise have an interest in the property are not put on notice of the abandonment.

## C. Section 1028A

On July 15, 2004, the Identity Theft Penalty Enhancement Act was signed into law. Among other things, it created a new offense of "aggravated" identity theft, which prohibits the knowing transfer, possession, or use, without lawful authority, of a means of identification of another person during and in relation to any of over 180 federal nonterrorism-related felony offenses, 18 U.S.C. § 1028A(c), and any of over 100 federal terrorism-related felonies, § 2332b(g)(5)(B). 18 U.S.C. § 1028A(a)(1) and (2). It also prohibits the knowing transfer, possession, or use, without lawful authority, of a false identification document during, and in relation to, any of the over 100 federal terrorism-related felonies implicated by 18 U.S.C. § 1028A(a)(2). Note that the felony committed

during and in relation to the identity theft must also be proven.

The predicate offense does not have to be charged as a substantive offense in order to adequately charge a § 1028A offense. Judicial interpretations of § 924(c) may be useful in determining whether prosecutors must charge one or more substantive predicate offenses as separate counts along with a section 1028A offense. In *U.S. v. Crump*, 120 F.3d 462, 466 (4th Cir. 1997), the court construed the statutory language "during and in relation to" of § 924(c)(1) to find that a defendant's conviction under § 924(c)(1) did not depend on his being convicted of the predicate offense either previously or contemporaneously, as long as all of the elements of that offense were proven and found beyond a reasonable doubt.

Congress expressly excluded conventional identity theft, or violations of § 1028(a)(7), from the list of predicate offenses for § 1028A. This means that a violation of § 1028(a)(7) may not be charged as a predicate felony for purposes of a § 1028A violation. It may be entirely appropriate, however, to charge a defendant in the same indictment or information with one or more violations of § 1028(a)(7) and one or more violations of section 1028A, so long as each section 1028A charge is based solely on one or more of the predicate offenses set forth in §§ 1028A(c) or 2332b(g)(5)(B).

Note also that certain offenses that are commonly associated with identity theft, such as mail theft, 18 U.S.C. § 1708, and uttering counterfeit securities, 18 U.S.C. § 513, are not predicate offenses for § 1028A.

**Section 1028A jurisdictional component**. In pleading and proving that the prohibited transfer, possession, or use occurred "during and in relation to" any of the felonies enumerated in §§ 1028A(c) and 2332b(g)(5)(B), federal jurisdiction must be alleged and proven. It is therefore critical that the specific predicate felony be alleged and that its elements be proven during the course of a Federal Rule of Criminal Procedure 11 change of plea colloquy or during trial.

**Section 1028A penalties**. Aggravated identity theft is punishable by a minimum mandatory 2 year term of imprisonment, consecutive to the sentence for the underlying felony, if the offense is committed during and in relation to any of the enumerated nonterrorism-related felony offenses. 18 U.S.C. § 1028A(a)(1). It is punishable by a minimum mandatory 5 year term of imprisonment, consecutive to the sentence for the underlying felony, if the offense is committed during and in relation to any of the enumerated terrorism-related felony offenses. 18 U.S.C. § 1028A(a)(2).

A court is prohibited from placing anyone who has been convicted of aggravated identity theft on probation. 18 U.S.C. § 1028A(b)(1). A court is also prohibited from imposing a sentence for aggravated identity theft concurrent with any other term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identification was transferred, possessed, or used. 18 U.S.C. § 1028A(b)(2). Should a defendant be convicted of a predicate felony, a court is prohibited from fashioning a less severe sentence for that predicate felony in order to compensate for the minimum mandatory term of imprisonment imposed for the § 1028A violation. A term of imprisonment imposed on a person for aggravated identity theft may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional aggravated identity theft conviction. 18 U.S.C. § 1028A(b)(4).

**Section 1028A forfeiture**. Section 1028A does not contain a forfeiture provision. It is important, therefore, to either include a predicate felony as a substantive count and forfeit property through that count or, if appropriate, include a conventional identity theft count under § 1028(a)(7) and forfeit the property through that count. Forfeiture through the predicate felony count or the § 1028(a)(7) count will usually involve the forfeiture provisions referenced in 18 U.S.C. § 982(a)(2)(A) and (B).

**Sections 1028 and 1028A elements**. The "knowing" element does not require proof that the defendant knew that the owner of the documents actually existed, or that the defendant knew the means of identification was of a "real" person. *United States v. Hurtado*, 508 F.3d 603, 609 (11th Cir. 2007) (citing *United States v. Montejo*, 442 F.3d 213, 217 (4th Cir. 2006), *cert. denied,* 127 S. Ct. 366 138 (2006)). The *Hurtado* and *Montejo* courts concluded that § 1028A does not require proof that the defendant knew the means of identification used was of a "real" person. The "plain language" of the statute shows that "knowingly" modifies "transfers, possesses, or uses," and not the phrase "means of identification of another." The statute requires the government to prove that a defendant knowingly possessed, transferred, or used a means of identification which contained identification information belonging to a real person, but the government does not have to prove that the defendant knew that the means of identification was of an actual person. *See also United States v. Hines*, 472 F.3d 1038, 1039 (8th Cir. 2007), *cert. denied*, 128 S. Ct. 235 (2007); *United States v. Godin*, 489 F. Supp. 2d 118, 120 (D. Me. 2007); *United States v. Kowal*, 486 F. Supp. 2d 923, 936 (N.D. Iowa 2007); *United States v. Contreras-Macedas*, 437 F. Supp. 2d 69 (D.D.C. 2006); and *United States v. Crounsset*, 403 F. Supp. 2d 475 (E.D. Va. 2005). *Cf. United States v. Beachem*, 399 F. Supp. 2d 1156 (W.D. Wash. 2005).

The "without lawful authority" element does not require proof of a theft. *United States v. Hurtado*, 508 F.3d at 608 (passport fraud using documents purchased from third party); *United States v. Hines*, 472 F.3d at 1040.

**Sections 1028 and 1028A definitional terms**. The definitions applicable to § 1028 apply to § 1028A. 18 U.S.C. § 1028(d). Although there are several terms defined at 18 U.S.C. § 1028(d), the two terms relevant to §§ 1028(a)(7) and 1028A violations are "means of identification" and "transfer."

> [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 an access device.

18 U.S.C. §1028(d)(7).

> [T]he term "transfer" includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others.

18 U.S.C. § 1028(d)(10).

## VII. Most serious, readily provable offense must be pursued

Federal prosecutors should bear in mind the requirements of the Attorney General's memorandum, dated September 22, 2003, entitled "Department Policy Concerning Charging Criminal Offenses, Disposition of Charges, and Sentencing." *Available at* http://www.usdoj.gov/opa/pr/2003/September/03_ag_516.htm. That memorandum, which requires that federal prosecutors charge and pursue the most serious, readily provable offenses in criminal prosecutions,

applies in cases arising under § 1028A and any other identity theft-related offenses.❖

**ABOUT THE AUTHOR**

❑**Sean Hoar** has served with the United States Department of Justice in Eugene, Oregon, as an Assistant United States Attorney since 1991. His caseload consists primarily of complex white collar and high-tech crime, including identity theft and Internet fraud. He teaches a course in Cybercrime at the University of Oregon School of Law and coordinates the CyberSafe Initiative, a public/private partnership to reduce vulnerabilities in the Internet. He also served on the President's Identity Theft Task Force, which developed federal legislation and other action to combat identity theft at a national level.✠

# Identity Theft and Social Security Numbers: Attacking Identity Theft at its Source

*John K. Webb*
*Deputy Criminal Chief for White Collar and Economic Crimes,*
*Middle District of Tennessee*

## I. Role of social security number in identity theft

The social security number (SSN) is an essential piece of information crucial to the proper functioning of the American financial system. It also plays a significant role in identity theft. SSNs are commonly used to match individuals to their credit and other financial information, which makes it the most sought-after personal identifier by identity thieves.

Identity theft is not typically a stand-alone crime; rather, it is usually a component of one or more white-collar or financial crimes, such as bank fraud, credit card or access device fraud, or the use of counterfeit financial instruments. Thus, identity thieves use the SSN as a key to access the financial assets of millions of unsuspecting victims annually, and misuse of the SSN poses a risk to the personal privacy and financial security of every American. American citizens and legal residents need an SSN to obtain employment, a driver's license, or government benefits, among other uses. For these reasons, the SSN is coveted by identity thieves and other criminals seeking to create false identities or commit financial fraud.

Today, the SSN is a fundamental element of almost every identity theft case, and Congress has long recognized that disclosure of the SSN is a threat to individual privacy. With the enactment of the Privacy Act in 1974, Congress explicitly recognized the particular risk to privacy brought about by the threat of the misuse and unnecessary disclosure of the SSN and enacted express

restrictions on the use of the SSN. Privacy Act, Pub. Law No. 93-579, 88 Stat. 1896 (1974).

