May 2002
Volume 50
Number 3

United States
Department of Justice
Executive Office for
United States Attorneys
Office of Legal Education
Washington, DC
20535

Kenneth L. Wainstein
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 bi-monthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201. Periodical postage paid at Washington, D.C. Postmaster: Send address changes to Editor, United States Attorneys' Bulletin, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201

Managing Editor
Jim Donovan

Assistant Editor
Nancy Bowman

Law Clerk
Ginny Nissen

Internet Address
www.usdoj.gov/usao/eousa/foia/foiamanuals.html

Send article submissions to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center Office of Legal Education 1620 Pendleton Street Columbia, SC 29201

Anti-Terrorism

In This Issue

This issue of the United States Attorneys' Bulletin is dedicated to Thomas G. Schrup, the Director of Training, Criminal Division, United States Department of Justice.

On March 15, 2002, Tom and his wife, Carlotta Lea Schrup, died in a plane crash near Ocean City, Maryland.

As Director of the Criminal Division's Training Center since 1996, Tom was instrumental in developing partnerships with a variety of federal agencies and outside resource organizations. He was a driving force for introducing cutting-edge technology and dramatically expanding the training opportunities for Division personnel.

Tom will be remembered by his friends and colleagues for his firm commitment to his profession and his exemplary service to the Criminal Division.

Use of the Social Security Fraud Statute in the Battle Against Terrorism (42 U.S.C. § 408(a)(7)(A)-(C))

John K. Webb
Special Assistant United States Attorney
Central District of California and
District of Arizona

I. Introduction

As unlikely as it might seem at first, a little-known felony fraud section of the Social Security Act (42 U.S.C. § 406, 1-189) (the "Act") has emerged as a highly effective weapon in the domestic war against terrorism. Since the terrorist events of September 11, prosecutors in some districts have used § 408(a)(7) of Title 42 to charge and detain individuals suspected of engaging in, or suborning, terrorist activities, and who have misused or misrepresented a social security account number ("SSN"). Specifically, under § 408(a)(7) of the Act, a person is subject to criminal penalties if he or she:

> (1) willfully, knowingly, and with an intent to deceive uses a social security number on the basis of false information furnished to the SSA (408(a)(7)(A));
>
> (2) falsely represents, with an intent to deceive, a number to be the social security number assigned to him or her or to another person (408(a)(7)(B)); or
>
> (3) knowingly altered a social security card issued by the SSA, bought or sold a card that was, or was purported to be, a card so issued, counterfeited a social security card, or possessed a social security card or counterfeit social security card with an intent to sell or alter it (408(a)(7)(C)).

An individual who wrongfully uses or misrepresents a social security number can also face criminal penalties under 18 U.S.C. § 1001, which makes it a criminal offense to make false statements in any matter under the jurisdiction of any federal department or agency of the United States. Thus, in any instance where an individual has misused or misrepresented a social security number on a document presented to any federal department or agency, two separate felonies may be charged using 42 U.S.C. § 408(a)(7)(B) and 18 U.S.C. § 1001, respectively. Similarly, a person who uses or provides counterfeit social security number cards can be charged with violations of both 42 U.S.C. § 408(a)(7)(C) and 18 U.S.C. § 1028(a)(6) and (7), which prohibit the knowing transfer of stolen or false identification documents. The same misuse of social security numbers can be applied to other forms of fraud and misrepresentation with respect to government documents, including false attestations and/or statements made to employers on I-9 forms for the purpose of satisfying a requirement of § 274A(b) of the Immigration and Nationality Act, 8 U.S.C. § 1324(b), and false statements made on applications for FAA security badges, passports, visas, or asylum applications. *See* 18 U.S.C. § 1546(b)(2) and (3).

A person convicted of a violation of § 408(a)(7) is guilty of a Class D felony, and will be fined or imprisoned for not more than five years, or both. Because most terrorist suspects have engaged in some form of SSN misuse, identity theft, or immigration fraud, prosecutors generally prefer charging social security number misuse under § 408(a)(7)(B). This section provides prosecutors with a reliable and convenient means of charging and detaining individuals suspected of terror-related activities.