The extent of the threat to individual privacy is readily apparent when considering that the SSN is used as an identification code that brings individuals into daily contact with databases containing a wide range of financial, medical, educational, and credit information. Once obtained by an identity thief, the SSN opens practically every door related to a person's identity and personal history and completely compromises an individual's personal privacy. The development and expansion of the Internet has contributed significantly to the danger of identity theft that is inherent to disclosure of the SSN. Today, even with the explosion of identity theft, the demand continues for disclosure of an individual's SSN for purposes unrelated to its initial intended use. The result is the frequent and indiscriminate use and disclosure of the SSN, resulting in even more identity theft crimes.

## II. History, use, and expansion of the SSN

### A. Creation of the SSN

On August 14, 1935, Congress enacted legislation creating the Social Security Administration. *See* Social Security Act (SSA), Pub. L. No. 74–271, 49 Stat. 620 (1935) (codified, as amended, in scattered sections of 42 U.S.C.). The purpose of the Social Security Act was the creation and implementation of a social insurance program designed to pay benefits to retired workers, ensuring a continuing portion of income after retirement. *Id*. The amount of these social benefits was based, in part, on the amount of the workers' earnings. Therefore, the Social Security Administration needed a system to keep track of earnings by individual workers and for employers to report these earnings. Included in the SSA of 1935 was authorization for the Social Security Administration to establish a recordkeeping system to help manage the Social Security program. While it did not expressly mention the use of the SSN, the SSA authorized the creation of some type of recordkeeping scheme. Thus, on or about November 24, 1936, the first "applications for SSNs (Form SS-5)" were distributed by the Post Office Department to persons who were working or expected to work in jobs covered by Social Security old-age insurance. *See* Special Collections-Chronology (*Social Security Online*), *available at* http://www.ssa.gov/history/1930.html.

Over the years, use of the SSN has been expanded by government agencies and the private sector for a variety of purposes. *See, e.g*., A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY 399 (1972). The Social Security Administration Office of Inspector General (SSA/OIG), which operates a fraud hotline to receive allegations of fraud, waste, and abuse, has in recent years reported that one in five hotline calls involve identity theft. *See Prepared Statement of the FTC on Identity Theft and Social Security Numbers*, hearing before the Subcommittee on Social Security, House Committee on Ways and Means (June 15, 2004), *available at* http://www.ftc.gov/os/testimony/04615idtheftssntest.pdf. According to SSA/OIG, the dramatic rise in SSN misuse over the years has resulted partly from opportunities for fraud associated with the status of the SSN as a "de facto" national identifier, which is used exclusively by federal and state governments, banks, credit bureaus, insurance companies, medical care providers, and innumerable other industries. *See* U.S. General Accounting Office, *Identity Fraud*, GAO/SSA-02-830T (June 25, 2002), *available at* http://www.gao.gov/new.items/d02830t.pdf.

### B. Public and private sector expansion of the use of the SSN

The uniqueness and broad applicability of the SSN have made it the identifier of choice for government agencies and private businesses, both for compliance with federal requirements and for the agencies' and businesses' own purposes. In addition, the boom in computer technology over the past few decades has prompted private businesses and government agencies to rely on the SSN as a way to accumulate and identify information for their databases.

**Public sector use of the SSN**. SSN use has grown, in large part, because of federal requirements. Widespread SSN use in government began with a 1943 Executive Order issued by President Franklin D. Roosevelt which

- (i) required all Federal agencies to use the SSN "exclusively" whenever a new identification system for individuals was needed
- (ii) instructed the Social Security Board to cooperate with Federal uses of the SSN by issuing and verifying numbers for other Federal agencies.

*See* Exec. Order No. 9,397; 3 C.F.R. § 283-284 (1943-1948 Comp.). Since the 1943 Executive Order, the number of federal agencies and others relying on the SSN as a primary identifier has escalated dramatically, in part because a number of federal laws have been passed authorizing or requiring use of the SSN for specific activities. *See* U.S. General Accounting Office, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO/SSA-02-352 (May 31, 2002), *available at* http://www.gao.gov/new.items/d02352.pdf.

In many instances, use of an SSN is required by law to determine the eligibility of an individual for receipt of federally-funded program services or benefits, such as SSA Title II benefits (Retirement, Disability, or Survivor's) or Supplemental Security Income benefits payments. Use of the SSN also serves as a unique identifier for such government-related activities as paying taxes or reporting wages and earnings. The government was first permitted to use the SSN for tax reporting purposes in 1961, when Congress authorized the Internal Revenue Service (IRS) to use the SSN as taxpayer identification numbers. *See* Pub. L. No. 87-397, 75 Stat. 828 (1961) (codified as amended at 26 U.S.C. §§ 6113, 6676).

**Private sector use of the SSN**. Since issuance of the first SSN in 1936, the private sector, for all practical purposes, has taken control of the SSN. Individuals must now provide it when applying for credit, when seeking medical or other insurance coverage, for leasing an apartment, seeking cell phone service, ordering merchandise, or applying for a job. Private sector entities such as information resellers, credit reporting agencies (CRAs), and health care organizations generally obtain SSNs from various public and private sources and use SSNs to help identify individuals. *See* U.S. General Accounting Office, *Social Security Numbers*, GAO-04-1099T (Sept. 2004), *available at* http://www.gao.gov/new.items/d041099t.pdf.

Information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing consumer information that includes SSNs for informational services. CRAs, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. Information resellers obtain SSNs from various public sector records, including bankruptcies, tax liens, civil judgments, criminal histories, deaths, real estate ownership, driving histories, voter registrations, and professional licenses. They also mine SSNs from the Internet and frequently employ individuals who go to courthouses to obtain hard copies of public records from which SSNs are gleaned. This widespread use of the SSN invites the attention of identity thieves.

## III. Legislative history regarding criminal misuse of the SSN

In recent years, Congress has become increasingly sensitive to the problem of SSN misuse as a component of identity theft, and Congressional committees have conducted frequent hearings in preparation for offering various legislative solutions to combat the danger. Congress specifically addressed the increasing concern over the need to control the proliferation and misuse of the SSN in 1974, during the enactment of the Privacy Act. Specifically, Section 7 of the Privacy Act made it unlawful for any agency to deny any right, benefit, or privilege to any individual "because of such individual's refusal to disclose his Social Security Account Number." *See* Pub. Law No. 93-579, Sec. 7, 88 Stat. 1896, 1909 (1974). The Privacy Act further

provided that any agency requesting an individual to disclose his or her SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." *Id.* By enacting these protections, Congress sought to prevent the privacy violations made possible by the proliferation of the use of SSNs.

Beginning in 1972, Congress moved to penalize the disclosure and misuse of the SSN by amending the SSA to add misdemeanor penalties for fraudulent use of the SSN. This was specifically designed by Congress to prevent any person from obtaining federal benefits by using a fraudulent SSN. *See* 1972 Social Security Amendments, Pub. L. No. 92-603, 86 Stat. 1320 (1972) (codified as amended in scattered sections of 42 U.S.C.). In response to growing concerns about individual privacy, and the damage that could occur from the fraudulent misuse of a person's identity and SSN, Congress enacted additional amendments to the Act in 1976 and 1981.

The 1976 Amendments to the SSA substantially expanded the reach of the Act's fraud penalty. In addition to penalizing those using false SSNs to obtain Social Security Administration benefits, the 1976 amendments included penalties for individuals who misused social security numbers "**for any other purpose**." Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520 (1976) (codified at 42 U.S.C. § 405(c)(2)(C)(i)) (emphasis added). The House Conference Report to the 1976 Act spoke directly to the broadened statutory language, stating:

> [The Senate amendment] makes a misdemeanor the willful, knowing, and deceitful use of a social security number **for any purpose**. In addition, the Senate amendment changes the Privacy Act so that a State or political subdivision may use social security numbers for the purpose of establishing the identification of individuals affected by any tax, general public assistance, driver's license, and motor vehicle registration laws.

H.R. REP. NO. 94-1515 (1976) (Conf. Rep.) *reprinted in* 1976 U.S.C.C.A.N. 2897, 4030, 4118, and 4194-95.

The 1976 report of the Senate Finance Committee further explained the addition of the language "for any other purpose" to the Act:

> While the Social Security Act currently provides criminal penalties for the wrongful use of a social security number for the purpose of obtaining or increasing certain benefit payments, including social security benefits, there is no provision in the Code or in the Social Security Act relating to the use of a social security number for purposes unrelated to benefit payments. **The committee believes that social security numbers should not be wrongfully used for any purpose**.

S. REP. NO. 94-938(I) (1976), *reprinted* in 1976 U.S.C.C.A.N. 3438, 3819 (emphasis added).

This insightful look into the legislative history of the SSA demonstrates that Congress understood the importance of protecting the SSN from misuse and identity thieves, and intended to make a clear legislative statement for future guidance in protecting the SSN. Courts have since considered and upheld the legislative intent behind the words "for any other purpose." *See United States v. Silva-Chavez*, 888 F.2d 1481 (5th Cir. 1989).

In 1981, Congress once again amended 42 U.S.C. § 408, changing the offense from a misdemeanor to a felony and adding the language "**or for the purpose of obtaining anything of value from any person**" before **"or for any other purpose."** Omnibus Reconciliation Act, Pub. L. No. 97-123, sec. 4, 95 Stat. 1659, 1663-64 (1981) (emphasis added). While the House Conference Report accompanying the amendment offers no explanation of the reasons for the change, *see* H.R. REP. NO. 97- 409 (1981) (Conf. Rep.) *reprinted in* 1981 U.S.C.C.A.N. 2681, 2687-88, the text of the amendment makes clear Congress's intent both to punish a broader range of acts and to impose a stiffer penalty for misuse of the SSN. In summing up the prior law, the House Conference Report stated:

> Criminal penalties are provided for: (1) knowingly and willfully using a social security number that was obtained with false information, (2) using someone else's social security number, or (3) unlawfully disclosing or compelling the disclosure of someone else's social security number.

H.R. REP. NO. 97-409 (Conf. Rep.) (1981) *reprinted in* 1981 U.S.C.C.A.N. 2681, 2687.

## IV. Statutory authority for prosecuting SSN misuse and identity theft

### A. The statutory framework of 42 U.S.C. § 408(a)(7)(A)-(C)

The 1981 Felony Amendments to the Social Security Act, which made SSN misuse a felony punishable by 5 years in prison and a fine up to $250,000, provide prosecutors with a valuable tool for combating identity thieves. *See* Omnibus Reconciliation Act, Pub. L. No. 97-123, 95 Stat. 1659, 1663-64 (1981). The statutory framework of the Act sets forth simple elements for prosecution of identity thieves who use SSNs in their schemes to defraud unwary victims. It is not necessary that the SSN used by a criminal or identity thief actually correspond to an SSN issued to a real person, alive or deceased, by the Commissioner of Social Security. Many criminals make up a number that simply happens to correspond to a valid SSN. The flexibility of the Act's primary criminal provisions relating to misuse of a social security number (§ 408(a)(7)(A)-(C)) make it a popular charging statute for prosecutors. The Act states, in part:

> In general
>
> Whoever–
>
> (7) for the purpose of causing an increase in any payment authorized under this subchapter (or any other program financed in whole or in part from federal funds), or for the purpose of causing a payment under this subchapter (or any such other program) to be made when no payment is authorized thereunder, or for the purpose of obtaining (for himself or any other person) any payment or any other benefit to which he (or such other person) is not entitled, or for the purpose of obtaining anything of value from any person, **or for any other purpose**.
>
> (A) willfully, knowingly, and with intent to deceive, uses a social security account number, assigned by the Commissioner of Social Security (in the exercise of the Commissioner's authority under § 405(c)(2)(A) of this title to establish and maintain records) on the basis of false information furnished to the Commissioner of Social Security by him or by any other person;
>
> (B) with intent to deceive, falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to him or to another person, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to him or to such other person;
>
> (C) knowingly alters a social security card issued by the Commissioner of Social Security, buys or sells a card that is, or purports to be, a card so issued, counterfeits a social security card, or possesses a social security card or counterfeit social security card with intent to sell or alter it.

42 U.S.C. § 408(a)(7)(A)-(C) (emphasis added).

### B. SSN misuse and the identity theft statutes

**18 U.S.C. § 1028(a)(7)**. 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 the 1998 Act as an added protection against SSN misuse.

While the inclusion of the SSN in the statutory definition of means of identification was welcomed by prosecutors, the elements needed to prove a violation of § 1028(a)(7) also required proof that a defendant's transfer or use of a means of identification of another person was in or affected interstate or foreign commerce, or the means of identification was transported in the mail in the course of the transfer or use. Proof of the interstate commerce elements are sometimes problematic, resulting in prosecutors frequently deciding not to charge a defendant with a violation of § 1028(a)(7). Section 408(a)(7)(B) of the social security felony fraud statute, which governs SSN misuse, does not require proof of an interstate commerce nexus. Thus, it is sometimes much easier for a prosecutor to use § 408(a)(7)(B) when faced with charging decisions against an identity thief who has used the SSN of a victim.

**18 U.S.C. § 1028A (Aggravated Identity Theft)**. The Identity Theft Penalty Enhancement Act of 2004 (ITPEA) created a mandatory term of imprisonment of 2 years for those convicted of knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person. *See* Pub. L. No. 108-275, 118 Stat. 831 (2004). When enacting the ITPEA, Congress adopted the definition of "means of identification" found in 18 U.S.C. § 1028(a)(7), which included 42 U.S.C. § 408(a)(7)(B) (SSN Misuse) as a predicate offense for charging a violation of aggravated identity theft.

## V. Charging SSN misuse in identity theft prosecutions

The felony provisions of 42 U.S.C. § 408(a)(7)(A)-(C), which deal with the misuse of an SSN, are particularly effective in charging cases involving identity theft. As previously mentioned, the elements of proof for each subsection of § 408(a)(7) are more flexible than those required by 18 U.S.C. § 1028, and the SSA is a predicate felony for purposes of charging aggravated identity theft under 18 U.S.C. § 1028A. The following is a description of each of the three subsections of § 408(a)(7), including a breakdown of the elements necessary to prove a charge under each and a brief suggestion of when and how each subsection should be charged.

**42 U.S.C. § 408(a)(7)(A)**

**Elements of proof**

- willful and knowing use of a social security number;
- with intent to deceive;
- based on false information furnished to the Commissioner of Social Security.

*See* 42 U.S.C. § 408(a)(7)(A).

**When to charge**

Any fraudulent use of a SSN, whether made-up by the offender or obtained on the basis of false information supplied to the Social Security Administration and used deceitfully, is actionable and constitutes a felony for purposes of § 408(a)(7)(A). For example, a subject in the United States on a tourist visa secures a nonwork SSN using his French passport. The subject then uses an alias to file a bogus application for asylum, resulting in Immigration and Customs Enforcement (ICE) approval and issuance of a green card and alien registration number. The subject then uses his new name and illegally procured ICE documents to apply for a second SSN, thus completing the creation of a new identity. The subject then uses the second SSN to secure credit cards, open bank accounts, and apply for employment. The subject's use of the SSN is actionable because he used false and fraudulent documents (deceptively procured from ICE) to deceive the Social Security Administration into issuing him a new SSN. *See United States v. Pryor,* 32 F.3d 1192 (7th Cir. 1994) (defendant acted "willfully, knowingly, and with intent to deceive" in illegally using an SSN obtained on the basis of false information).

**42 U.S.C. § 408(a)(7)(B)**

**Elements of proof**

- false representation of a social security number;
- with intent to deceive;
- for any purpose.

*See United States v. Means*, 133 F.3d 444, 447 (6th Cir. 1998) (setting forth the elements for prosecution of a case under 42 U.S.C. § 408(a)(7)(B)); *see also United States v. McCormick*, 72 F.3d 1404, 1406 (9th Cir. 1995).

**Alternative elements**

The majority of jurisdictions apply the *Means* standard, as set forth above. However, a few jurisdictions break down the language of § 408(a)(7)(B) to include a fourth element:

- for any purpose;
- with intent to deceive;
- represented a particular social security account number to be his;
- which representation is false.

*See United States v. O'Brien*, 878 F.2d 1546 (1st Cir. 1989).

**When to charge**

Subsection (B) is the most commonly charged subsection of § 408(a)(7) because of its broad application and straightforward elements of proof. It is typically charged whenever a subject has stolen a victim's identity and fraudulently used the victim's SSN. The charging standard, "for any purpose," is broad and self-explanatory, and any false representation of an SSN, with an intent to deceive, is actionable conduct that may be charged as a felony under § 408(a)(7)(B). *See United States v. Silva-Chavez*, 888 F.2d 1481 (5th Cir. 1989).

The definition of "identification document includes social security numbers." According to 18 U.S.C. § 1028(d)(3), an "identification document" is "a document made or issued by or under the authority of the United States Government . . . which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals." The House Report accompanying what became § 1028 demonstrates that the definition includes not only "identification documents, such as driver's licenses, which are widely accepted for a variety of identification purposes," but also those " 'commonly accepted' in certain circles for identification purposes, such as identification cards issued by state universities and Federal government identification cards." H.R. REP. NO. 802, 97th Cong., 2d Sess. 9 (1982), *reprinted in* 1982 U.S.C.C.A.N. 3519, 3527. The House Report also notes that identification documents "normally will include such identifying elements as an individual's name, address, date, or place of birth, physical characteristics, photograph, fingerprints, employer, or any unique number assigned to an individual by any Federal or State government entity." *Id.*

Decisions from the Fourth and Ninth Circuits have confirmed that social security cards are identification documents within the meaning of 18 U.S.C. §1028(a)(2), which provides criminal penalties for anyone who "knowingly transfers an identification document . . . or a false identification document knowing that such document . . . was stolen or produced without lawful authority." *See United States v. Abbouchi*, 494 F.3d 825 (9th Cir. 2007). *Abbouchi* addresses the previously unsettled question of whether social security cards fit within the definition of the identity theft statute (18 U.S.C. § 1028(d)(3)). While the question of social security cards as a means of identification was first addressed in 1985 by the Fourth Circuit in *United States v. Quinteros*, 769 F.2d 968, 970 (4th Cir. 1985) (court relied on testimony that social security cards were "commonly accepted" as identification documents), other jurisdictions have either refused to affirmatively address the question or have ignored it (largely because the Social Security Administration has remained steadfast in its contention that social security cards are not intended to be used for identification purposes).