II. Rampant misuse of social security numbers among individuals living or operating illegally in the United States

Investigations by the FBI and other law enforcement agencies since September 11 have identified a large number of aliens living within the United States who are actively utilizing false identities supported by bogus documentation. In almost every instance, this includes the use of counterfeit or fraudulently issued social security numbers, or legitimately issued numbers that have been stolen from other individuals or issued illegally by a corrupt SSA employee. Fraudulent SSN's are used to obtain drivers' licenses, to secure employment, to apply for loans and credit cards, and to live anonymously while avoiding detection by federal and state authorities. Sometimes the SSN's are completely fictitious, comprised of a random combination of familiar numbers. While these numbers are usually easily detected by law enforcement, they can be quickly and cheaply purchased on the black market and provide sufficient deception to secure the thief quick access to public services. Other times identity thieves adopt names and social security numbers culled from newspaper death notices, or from information lists found on the Internet. For example, some Internet hacker sites provide extensive lists of social security numbers, both legitimate and bogus, available to anyone with access to the sites. In addition, these Internet sites sometimes include corresponding names, addresses, dates of birth, telephone numbers, and credit card numbers of individuals. In one instance in 2001, the Office of the Inspector General/Social Security Administration ("OIG/SSA") investigated and prosecuted an individual who advertised several thousand valid social security numbers (with names) for purchase on eBay, with bids for each number starting at one dollar.

In some instances, a legitimate number (one actually issued by SSA) can be purchased from a black-market vendor who has stolen the number from an unsuspecting individual. When a legitimate social security number holder has his number stolen, she is usually unaware of the theft until her credit is destroyed or her identity is used criminally by the thief. A legitimate SSN, unless reported stolen, will allow the thief almost unlimited access to employment, credit cards, replacement social security cards, driver's license, and any other sensitive identity document available to a legitimate social security number holder.

It is not unusual for an alien to deceive SSA into issuing a valid social security number by filing applications containing false information supported by bogus identity documents. In order to secure a new or replacement social security number, SSA requires that an individual show proof of identity, including at least two identification documents such as a driver's license, U.S. passport, birth certificate, U.S. government or state employee ID card, school ID card, record, or report card, marriage or divorce record, military records, clinic, doctor, or hospital records, adoption records, or alien registration number. *See* SSA *Programs and Operations Manual* ("POMS", §§ RM 00203.100-400 (2001). Library cards, vehicle registration, rental or lease agreements, credit cards, check cashing cards, bank deposit slips, telephone or utility bills, or any identification documents issued by a commercial firm are not considered identity documents and cannot be used to secure a social security number. *See* POMS § RM 00203.770.

Unfortunately, very well-crafted, false identification documents are available on the Internet and/or can be easily purchased on the black market. SSA frequently discovers and rejects applications for social security numbers that are supported by a combination of bogus identity documents, including a fake driver's license, counterfeit birth certificate, fake baptism certificate, or false INS alien registration number. However, some bogus documents are almost impossible to detect, and SSA sometimes issues social security numbers that are based on fraudulent representations. Once a new SSN has issued, SSA has little ability to prevent fraud or misuse associated with the number, and the recipient is free to live, work, and travel freely within the United States until his illegal activities are discovered. In recent testimony before Congress, SSA Commissioner James B. Lockhart, III reported that an audit of social security numbers issued during 2001 revealed that 999 of 3,557 original SSN applications reviewed by the

SSA/OIG were approved based on improper evidentiary documentation. (*See* Testimony of James B. Lockhart, III, U.S. Senate Committee On Finance, confirmation hearing for Deputy Commissioner of SSA, 11/15/01).

Legitimate social security numbers issued by corrupt SSA employees are the identity documents most prized by identity thieves and bring the most value on the black market. Newly issued social security numbers are almost impossible to detect and provide a legitimate cover for illegal activities and for aliens seeking to blend into American society. In the past five years, the SSA Inspector General has investigated fifty-five cases involving sixty-one SSA employees who have disclosed, sold, or released SSN information. (*See* Testimony of James B. Lockhart, III, U.S. Senate Committee On Finance, confirmation hearing for Deputy Commissioner of SSA, 11/15/01). Criminal allegations involving SSA employees include the processing of false social security number card applications, the selling of legitimate social security numbers, and the printing of counterfeit social security number cards. Forty-five cases have resulted in criminal convictions, approximately half of which resulted in incarceration of the corrupt employees. Until 9-11, a long-standing SSA policy allowed individuals to obtain up to fifty-two "replacement" social security cards during any one-year period. Prior to the events of September 11, audits by the SSA Inspector General had identified this policy of almost unlimited access to "replacement" social security cards as ripe for abuse, noting that during year 2000, 192 individuals obtained six or more replacement SSN cards. (*See* Testimony of James B. Lockhart, III, U.S. Senate Committee On Finance, confirmation hearing for Deputy Commissioner of SSA, 11/15/01).