Since enactment of 18 U.S.C. § 1028(a), the question has not been properly addressed in the context of identity theft. However, with its decision in *Abbouchi*, the Ninth Circuit effectively put the issue to bed by referencing both *Quinteros* and the legislative history of 18 U.S.C. § 1028(a)(2) in reaching its decision. Abbouchi had argued that social security cards were not "identification documents" within the meaning of 18 U.S.C. § 1028(a)(2). As in *Quinteros*, the court in *Abbouchi* accepted the testimony of a Social Security Administration expert that social security cards are commonly accepted as identification. *Id.* Indeed, the expert testified that the Social Security Administration issues cards to senior citizens for use as identification for cashing checks and that the organization removed the "Not for Identification Purposes" legend from these cards in 1972, to reflect the emerging use of social security cards as a form of identification. *See also United States v. Hammoude*, 51 F.3d 288, 292 (D.C. Cir. 1995) (the definition of "identification documents" includes social security cards and Form I-94 Arrival-Departure Records).

**42 U.S.C. § 408(a)(7)(C)**

**Elements of proof**

- knowingly alters a social security card; or
- counterfeits or possesses a social security card with intent to sell or alter it;
- or defendant buys or sells a social security card.

**When to charge**

This subsection is typically charged when a subject has knowingly altered a social security card (usually to remove work restrictions from the face of the card), or has manufactured or counterfeited a card or cards for sale on the black market. This section can also be charged when an individual is discovered to have purchased a social security card for his own use or for resale. Counterfeit SSNs are frequently used by identity thieves when hijacking a victim's identity and accessing existing accounts, opening new accounts, and cashing forged or counterfeit checks.

## VI. Conclusion

The SSN is a fundamental element of almost every identity theft case, and Congress has long recognized that disclosure of the SSN is a threat to individual privacy. The extent of the threat is readily apparent when considering that the SSN is used as an identification code that brings individuals into daily contact with public and private sector databases containing a wide range of financial, medical, educational, and credit information. Once obtained by an identity thief, the SSN opens practically every door related to a person's identity and personal history, and completely compromises an individual's personal privacy. The Social Security felony fraud statute provides excellent tools for prosecutors who are faced with charging decisions that sometimes require simple elements for proof of SSN misuse.❖

**ABOUT THE AUTHOR**

❑**John K. Webb** is Deputy Criminal Chief for White Collar and Economic Crimes with the United States Attorney's Office (USAO) for the Middle District of Tennessee. Previously, Mr. Webb was an Assistant United States Attorney in the Major Frauds Section of the USAO for the Central District of California, Los Angeles, where he served as Identity Theft Coordinator and prosecuted white collar fraud and economic crimes. Mr. Webb is a frequent lecturer on the topics of identity theft, SSN misuse, and federal benefits fraud, and regularly provides training on identity fraud for federal, state, and local law enforcement agencies. He has served as an instructor at the National Advocacy Center and regularly contributes articles on identity theft, social security number misuse, and other topics to the *USA Bulletin*. Mr. Webb is the author of Chapter Six of "Identity Theft and Social Security Fraud," a treatise published by the U.S. Department of Justice Executive Office of United States Attorneys.✠

# Identity Theft Sentencing

*Richard W. Goldberg*
*Chief of the Financial Institution Fraud and Identity Theft Section*
*Eastern District of Pennsylvania*

## I. Introduction

When working up an investigation, prosecutors generally focus on trial, as they should. The burden of proof is a burden, frequently exacerbated by evidence gone missing on the trial's opening day. The sentencing is an afterthought, which some superstitiously will not even consider until the defendant stands convicted.

The defense, however, is focused on sentencing from minute one. An acquittal or immunity would be nice, but the odds are that the defendant will be convicted. From the start, the task is to minimize the punishment at sentencing.

Prior to *United States v. Booker*, 543 U.S. 220 (2005), the Sentencing Guidelines worked their logical and regimented process, and sentencings were fairly rote, predictable events. After *Booker*, those sentencings became sweet nostalgia. The door had been opened for all manner of mitigating evidence intended to reduce the sentence.

In identity theft cases, that open door swings both ways and provides an opportunity, in fact a responsibility, to educate the sentencing court on the crippling effect of this crime. Evidence can now be presented which, while it might have been introduced in the past by way of the occasional upward departure motion, is more readily admissible in a broader *Booker* inquiry. All that is required is to gather information from the victims and fully present the crime's impact to the court.

This article focuses on building good sentences in identity theft cases. The central tenet is that the individual victim's experience must be brought into the courtroom.

## II. Building sentences

After *Booker*, constructing a government identity theft sentencing presentation is a five-part process.

### A. Collecting sentencing evidence

While all prosecutions and sentencings require the gathering of evidence, identity theft cases present unique challenges. First, the size of the victim community is generally unknown. The defendant was caught pretending to be three different employees of a drug company. Are these the only victims or is the entire employee list at large? How many other members of this criminal's community have that employee list? Was the theft upstream of this company so that other companies have also had their personnel information stolen?

Moreover, once the victim group is defined, the notification issues may seem monumental. Nevertheless, the victims need to be found and queried as to whether they have suffered an identity theft.

Convincing the agent on the case to investigate the victim group is crucial. Most agents are eager to work when their efforts result in increased restitution or an enhanced sentence for the identified defendant. If they get pressure to move on to other cases, it may help to emphasize that an investigation of other victims may result in additional charges against the known defendant or uncover additional defendants.

Once the targeted community is identified, relevant information about each victim should be obtained. Before *Booker*, the victim's actual losses were used to calculate the guidelines and subsequent restitution. After *Booker*, however, the court is directed to 18 U.S.C. § 3553, which makes relevant a broader range of evidence. In forming its sentence, the court "shall consider" the nature and circumstances of the offense. 18 U.S.C. § 3553(a)(1). The sentence must reflect the "seriousness of the offense . . . and provide [a] just

punishment for the offense." *Id*. at § 3553 (a)(2)(A).

This makes relevant an entire spectrum of consequential damages from the crime which were not particularly germane under the Sentencing Guidelines. So, in querying the victim community, in addition to determining the victims' "actual loss" as defined by the Guidelines, it is worth asking the following questions:

- How much time did the victim spend on making it clear that he or she did not authorize the use of his or her identification information (which could mean clearing credit history or other work to show that the victim did not make the unauthorized purchases or commit a crime)?
- As a result of this crime, was the victim unable to do something (get a job or obtain a loan to buy a house or send a child to college)?
- Did the rate on any of the victim's loans change as a result of this crime?
- Has the victim been accused of a crime as a result of what the defendant did?
- Has the victim's reputation suffered as a result of this crime?
- Has this crime affected the victim's work or caused embarrassment?
- Has the victim suffered emotionally as a result of this crime?
- Has the victim suffered physically as a result of this crime?
- Does the victim have particular concerns about a spouse or family member as a result of this offense (such as causing a spouse to lose a security clearance or job)?
- Has this crime created any other disruption for the victim or his or her family?

These questions are obviously and purposefully open-ended. The myriad effects of identity theft are as disparate as the ways in which the victims live their lives and organize their finances. A low-dollar financial crime may have virtually no impact on a wealthy victim, but may emotionally cripple a single parent struggling to make ends meet. As discussed below, the collateral consequences of the defendant's crime, while not generally relevant to the Sentencing Guideline calculation, are relevant at sentencing and should be presented to the court.

## B. The Sentencing Guidelines framework

The sentencing process, of course, begins with an application of the Sentencing Guidelines to the case. In the vast majority of identity theft cases, only two Guidelines sections are used in determining the offense level: U.S.S.G. § 2B1.1, or §§ 2L2.1 or 2L2.2 (2007).

Immigration document fraud cases are governed by U.S.S.G. §§ 2L2.1 and 2L2.2 (2007). Adjustments under these sections are largely mathematical and simple: number of documents, alienage, prior offenses, and use of passports.

The analysis under the financial fraud guideline, Section 2B1.1, is entirely different. The first issue arises in the first clause. The base offense level depends on the charge of conviction, as a defendant convicted of a crime with a maximum sentence of over 20 years imprisonment (such as bank fraud) is awarded an initial Level 7, rather than a Level 6. U.S.S.G. § 2B1.1(a)(1) (2007).

The next adjustment is for loss, which the Guidelines generally define as actual or intended loss. U.S.S.G. § 2B1.1, cmt. n.3 (2007). Loss is defined as "pecuniary harm," meaning that it must be measurable in money. *Id*. cmt. n.3(a)(III). Emotional distress, harm to reputation, and nonmonetary harms, are specifically excluded. Credit cards are subject to a special rule, in that unauthorized or counterfeit cards are each counted as at least a $500 loss. *Id*. cmt. n.3(F)(I).

Several other adjustments may apply in identity theft cases. These include adjustments for the number of victims, for a defendant in the business of receiving stolen property, for relocating the scheme to another jurisdiction to evade law enforcement, and for use of sophisticated means. *Id*. §§ (b)(2), (4), (9).