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

In 1981, Congress amended the misdemeanor provisions of the Act, making Social Security fraud (including SSN misuse) a felony, punishable by five years in prison and a fine up to $5,000. (*See* 1981 Amendments. Pub. L. 97-123). The SSA felony fraud statute, cited as 42 U.S.C. § 408(a)(1)-(8), contains the Social Security Act's primary criminal provisions. The statute, set forth below in pertinent part, comprehensively spells out restraints on fraud by specifying requirements for disclosure of specific events, and by identifying facts that affect the right to payment of SSA benefits.

> 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** (emphasis added)
>
> (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.

IV. Legislative history of the fraud provisions of 42 U.S.C. § 408(a)

A. The 1972 amendment

In 1972, misdemeanor fraud provisions were first added to the Act, designed by Congress for the sole purpose of preventing any person from obtaining federal benefits by using a fraudulent social security number. Specifically, the Act's 1972 fraud subsection forbade anyone from using a social security number to increase any payment or to obtain any improper payment or benefit under any federal program. (*See* Social Security Amendments of 1972, Pub.L. No. 92-603, sec. 130(a), 1972 U.S.C.C.A.N. 1548, 1586; *See also* H.R.CONF.REP. NO. 92-1605(1972) *reprinted in* 1972 U.S.C.C.A.N. 4989, 5370, 5373 (citing prevention of improper benefit payments as the sole purpose behind the new provisions)).

B. The 1976 amendment

In 1976, the reach of the penalty was expanded substantially when the Act was amended to include not only those who sought unauthorized or excessive federal benefits, but also those who misused social security numbers "**for any other purpose**."(emphasis added). (*See* Tax Reform Act of 1976, Pub.L. No. 94-455, sec. 1211, 90 Stat. 1520, 1711 (1976); codified at 42 U.S.C. § 405(c)(2)(C)(i)) (the "1976 Act"). 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.

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

In a particularly revealing and crucial portion of the legislative history, the 1976 report of the Senate Finance Committee also sought to explain the addition of the words "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**. (Emphasis added).

See S.Rep. No. 94-938(I) (1976), reprinted in 1976 U.S.C.C.A.N. 3438, 3819.

This insightful look into legislative history demonstrates that Congress has unequivocally explained that the words "for any other purpose" mean precisely what they say. Courts have reached similar conclusions regarding the legislative intent behind the words "for any other purpose." *See United States v. Silva-Chavez*, 888 F.2d 1481 (5th Cir. 1989).

C. The 1981 amendment

In 1981, Congress 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."** (emphasis added). (*See* Omnibus Reconciliation Act, Pub.L. No. 97-123, sec. 4, 95 Stat. 1659, 1663-64 (1981)). While the House Conference Report accompanying the amendment offers no explanation of the reasons for the change (*see* H.R.CONF.REP. NO. 97- 409 (1981)) *reprinted in* 1981 U.S.C.C.A.N. 2681, 2687-88), the text of the amendment makes clear Congress' intent both to punish a broader range of acts and to impose a stiffer penalty. 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.

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

V. Charging decisions and elements of the crime: 42 U.S.C. § 408(a)(7)(A)-(C)

The felony provisions of 42 U.S.C. § 408(a)(7)(A)-(C) are particularly effective in charging cases where an individual has entered the country illegally, or has tried to manipulate the identification systems currently in place. The elements of proof for each subsection of § 408(a)(7) are more flexible than those required by 18 U.S.C. § 1028, a better known identity theft statute, that also contains subsections dealing with the misuse of a social security number. What follows 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.

In an effort to make the discussion of the charging elements more meaningful, a fact-driven case study has been provided at the end of this article. The case study is not necessary to an understanding of the subsections and elements of § 408(a)(7), but the factual description can provide helpful insight into applying the elements for the subsections set forth below. The case study involves an individual indicted, because of venue issues, in both the Central District of California and the District of Arizona.

A. 42 U.S.C. § 408(a)(7)(A) provides, in pertinent part:

> In general
>
> Whoever–
>
> (7) . . . . . for the purpose of obtaining anything of value from any person, **or for any other purpose** (emphasis added)
>
> (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) 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;

Elements of the crime

The elements required to prove a violation of § 408(a)(7)(A) are:

> (1) willful and knowing use of a Social Security account number;
>
> (2) with intent to deceive;
>
> (3) 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 social security card obtained on the basis of false information supplied to SSA, and used deceitfully, is actionable and constitutes a felony for purposes of § 408(a)(7)(A). For example: a subject in the U.S. on a tourist visa secures a non-work SSN using his French passport. The subject then uses an alias to file a bogus application for asylum, resulting in INS approval and issuance of a green card and alien registration number. The subject then uses his new name and illegally procured INS documents to apply for a second social security number, thus completing the creation of a new identity. The subject then uses the second social security number to secure credit cards, open bank accounts, attend flight training, and make applications for employment as a pilot. The subject's use of the social security number is actionable because he used false and fraudulent documents (deceptively procured from the INS) to deceive SSA into issuing him a new social security number, and he may be charged with a felony under § 408(a)(7)(A). *See United States v. Pryor, 32 F.3d 1192 (7th Cir. 1994)* (Defendant acted "willfully, knowingly, and with intent to deceive," in illegally using social security number obtained on basis of false information).

B. 42 U.S.C. § 408(a)(7)(B) provides, in pertinent part:

> In general
>
> Whoever–

> (7) . . . . . for the purpose of obtaining anything of value from any person, **or for any other purpose** (emphasis added)
>
> (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;

42 U.S.C. § 408(a)(7)(B).

Elements of the crime

The elements required to prove a violation of 42 U.S.C. § 408(a)(7)(B) are:

> (1) false representation of a Social Security account number;
>
> (2) with intent to deceive;
>
> (3) 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:

> (1) for any purpose;
>
> (2) with intent to deceive;
>
> (3) represented a particular Social Security account number to be his;
>
> (4) which representation is false.

See United States v. O'Brien, et. al., 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 misrepresented a social security number to open a bank account; apply for a credit card; secure credit for a cell phone; rent or lease an apartment or car; apply for employment; or enroll in flight training. The charging standard, " **for any purpose,"** is broad and self-explanatory, and any false representation of a social security number, 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).

Intent to deceive and the "use" vs. "possession" distinction

Direct evidence is not always necessary in order to prove that a defendant intended to use a social security card or number for deceptive purposes. Mere possession of a social security card or number that does not belong to a defendant is sometimes sufficient to support a finding that the defendant intended to deceive. *United States v. Charles*, 949 F.Supp. 365 (D. VI 1996). In *Charles*, the government was unable to produce direct evidence that the defendant had actually applied for a driver's license using a false social security number, but concluded that the jury could infer that the defendant received the social security card through false representations when the government's evidence showed that:

> (1) the Police Department Licensing Section had printed defendant's license; and
>
> (2) generally, in order to obtain such a license, an applicant must give a social security number to the licensing agent.

However, mere possession of false identity documents, including a false social security number, might not always be enough to convict. Some courts have held that the term "represent" connotes a positive action, not merely passive possession, and have thus reasoned that Congress, by using the term "represent," meant to proscribe the "use," not merely the "possession," of a false social security number. *United States v. McKnight*, 17 F.3d 1139, 1144-45(8th Cir. 1994). However, the concurring opinions of two *McKnight* panel members underscore that this is not a hard and fast rule: "We write separately to make explicit that possession of an identification card bearing a false social security number can, in

some instances, provide a sufficient predicate for a jury to properly infer that a defendant falsely represented a social security number in violation of 42 U.S.C. § 408(a)(7)(B)."*Id.* at 1146; *see also United States v. Teitloff*, 55 F.3d 391, 394 (8th Cir. 1995) (court rejected defendant's contention that he did not technically "use" the social security number because the DMV computer system automatically provided that information when he supplied the other person's identification documents).

When a defendant acts willfully and knowingly

A defendant may be found to have acted willfully, knowingly, and with intent to deceive, even if the defendant did not intend to deceive federal officials when he presented them with documents containing a false social security number. *U.S. v. Pryor*, 32 F.3d 1192 (7th Cir. 1994) (defendant's driver's license had been suspended and he was found to be carrying false documents which he acknowledged that he planned to present if pulled over for a traffic violation).