Identity theft crimes are also covered by Section (b)(10), which is specifically written for application to these cases. This section provides for a 2-level increase (or to level 12, if it has not yet been reached) if the defendant:

- (A)(i) possessed device-making equipment
- (B)(i) produced an unauthorized or counterfeit device (such as a credit card)
- (C)(i) transferred or used identification information to get another identification
- (C)(ii) possessed five or more identifications that were produced from identification information.

U.S.S.G. § 2B1.1(b)(10) (2007).

The first two categories are straightforward. The second two categories are the "breeder" provisions. These sections refer to the defendant's taking stolen identity information and using it to create items which act as identification, such as using stolen identification information to get a driver's license or open a credit card or bank account. *Id*. cmt. n.9, background. An example of conduct not covered by this provision is using a stolen credit card or cashing a stolen check.

A caveat is necessary regarding the aggravated identity theft statute, 18 U.S.C. § 1028A. It is frequently used in identity theft cases with its mandatory minimum sentence of 2 years' imprisonment. U.S.S.G. § 2B1.6, cmt. n.2 (2007) states that, if a sentence is imposed under § 1028A, "do not apply any specific offense characteristic for the transfer, possession, or use of a means of identification when determining the sentence for the underlying offense." This should apply only to the means of identification charged in the § 1028A count. It could, however, be used to knock out all of the § 2B1.1 specific offense adjustments discussed above.

The final step in the Sentencing Guidelines offense level process involves the Chapter 3 adjustments. Identity theft cases are particularly apt for these adjustments.

Section 3A1.1 adds two levels where the defendant knew, or should have known, that the victim was vulnerable. U.S.S.G. § 3A1.1(b)(1) (2007). Defendants in identity theft cases frequently victimize the elderly in the belief that they will be slow to discover the crime. Where there are a large number of vulnerable victims, as in the theft of the identification records of a retirement home, an additional two levels can be added. *Id*. § 3A1.1(b)(2).

Section 3A1.2 applies an enhancement where the crime has an official victim. U.S.S.G.§ 3A1.2 (2007). For this adjustment to apply, the offense must have been motivated by the official status of the victim. Such an adjustment would obviously apply for retaliation against a law enforcement officer following arrest, but could also apply in the case of a military or government identification theft.

The last victim-related adjustment is for an offense that involved, or intended to promote, terrorism. U.S.S.G. § 3A1.4 (2007). Such an enhancement, of 12 levels or to level 32, could apply in an identity theft case where false documents were obtained in furtherance of a terrorism scheme.

Role-in-the-offense adjustments are also frequently applicable in identity theft cases. Section 3B1.3 adds two levels for abuse of a position of public or private trust, or use of a special skill which significantly facilitated the commission or concealment of the offense. U.S.S.G. § 3B1.3 (2007). The commentary to this section is directed specifically to identity theft: a defendant who exceeds the authority of his position to obtain a means of identification receives the enhancement. *Id*. cmt. n.2(B). The examples given include a volunteer at a charitable organization, a hospital orderly, and a motor vehicle bureau employee who purloins information. Thus, the adjustment should apply to virtually all identity theft "insiders." Even bank tellers, who are exempt from application of this section for the purposes of embezzlement sentencing, are exceeding their authority when they steal identification information.

Investigations which uncover identity theft rings or kingpins will be able to use the leadership enhancement. U.S.S.G. § 3B1.1 (2007). This standard adjustment, which varies based on the number of perpetrators and the defendant's role in the organization, varies from a 2 to 4 level offense level increase.

The Guidelines also provide two additional offense levels for obstructing the administration of justice. U.S.S.G. § 3C1.1 (2007). Be warned that merely providing a false name or document at arrest does not earn this enhancement unless that conduct "resulted in a significant hindrance" of the investigation or prosecution. *Id*. cmt. n.5(A). Other conduct in identity theft cases may support the enhancement if the defendant persists in claiming a false identity, such as producing a counterfeit document or providing materially false information to a judge or magistrate. *Id*. cmt. n. 4 and (f).

Before leaving the Guideline calculation section, a word about the criminal history section. Criminal histories in identity theft cases are calculated like histories in other cases. There is a criminal livelihood section which can take a defendant's offense level to 13, if the government can show that criminal conduct was the defendant's primary occupation during a twelve-month period. U.S.S.G. § 4B1.3 (2007). This can be proven by showing that the defendant derived more than 2,000 times the existing federal hourly minimum wage through a pattern of criminal conduct during twelve months. *Id*. cmt. n.2. Of course, it is likely that other provisions of the Guidelines would raise the offense level of such a persistent felon far in excess of 13.

## C. Upward departures

Because the Guidelines specifically state that nonfinancial harms are not to be considered in offense level calculations, identity theft cases, which are rife with such harms, are excellent candidates for government upward departure motions. In fact, the Guidelines specifically invite such motions.

The commentary to § 2B1.1 lists many areas for upward departure consideration which are applicable in these cases. First are the general "not adequately addressed in the guidelines" type departures: causing or risking substantial nonmonetary harm, substantial expense (late fees, penalties, interest) not considered in the loss calculus, and risk of substantial loss, also not considered in the loss calculus. U.S.S.G. § 2B1.1, cmt. n.19(a)(ii), (iii), (iv) (2007). Thus, the attorney fees or increased interest a victim must pay because of an identity theft can be grounds for an upward departure.

The Guidelines, however, get even more specific about possible upward departures in identity theft cases. In these cases, the court is encouraged to consider these upward departure factors:

- Whether the offense caused substantial harm to the victim's reputation or credit record, or whether the victim suffered inconvenience in attempting to fix the damage.
- Whether the victim was erroneously arrested or denied a job because of the theft.
- Whether the defendant obtained many identifications in one victim's name, attempting, on a comprehensive scale, to assume the victim's identity.

*Id*. n.19(vi).

Last, because the damage suffered by identity theft victims takes so many forms, it is useful to remember the catch-all upward departure section which permits a departure for an aggravating circumstance not adequately taken into consideration by the Sentencing Commission in formulating the guideline range. U.S.S.G. § 5K2.0 (2007).

Remember to provide notice of a request for upward departure before sentencing. Opinions which have upheld upward departures in identity theft cases are *United States v. Karro*, 257 F.3d 112, 121 (2d Cir. 2001); *United States v. Sample*, 213 F.3d 1029, 1032-34 (8th Cir. 2000); *United States v. Wells*, 101 F.3d 370, 372-75 (5th Cir. 1996); *United States v. Akindele*, 84 F.3d 948, 952-56 (7th Cir. 1996).

## D. *Booker*

As the Supreme Court set forth in *United States v. Booker*, 543 U.S. 220 (2005), the sentencing bases in 18 U.S.C. § 3553 must be explicitly considered by the court in imposing sentence. *Id.* at 259-61. The Sentencing Guidelines are not irrelevant in this consideration, but are only advisory. Defense attorneys view the § 3553 categories as an opportunity to present mitigating evidence to the court, heretofore irrelevant by operation of the Guidelines. They want to present a broader picture of the defendant's life, showing the impact of sentencing and the possibility of a bright future for the defendant.

Prosecutors must use the door opened by *Booker*, particularly in identity theft cases. The seriousness of the offense is an explicit factor to be considered by the sentencing court. 18 U.S.C. § 3553(a)(2)(A). Our victims' futures are often permanently clouded by identity theft. In a violent crime case, there is unlikely to be a further crime once the violent event is over and the defendant has been incarcerated. In many simple fraud cases the victim is made whole by restitution. Stolen medical records, which can be taken to a copy center and reproduced hundreds of times and then sold and resold, can lead to victimization in perpetuity, complete with embarrassment, anxiety, financial loss, and inconvenience. As described by one victim:

> Numerous doctor's visits were necessary as a result of my high blood pressure escalating to dangerous levels. I experienced loss of sleep as well as feelings of fear, anger, and paranoia. Can you imagine the surprise of discovering that your identity had been stolen especially from your Credit Union which is supposed to be safe and employ trustworthy respectable individuals?! I am experiencing psychological scars as I am having great difficulty in moving on as a result [of] this incident.

*United States v. Brown*, Crim. No. 01-204 (E.D. Pa. 2002) (government sentencing memo).

Painting a vivid picture of the victim's future anxiety must be done with evidence. This highlights the importance of finding and interviewing victims, or at least sending them a questionnaire, so that their information can be placed before the sentencing judge.

Last, alternative pleading should be employed to ensure that the court has the maximum flexibility in determining a sentence. Having been provided with evidence of the devastating impact of this crime, the court may want to grant both an upward departure and make a ruling under *Booker* to protect the sentence.

## E. Meeting defenses

Where a financial institution has made the victims whole, defendants attempt to substitute the bank as the victim. Thus, they argue, there should be no multivictim-enhancement or other victim-oriented adjustment, such as vulnerable victim.