The "moral turpitude" exception

The Ninth Circuit has held that an alien's use of a false social security number to further otherwise legal conduct is not a crime of "moral turpitude." *Beltran-Tirado v. Immigration and Naturalization Service*, 213 F.3d 1179, 1184 (9th Cir. 2000). The significance of this decision lies in the impact such a conviction would have on the illegal alien's eligibility for inclusion on the Immigration and Nationality Act registry. *See* 8 U.S.C. 1259. The registry statute was originally enacted by Congress in 1929 as a means to regularize the status of long-time illegal aliens residing in the United States, and has been updated periodically since. Under current registry provisions, conviction for a crime of moral turpitude would preclude an alien from eligibility because he would not be considered "of good moral character."

"*Otherwise legal behavior*"

In *Beltran-Tirado*, defendant lived under an assumed identity, using the name and social security number of the victim to obtain employment, marry twice, obtain a driver's license, credit cards, and a HUD loan. Beltran's earnings attracted the interest of the IRS, resulting in her arrest and conviction under 42 U.S.C. § 408(a)(7)(B) and 18 U.S.C. § 1546(b)(3). The INS moved to deport her, but the Ninth Circuit intervened to interpret the legislative history of 42 U.S.C. § 408 and carve out an exception to a conviction for a crime of moral turpitude by allowing the use of a false social security number to further "otherwise legal behavior." The *Beltran-Tirado* case appears consistent with an earlier decision by the Ninth Circuit in which the court concluded that "the crime of knowingly and willfully making any false, fictitious or fraudulent statements or representations to an agency of the United States is not a crime of moral turpitude because a jury could convict if it found that the defendant had knowingly, but without evil intent, made a false but not fraudulent statement." *Hirsch v. INS*, 308 F.2d 562, 567 (9th Cir. 1962).

Sale of false or counterfeit Social Security cards is a crime of moral turpitude

Another California federal court, citing *Beltran-Tirado* (n.8), held that the sale of false or counterfeit social security numbers is a crime that involves moral turpitude. *Souza v. Ashcroft*, 2001 WL 823816 (N.D. Cal.). The court distinguished between those who sell rather than use false or counterfeit social security cards ("persons convicted of the crime of selling false or counterfeit social security cards have, like persons convicted of the analogous crime of selling counterfeit green cards, committed a crime of moral turpitude") *Id.* at *3, and stated that Congress, in amending 42 U.S.C. § 408, specifically excluded from the exemption those who sell, rather than use, false or counterfeit social security cards. The reason for this distinction is apparent. Sale of false alien registry documents (green cards), as well as the crime of selling false or counterfeit social security cards, inherently involves a deliberate deception of the government and an impairment of its lawful functions.

Multiple false representations and the rule against multiplicity

When an individual makes multiple false

representations by misrepresenting a social security number on multiple credit card applications, bank accounts, or federal documents relating to employment (I-9, W-4), each use or representation constitutes a separate offense. Each of the separate offenses is supportable by a different set of predicate facts, and is actionable under § 408(a)(7)(B). In addition, each use or representation on a federal form is actionable as a false statement under 18 U.S.C. § 1001, and can be charged as a separate offense also supportable by a different set of predicate facts. While charging multiple counts might not be desirable, doing so when separate predicate facts exist would not run afoul of the rule against multiplicity that prohibits the charging of a single offense in several counts. *United States v. Castaneda*, 9 F.3d 761, 765 (9th Cir. 1993) (holding that a defendant may properly be charged with committing the same offense more than once as long as each count depends on a different set of predicate facts); *see also United States v. Hurt*, 795 F.2d 765, 774-75 (9th Cir. 1986).

Use of false Social Security on non-federal documents

It is not necessary that the false use or representation of a social security number have a detrimental effect in some way on the government to be actionable. *See United States v. Holland*, 880 F.2d 1091 (9th Cir. 1989). Any use of a false social security number on non-federal documents is still actionable under § 408(a)(7)(B). For example, the subject in the case study used his falsely obtained SSN when completing multiple applications seeking employment as a pilot, and in applying for taxi permits with airport cab companies. Even though the airline and cab company employment applications are not federal documents, the subject can still be charged under 408(a)(7)(B). Further, it is not necessary to prove that the defendant used a false social security number for payment, gain, or pecuniary value. *United States v. Silva-Chavez*, 888 F.2d 1481 (5th Cir. 1989).

C. 42 U.S.C. § 408(a)(7)(C) provides, in pertinent part:

> In general
>
> Whoever–
>
> (7) . . . . . for the purpose of obtaining anything of value from any person, **or for any other purpose** (emphasis added)
>
> (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.

Elements of the crime

The elements required to prove a violation of § 408(a)(7)(C) are:

> (1) knowingly alters a social security card; or
>
> (2) counterfeits or possesses a social security card with intent to sell or alter it; or
>
> (3) buys, or sells a social security card.

42 U.S.C. § 408(a)(7)(C).

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. *Note*: Nothing in the case study supports a charge under 42 U.S.C. § 408(a)(7)(C).

Altered or counterfeited cards

In order to qualify as counterfeit, a social security card must include the name of the number holder and the social security number. *United States v. Gomes*, 969 F.2d 1290 (1st Cir. 1992) ("A bogus document is counterfeit if it is calculated to deceive an honest, sensible, and unsuspecting person of ordinary observation and care dealing with a person supposed to be upright and honest"). *Id.* at 1293. Conduct charged under §408(a)(7)(C) most commonly arises from:

1) the printing or manufacture of counterfeit

social security cards for resale on the black market; or

2) the altering of social security cards to remove work restrictions from the face of the card.

The altered and/or counterfeited cards are then used to secure false identification documents, open bank accounts, apply for credit cards, and to work, including employment in sensitive positions at airports, government facilities, and other locations requiring security clearances. To qualify as counterfeit, a bogus copy of a social security card does not have to be such a good imitation that it baffles an expert. *Gomes*, at 1294 (" . . the law does not criminalize only masterpieces").

D. Sentencing Guidelines for 42 U.S.C. § 408(a)(7)

Prosecutions under 42 U.S.C. § 408(a)(7) are governed under the U.S. SENTENCING GUIDELINES MANUAL, § 2B1.1 (2001), which covers basic economic offenses involving fraud or deceit (including false identity, theft, embezzlement, receipt of stolen property, and property destruction). The basic offense level is six, with offense levels increasing as the loss amount rises. For a first-time offender with no prior convictions, the minimum guideline range would be 0-6 months. This range is, however, subject to possible enhancements.

Identity theft enhancement

If the social security number misuse includes possession of any device-making equipment or counterfeit access device, or the unauthorized transfer or use of any unlawful means of identification, or possession of five or more means of identification unlawfully produced or obtained by some other means of identification, the offense level is enhanced by two levels. However, if the resulting level is lower than twelve, the guidelines require that the offense level be increased automatically to level twelve. *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(9).

Cross references with other guidelines

If other offenses are charged in an indictment along with § 408(a)(7), their guidelines can be cross-referenced and applied (e.g., 18 U.S.C. § 1001, 18 U.S.C. § 1341, 18 U.S.C. § 1342, or 18 U.S.C. § 1343). These include crimes involving the theft of a firearm, destructive device, explosive material, or controlled substance (USSG §2D1.1); a crime involving unlawful possession, attempt or conspiracy (USSG §2D2.1); unlawful receipt, possession, or transportation of firearms or ammunition (USSG §2K1.3).

Intended loss

The offense level in cases involving social security number misuse and identity theft fraud is calculated by applying the guidelines and, if appropriate, by determining the amount of loss. U.S. SENTENCING GUIDELINES MANUAL § 2B1.1. In cases involving terrorism suspects, fraud losses can be generated in a number of ways, including credit card losses, bank loan fraud, or money laundering used to fund terrorist activities. Sometimes fraud losses are interrupted before the entire crime is completed, resulting in a real money loss of less than was otherwise intended. In such cases, if the loss the defendant was attempting to inflict can be determined, that figure should be used if it is greater than the actual loss. The fact that the fraudulent scheme was interrupted before its full loss was realized is of no importance. *United States v. Lorenzo*, 995 F.2d 1448, 1460 (9th Cir. 1993) (defendants held to higher intended loss for sentencing purposes, although they actually received a considerably smaller sum); *see also United States v. Robinson*, 94 F.3d 1325, 1328 (9th Cir. 1996) (holding intended loss appropriate measure in scheme interrupted by a government sting operation).