In meeting such a claim, it is important to remember that the Guidelines define "victim" as "any person who sustained any part of the actual loss" under the Guidelines calculation, which means harm readily measurable in money. U.S.S.G. § 2B1.1, cmt. n.1, and n.3(A)(i) and (iii) (2007). It will probably not be sufficient to cite the centrality of the victim's information to the crime or the victim's loss of security, neither of which are monetary harms. A better argument, perhaps, is that, until the bank decided to make the victim whole, the victim bore the loss. This is sufficient for the Guidelines definition of victim as one who bears "any part" of the loss. *See United States v. Lee*, 427 F.3d 881, 894-95 (11th Cir. 2005) (victims who were reimbursed by a third party are still considered victims for purposes of counting the number of victims), *distinguishing United States v. Yagar*, 404 F.3d 967, 970-72 (6th Cir. 2005) (small short-lived loss reimbursed by a third party does not render a victim countable for purposes of the number of victims enhancement).

Of course, losing such a battle over these guidelines enhancements is not fatal. That the Guidelines calculation does not include the

number of victims who had their identities stolen in determining the defendant's sentencing range simply provides more support for an upward departure or enhanced sentence under *Booker*.

## III. Conclusion

Prior to *Booker*, the Sentencing Guidelines could be relied upon to provide an orderly, fairly simple, and comprehensive method for sentencing. A Guideline sentencing proceeding typically demanded little of prosecutors because the Guidelines constricted relevant sentencing evidence enough that there was little to be presented to the court beyond that established at trial.

That world is gone. The sentencing process described above will require more work by law enforcement. With the door to the sentencing proceeding opened, however, prosecutors have been given a new opportunity to bring the victim's experience before the court and enhance sentences in identity theft cases.❖

**ABOUT THE AUTHOR**

❑**Richard W. Goldberg** is Chief of the Financial Institution Fraud and Identity Theft Section of the United States Attorney's Office for the Eastern District of Pennsylvania (Philadelphia). He is also a Computer Hacking Intellectual Property prosecutor and previously supervised the Narcotics and Major Crimes sections. Before joining the office, he worked for eight years in the Philadelphia District Attorney's Office.✠

# Task Force Versus Working Group: A Small District Perspective

*Alfred Rubega*
*Assistant U.S. Attorney*
*District of New Hampshire*

## I. Introduction

In New Hampshire, we have a "working group," not a "task force." New Hampshire is a small district, with only twenty-four attorneys, in a single office. In early 2002, the U.S. Attorney, and a particularly aggressive and talented Postal Inspector, decided that the District should have a focused response to identity crimes.

The possibility of setting up an Identity Crimes Task Force was briefly considered, but was quickly rejected, because a properly run task force requires dedicated personnel from participating agencies and a committed physical space. None of the prospective member agencies were able to provide these resources. Also, many of the agencies that are responsible for identification theft and fraud investigations in New Hampshire have no agents based in the state, but rather work out of offices in Boston, Massachusetts. Therefore, a "working group" was created where the agencies would meet monthly to share information, learn new strategies, and develop case leads.

The "working group" model allows for participation by many federal, state, and local agencies, on an informal basis, with no requirement for dedicated resources. Agents can be members of the Identity Crime Working Group while they still maintain their other responsibilities and workloads. This more low-key approach, albeit dictated by the relative scarcity of available resources, has nonetheless resulted in an

abundance of interesting and significant cases, along with other worthwhile work.

This article is written in an effort to provide a simple and efficient template for use in starting up and maintaining an Identity Crimes Working Group. The belief is that what has worked for the District of New Hampshire will be of particular value to AUSAs from a same-size, or smaller, district.

## II. The five main factors that worked for the District of New Hampshire

- Regular meetings at the United States Attorney's Office, on the same day each month, at the same time, for whomever can make it;
- E-mail reminders to the entire membership list several days before the meeting;
- Additional e-mail distribution of other useful information, such as Be On the Lookout (BOLO) warnings, computer virus warnings, descriptions of fraud techniques, and other noteworthy items, between meetings;
- Educational presentations to the working group, whenever possible, by members or outside agencies and/or entities, to include vendors of tools, such as facial recognition and other law enforcement-useful software, as well as the occasional hosting of off-site meetings by member agencies;
- Completely voluntary participation in all respects, no minimum participation, attendance, or other requirements, and broadly inclusive "membership" criteria.

## III. Why have these factors worked?

### A. Regular meetings

This may seem a mundane or unimportant detail, but it is not. For one thing, it reduces the likelihood of "dropping the ball" on logistical details (such as reserving a conference room) associated with hosting the meeting, since the day and time of the regular meetings do not vary.

The same day, time, and place regularity also simplifies the composition of the e-mail reminder notices and lessens the possibility that the AUSA, or his or her support staff, will forget to send them.

Most important of all, the regular meeting structure helps to encourage attendance, since members can plan on a regular basis for the meetings and can place the meetings on their calendars well in advance. Agents sometimes lose track and miss meetings they want to attend if the date, time, and place is a constantly moving target, for which they cannot regularly plan. Consequently, they may tend to give up on attendance if the meeting date, time, and place frequently changes.

With a standard meeting structure, the point of contact will probably find, after a while, that the more regularly attending, productive, and enthusiastic members will begin to call or e-mail in advance of the usual meeting date to ensure that it is still on, if they have not received the e-mail reminder notice. This can serve as a needed reminder to send the notice.

Finally, it has been found that attendance will be maximized by avoiding meetings on Mondays or Fridays, or near the beginning or end of the month. This is why the District of New Hampshire has chosen to meet on the third Tuesday of each month.

### B. E-mail reminders

This needs little elaboration. Each month, add the correct date to the standard notice and send it out. These reminders are effective for busy agents who have many other duties and responsibilities. They also help keep the meetings interesting by reminding the agents to bring new cases or information to discuss with the group. A sample of the e-mail follows.

Dear Group Member:

Reminder -

This month's Identity Crimes Working Group meeting will be:

1:30 PM, Tuesday, April 17, at the U.S. Attorney's office.

As always,

Please bring anything that would be of interest to the group members, including pertinent information on any cases you'd like to be considered for prosecution by this office, or on any cases with which group members might be able to assist with the investigation.

Hope to see you Tuesday.

Al

## C. Additional e-mail distribution of information between meetings

This can consume a lot of time, in that some members will often send in a large volume of material for distribution. The extra e-mails amount to "cyberspace" operation of the group, efficiently advancing its work, and enabling members who are chronically unable to attend meetings to benefit from, and productively contribute to, the work of the group. Even if the members do not always get together in person, knowing that they can call or e-mail other group members who have a specialized expertise will advance a lot of investigations which otherwise might stall.

If members are consistently provided with useful material that can advance their investigations, the group will benefit from continued referrals of cases from even those members who cannot attend all of the meetings.

## D. Educational presentations

This is by far one of the best tools for encouraging meeting attendance and enhancing the value and utility of meetings. It can also be one of the most burdensome logistically, because the Point of Contact (POC) is responsible for recruiting presenters and coordinating everything that they will need.

It is possible that the POC might be blessed with one or two members who are not only willing, but eager, to host a meeting at their facility once a year or so, in order to educate the membership as to who they are and what they do. This is especially true with less well-known federal agencies. Some of these agencies have a mandate to conduct periodic agency outreach. Having such agencies host a meeting produces an "everybody wins" situation.

By the way, accommodating the needs of an other-than-USAO host is the one exception that this District allows to the rule that meetings should always be at the same time, day, and place. Generally, we have found that the novelty of an occasional meeting in a different place overcomes any concomitant disadvantages.

## E. Completely voluntary and broad participation

Regardless of how fascinating and important this work is, most group participants work in more than just this area and have their priorities set by others.

This is especially true of detectives from local police departments. It is standard operating procedure, and is simply understood, that the detective tasked with white collar investigations for a local department does not do this work exclusively. Often these detectives have to work on high priority violent crime cases before they can get to their identity crime investigations.

This requires understanding that their participation will be very irregular. Make clear to one and all that they are welcome whenever, and to whatever extent, they are able to make it, and that they do not need to be concerned or embarrassed about low-level participation. Usually, they would love nothing more than to be more active and are not only because they have no choice. The only time they are heard from may be when they bring in the best case of the year. Everyone in the working group knows that their participation is voluntary. If the POC is too rigid or demanding, he or she will very soon be alone in the room.

The group will work best if all federal and state agencies that have responsibility over all forms of licensing, benefits, and visas and passports, in addition to local police departments, are included. This District has found that the law

enforcement agency that oversees motor vehicle licensing, registration, and titles (New Hampshire Highway Patrol) is indispensable. This agency reports directly to the Director of Motor Vehicles. They have been found to be a treasure trove of information and a great source of cases and leads.

AUSAs may be asking, what does this have to do with the practice of law? Good question. The answer is that it is not the practice of law, it is the administration of law enforcement. The AUSA designated as the district's Identity POC might have been named because he or she has "been there, and done that," and due to previous administrative or supervisory experience, someone in authority believes that the AUSA is well qualified to run a task force or working group.

If on the other hand, the appointed AUSA has not "been there and done that," this is a good opportunity for him or her to demonstrate to those who assigned the collateral duty that he or she has what it takes.

In summary, the Identity POC has a great opportunity to make a critically important difference to the citizens served, in an area of the criminal law that is a high priority for the Department of Justice. Congratulations and best of luck.

### IV. The easier-said-than-done category

Do not get discouraged if interest and participation falls off temporarily. Some of the best cases may result from some of the most poorly attended meetings. Even if only one other person attends the meeting, which might happen, keep the process moving each month. If the AUSA operates a working group for any length of time, he or she is likely to end up with a good deal more work than he or she can handle.

If you have a good solution to this last problem, please tell me.❖

**ABOUT THE AUTHOR**

❑**Alfred Rubega** is an Assistant United States Attorney in the District of New Hampshire.✠

# Model Programs: Eastern District of Pennsylvania

*Richard W. Goldberg*
*Chief of the Financial Institution Fraud and Identity Theft Section*
*Eastern District of Pennsylvania*

### I. Introduction

Law enforcement in the Eastern District of Pennsylvania faces identity theft issues typical of any major urban area. A large number of institutions control the identity information of millions of people, and the area has a veteran criminal community with the experience to exploit these institutions. Law enforcement agents in this area, however, are experienced in investigating and apprehending these criminals.

To maximize law enforcement's impact on identity thieves, the United States Attorney has adopted a three-part strategy.

- First, the coordination of law enforcement efforts in this area is paramount, an especially

difficult task because of the dispersed nature of identity theft information reporting. To facilitate information exchange, the U.S. Attorney's Office initiated the Regional Identity Theft Working Group.

- Second, to encourage agencies to refer identity thieves for federal prosecution, the U.S. Attorney's Office changed its prosecution policies.
- Third, the U.S. Attorney's Office has been involved both in identity theft training for law enforcement and outreach to public and private institutions, to remind them of their responsibility to safeguard information.

These initiatives are described below.

## II. The Working Group and Regional Identity Theft Network (RITNET)

The Regional Identity Theft Working Group consists of fraud investigators from local, state, and federal agencies, including state and local prosecutors. The Group is not a formal task force, and therefore, required no dedicated personnel or equipment. The Group initially met to exchange information about known fraud targets or schemes. The membership quickly realized that, while cooperation was important, it was a slow and unwieldy process. In an economy where identity thieves can victimize ten people from ten different jurisdictions in an hour at a shopping mall, law enforcement had to move quickly to stop identity theft gangs from exploiting information gaps between law enforcement agencies.

There is no central aggregation of identity theft information reported by victims and merchants. Small thefts committed in multiple jurisdictions, or reported to various local, state, or federal agencies, are not connected to similar thefts to reveal the workings of these gangs. A police department investigating a gang will have little chance of discovering whether other agencies are investigating the same gang.

This is also true in terrorism, drug, and firearm trafficking investigations, where false identities are being used.

The Working Group's solution was the creation of RITNET, which is designed to contain data on all stolen or criminally used identity information. This content will be uploaded from collecting agencies to RITNET, through the Mid-Atlantic Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN). The data will include locale, state, and federal law enforcement generated information, as well as victim reports through the Federal Trade Commission, delivery information from the United States Postal Service, and banking information through an industry clearinghouse. The content will be accessible by local, state, and federal law enforcement over a secure internet connection through the Regional Information Sharing System network (RISSnet), which is available nationwide to member law enforcement agencies.

RITNET will provide a central repository of stolen identity information. This will allow agencies to learn immediately whether a particular piece of identification (driver's license, credit card, address, social security number, among other things) has been reported stolen or used elsewhere in the course of a crime. It will also name investigators, thereby permitting agencies to coordinate when working on crimes involving the same, or connected, identities or credit card numbers. It will also allow law enforcement agencies to query the system to look for patterns revealing the operation of identity theft gangs and will help locate the sources of stolen identification information. The goal, of course, is to increase the number of identity theft gang and kingpin prosecutions.

Use of RITNET is free. All that is required is that agencies join MAGLOCLEN and sign a Memorandum of Understanding which requires agencies querying the database to contribute information to the database.

Local, state, and federal criminal investigators in the Working Group designed the RITNET database. Programming was underwritten by the

United States Postal Inspection Service. It is now being made available to local law enforcement agencies.

## III. Prosecution policies

The U.S. Attorney's Office has adopted two policies to encourage law enforcement agencies to refer cases for federal prosecution, in particular using the aggravated identity theft statute and its mandatory 2 year prison sentence.

- First, the U.S. Attorney's Office has adopted a zero dollar loss case intake policy. This means that, if a referring agency can demonstrate that a case has the potential to become a substantial or important case, the office will work the case whether or not the loss amount on the referred defendant or scheme is large. Thus, a mid-level identity thief in an organization could be prosecuted in a small dollar loss case, as part of a strategy to locate and capture the insider who is feeding information to the organization.
- Second, the Office has adopted a policy of charging aggravated identity theft, with its mandatory minimum sentence, whenever possible. The Office is also frequently seeking upward departures from the Sentencing Guidelines ranges because of the impact of the crime on its victims. The opportunity for increased sentences has served as an incentive for law enforcement agencies, federal and otherwise, to bring cases federally.

## IV. Training

The training aspect of the identity theft program has a segment for law enforcement and a segment for public and private institutions. The law enforcement segment is fairly standard and is designed for local agencies that have felt overmatched by the difficulty of investigating an identity fraud case. The key element of the training is delivering the message that federal agencies are willing and able to assist them, particularly in investigations which lead out of their counties to the next state or the opposite coast.

Training for large institutions focuses on the vulnerability of their databases. These entities, of course, have a responsibility to their customers (whether they be called clients, students, patients, or some other term) and their employees. Some of them have statutory obligations to protect customer information, such as Gramm-Leach-Bliley. 15 U.S.C. § 6801. Finally, all of these institutions face civil suit, and potential government regulation, in the event of a data breach. Attendees leave these sessions charged with the duty to review their data security from top to bottom in order to limit the incidence of identity theft.❖

### ABOUT THE AUTHOR

❑**Richard W. Goldberg** is Chief of the Financial Institution Fraud and Identity Theft Section of the United States Attorney's Office for the Eastern District of Pennsylvania (Philadelphia). He is also a Computer Hacking and Intellectual Property prosecutor and previously supervised the Narcotics and Major Crimes sections. Before joining the U.S. Attorney's Office, he worked for eight years in the Philadelphia District Attorney's Office.✠

# Oregon Identity Theft Fast Track Program

*Sean B. Hoar*
*Assistant United States Attorney*
*District of Oregon*

## I. Overview of the program

In January 2006, the United States Attorney's Office (USAO) for the District of Oregon implemented a program intended to increase accountability for identity thieves in Oregon. The program was designed with the purpose of decreasing the burden on local District Attorneys' offices, but increasing the total number of identity theft prosecutions. The program requires certain defendants who have committed aggravated identity theft in violation of 18 U.S.C. § 1028A(a)(1), which ordinarily is charged in conjunction with other federal crimes, to plead guilty to the aggravated identity theft charge, alone. They must further agree, without litigation, to serve a minimum mandatory 2-year term of imprisonment. In exchange for their pleas of guilty, defendants are not charged with certain predicate offenses, which would otherwise result in a consecutive sentence under the United States Sentencing Guidelines (U.S.S.G.). The program applies only to aggravated identity theft offenses involving nonterrorism-related predicate felonies under 18 U.S.C. § 1028A(a)(1). It does not apply when the predicate felony is a terrorism-related felony under § 1028A(a)(2).

The program relies upon a network of local investigators and prosecutors throughout Oregon to identify eligible defendants, refer them to designated agents of the FBI, Secret Service, and the Postal Inspection Service for follow-up work, and ultimately, to Assistant United States Attorneys (AUSAs) for prosecution.

A defendant is generally eligible to participate in the Oregon Identity Theft Fast Track Program if the identity theft case involves some interstate nexus and the actual or intended loss, whichever is higher, is more than $5,000, and less than $70,000. If the loss is less than $5,000, the defendant must be a manufacturer of fraudulent identification documents or the defendant's criminal activity must create a disproportionately adverse impact in the community. The disproportionately adverse impact will usually be shown through a lengthy criminal history and continual criminal activity. The offense should have ten or more victims, from multiple jurisdictions, but, like the monetary threshold, the victim threshold is flexible and will depend upon the adverse impact the offender has in the community. If any applicable organizer, leader, manager, or supervisor adjustments under U.S.S.G. § 3B1.1 apply, the defendant will be ineligible for the program, as it is intended for defendants who would usually fall below federal thresholds.

As indicated in the program name, it is designed to handle identity theft cases in a "fast track" manner. This means that each defendant is expected to plead guilty within 30 days of arrest, without litigation, to federal aggravated identity theft, thereby conserving law enforcement and prosecutorial resources. In doing so, defendants must agree to a 24-month term of imprisonment, and, among other things, waive all appellate and postconviction remedies. In exchange for their pleas of guilty, defendants will not be charged with predicate offenses, such as bank fraud or credit card fraud, which would otherwise result in a consecutive sentence under the U.S.S.G.

The program was originally launched through training programs in ten different Oregon counties, coordinated by the Oregon USAO. Through those training programs, representatives of local police agencies and District Attorneys' offices were identified as participants in the Oregon Identity Theft Fast Track Network. Local detectives, in consultation with the local prosecutors, conduct the initial screening of the case. If it appears to match the eligibility requirements for the program, they refer the matter to designated AUSAs. When the matter is referred to the Oregon USAO, one designated

AUSA in each of the three offices in Oregon (Eugene, Medford, and Portland) reviews the matter, opens a file, and determines whether it is ready to be charged or whether additional work must be done. Generally, the additional work is done by designated federal agents. Once a decision is made to file the case, if the defendant is in state custody, the AUSA generally contacts the defendant's attorney and offers an opportunity to participate in the program, rather than face a minimum mandatory 24-month sentence in addition to the underlying guideline sentence. Ideally, the defendant is not taken into federal custody until an agreement is reached about participation in the program.

If the defendant desires to participate in the program, a criminal complaint is filed and the defendant is taken into federal custody. The defendant must then waive the right to speedy indictment so that the case does not have to be presented to a grand jury prior to resolution. A standardized plea offer is then made to the defendant. When the AUSA is notified that the offer is accepted, an information is filed with the court and a change of plea/sentencing hearing is scheduled. At the change of plea/sentencing hearing, the defendant waives the right to indictment and pleads guilty to an information alleging one count of aggravated identity theft in violation of § 1028A(a)(1). The parties waive preparation of a presentence report and the court sentences the defendant to serve a 24-month term of imprisonment, followed by a 1-year term of supervised release, with a condition that the defendant must pay full restitution to all victims of the offense.

## II. "Fast track" programs must be authorized

The operation of any "fast track" program must be authorized by the Attorney General. For a number of reasons, the Oregon Identity Theft Fast Track Program meets the criteria set forth in the Attorney General's Memorandum dated September 22, 2003, Department Principles for Implementing an Expedited Disposition or "Fast-Track" Prosecution Program in a District, *available at* http://www.usdoj.gov/opa/pr/2003/September/03_ag_516.htm. The District of Oregon is increasingly burdened with the crime of identity theft. Since 2001, when the Federal Trade Commission began recording identity theft statistics, Oregon has ranked in, or near, the top ten nationally in states having the most identity theft victims per 100,000 in population. Largely due to strained prosecutorial and judicial resources in Oregon, many of the traditionally local identity theft offenses have been committed with impunity. Oregon District Attorneys' offices have decriminalized certain theft offenses due to their lack of resources. Declination of federal identity theft cases in favor of state prosecution is therefore not available in Oregon, due to the lack of state resources. The operation of the Oregon Identity Theft Fast Track Program has helped to ease the strained resources.

## III. Examples of cases filed

On April 14, 2006, **Matthew Allen Galen Pence,** CR06-60031-AA (Apr. 14, 2006), pled guilty and was sentenced to serve 2 years in federal prison for aggravated identity theft. He was also ordered to serve a 1-year period of supervised release after completion of his sentence and to pay $7,948.62 in restitution to victims of the offense. Mr. Pence was 23 years of age and prior to his arrest was a transient resident of Eugene and Springfield, Oregon. Between August and December 2005, he was arrested on three occasions and had in his possession personal information belonging to victims of identity theft whose mail had been stolen. In pleading guilty, Mr. Pence admitted that he used the information for the purpose of committing bank fraud, in order to obtain money from federally insured financial institutions. He did so by falsely representing that he was the lawful holder of bank checks and credit cards which had been stolen from identity theft victims. Methamphetamine use was a contributing factor to the offense. The investigation of this case was a joint effort by the Eugene and Springfield Police Departments and the United States Postal Inspection Service (USPS).

On September 5, 2006, **Kayla Dawn Bostick,** CR06-60081-HO (Sept. 5, 2006), pled guilty and was sentenced to serve 2 years in federal prison for aggravated identity theft. She was also ordered to serve a 1-year period of supervised release after completion of her sentence and to pay $403.02 in restitution to a victim of the offense. Ms. Bostick was 23 years of age and prior to her arrest on May 30, 2006, was a transient resident of Eugene, Oregon. When arrested, bags of stolen mail were found in her car, and she admitted that she used the stolen information, which included stolen credit cards, to obtain money for food, motels, cigarettes, and drugs. In pleading guilty, Ms. Bostick admitted that she used the information for the purpose of committing bank fraud in order to obtain money from federally insured financial institutions. She did so by falsely representing that she was the lawful holder of credit cards which had been stolen from identity theft victims. On November 21, 2006, codefendant **Melissa Irene Bly** pled guilty to possession of stolen mail. Methamphetamine use was a contributing factor to the offenses. The investigation of this case was a joint effort by the Eugene Police Department and the USPS.

On September 19, 2006, **Milton Eugene Scott**, CR06-60057-HO (Sept. 19, 2006), was sentenced to serve 2 years in federal prison for aggravated identity theft. He was also ordered to serve a 1 year period of supervised release after completion of his sentence and to pay $7,256.57 in restitution to victims of the offense. His restitution was ordered to be joint and several with two associates, **Vincent Anthony Palumbo** and **Carrie Denise Zumbrum**, who were previously sentenced to serve 2 years in federal prison for aggravated identity theft for their role in the same identity theft ring. Palumbo was sentenced on April 27, 2006, and Zumbrum was sentenced on June 30, 2006. Scott is 41 years of age, Palumbo is 31 years of age, and Zumbrum is 43 years of age. Prior to their arrests, they were transient residents of Bend, Eugene, Springfield, and Junction City, Oregon. In pleading guilty, each of them admitted that in October and November 2005, they committed bank fraud by cashing counterfeit checks with stolen identification documents. Methamphetamine use was a contributing factor to the offenses. The investigation of this case was a joint effort by the Bend Police Department, the Deschutes County Sheriff's Office, and the FBI.

On April 19, 2006, **Jamey Shane Thomas**, CR07-60047-AA (Apr. 19, 2007), was sentenced to serve 2 years in federal prison for aggravated identity theft. He was also ordered to serve a 1-year period of supervised release after completion of his sentence and to pay $8,570.47 in restitution to victims of the offense. He also agreed to abandon his interest in a 2001 Oldsmobile Aurora, which was seized from him because it was derived from, and was used to commit, the identity theft. Two associates, **Angell Christina Corcoran** and **Joseph George Rossi**, pled guilty on April 17, 2007, to possession of stolen mail. Stolen mail was the source material for Thomas' identity theft. In pleading guilty, Thomas admitted that in July through October 2006, he used stolen identity information for the purpose of committing bank fraud. He did so in part by cashing counterfeit checks. The use of methamphetamine was a contributing factor to the offense. Thomas is 29 years of age, and Corcoran and Rossi are both 24 years of age. The investigation of this case was a joint effort by the Coos Bay Police Department, the North Bend Police Department, the Myrtle Creek Police Department, the Coos County Sheriff's Office, and the USPS.

On April 19, 2007, **Andrew Jonathon Clark**, CR 07-60018-AA (Apr. 19, 2007), was sentenced to serve 2 years in federal prison for aggravated identity theft. He was also ordered to serve a 1-year period of supervised release after completion of his sentence and to pay $62,157.48 in restitution to victims of his offense. Clark agreed to abandon computer equipment which was seized from him because it was derived from, and was used to commit, the identity theft. In pleading guilty, Clark admitted that in October through December 2006, he used stolen identity information for the purpose of committing credit card fraud. He did so in part by purchasing stolen credit cards on the Internet and using them to purchase goods and services. The use of

methamphetamine was a contributing factor to the offense. Clark is 21 years of age. The investigation of this case was a joint effort by the Eugene and Springfield Police Departments and the United States Secret Service.

## IV. Conclusion

The successful investigation and prosecution of identity thieves requires teamwork throughout all sectors of law enforcement, including assistance from private sector counterparts, such as financial institution fraud investigators and loss prevention or security specialists. Identity thieves should not be left to act with impunity simply because of scarce law enforcement resources. Through the creative and collective use of resources, such as the Oregon Identity Theft Fast Track Program, we can accomplish much more, and we can ultimately impact the problem of identity theft.❖


**ABOUT THE AUTHOR**

❑**Sean B. Hoar** has served with the United States Department of Justice in Eugene, Oregon, as an Assistant United States Attorney since 1991. His caseload consists primarily of complex white collar and high tech crime, including identity theft and Internet fraud. He teaches a course in Cybercrime at the University of Oregon School of Law and coordinates the CyberSafe Initiative, a public/private partnership to reduce vulnerabilities in the Internet. He also served on the President's Identity Theft Task Force, which developed federal legislation and other action to combat identity theft at a national level.✠

# NOTES

# Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' BULLETIN to all federal law enforcement personnel who wish to receive it, we are requesting that you e-mail Nancy Bowman (nancy.bowman@usdoj.gov) with the following information: Name, title, complete shipping address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the BULLETIN, we ask that you have one receiving contact and make distribution within your organization. If you do not have access to e-mail, please call 803-705-5659. Your cooperation is appreciated.