Seriousness of offense and course of conduct

Intentional use of a false social security number is not a trivial offense. *United States v. Sullivan*, 895 F.2d 1030 (5th Cir. 1990). For sentencing purposes, a court is not limited to the conduct comprising the offense of conviction. The court can also consider the entire course of conduct involving the defendant. *Id.* at 1032; *see also United States v. Fulbright*, 804 F.2d 847 (5th Cir.1986). Where the conduct involving SSN misuse is particularly egregious, a court can impose an upward departure beyond the guideline range. *United States v. Scott*, 915 F.2d 774, 777 (1st Cir. 1990) (Where defendant fled prosecution

and stole the identity of another person and obtained, through fraud, a dead man's SSN, driver's license, and birth certificate). Upward departure is also warranted when the defendant's prior conduct and criminal history suggests a similar propensity towards identity theft and social security fraud. *United States v. Myers*, 41 F.3d 531, 533 (9th Cir. 1994).

In considering the facts set out in the case study, a departure for egregious conduct is entirely warranted. A strong case can be made for similar departures in most cases involving subjects indicted for activities related to the terrorist events of September 11, and a request for upward departure should be strongly considered.

E. Recent indictments using § 408(a)(7)(B)

AUSAs in Arizona and Los Angeles have used § 408(a)(7)(B) as the principal charge in several indictments involving individuals on terror watch-lists, or who are individually suspected of 9/11 related activities. It is notable that all nineteen of the hijackers in the September 11 attacks had social security numbers, and thirteen hijackers had obtained them legally (*See* Testimony of Hon. James G. Huse, Jr., Inspector General, Office of the Inspector General, Social Security Administration, before the Subcommittee on Social Security of the House Committee on Ways and Means; hearing on Social Security Administration's response to September 11, 2001 terrorist attacks; dated November 1, 2001). Law enforcement agencies are still learning about the extent of their activities, but it should not surprise anyone that the hijackers, and their suspected accomplices, committed identity theft and used false SSN's to blend into American society while planning the September 11 attacks. In fact, subsequent investigation has shown that securing and using social security numbers was a critical element of the plans of the terrorists and their support cells. In Arizona, five individuals have already been indicted as a result of investigations related to the events of 9/11, and two have recently been convicted after jury trials. Prosecutors have charged these individuals with a variety of counts, including 42 U.S.C. §§ 408(a)(7)(A) and (B) (SSN misuse); 18 U.S.C. § 1001 (false statements on documents presented to SSA, INS, FAA); 18 U.S.C. § 1014 (false statement to federal banking institution); 18 U.S.C. § 1029 (access device fraud); 18 U.S.C. § 1546 (passport fraud and false attestation); 18 U.S.C. § 1621 (perjury); and 18 U.S.C. § 371 (conspiracy). In each instance, the individual was found to have attempted to use a false identity or SSN to secure some strategic benefit such as: a driver's license, FAA certificate, credit card, bank account, grant of asylum, or employment as a pilot. Similar charges have been used successfully by prosecutors in the Central District of California, Los Angeles, to secure indictments against individuals identified as having ties to the events of 9/11. Jurors in both jurisdictions have shown little tolerance for identity thieves.

F. Securing search warrants using § 408(a)(7)(B)

Special Agents from OIG/SSA and the FBI have successfully asserted § 408(a)(7)(B) as statutory authority to secure a search warrant. In support of the search warrant, prosecutors attached an affidavit describing social security number misuse and setting out specific reasons for viewing SSN misuse as evidence of identity theft. By showing that the subject of the investigation used false information to create a second identity, prosecutors were able to establish probable cause that a "pilot's case" belonging to the subject contained more evidence of concealed identity and/or fraudulent activities. Based on a properly drawn affidavit describing violations of 42 U.S.C. § 408(a)(7)(B) and 18 U.S.C. § 1001, a federal magistrate signed a warrant allowing the agents to conduct a search of the subject's pilot's case. (a copy of the affidavit is available to AUSA's for review upon request). Information found in the pilot's case allowed prosecutors to secure initial indictment and superseding indictments. Neither the magistrate who issued the search warrant nor the judge who denied the subject's request for suppression and release at a subsequent detention hearing, found any problem with the probable cause or evidentiary support establishing a felony charge under § 408(a)(7)(B).

VI. "*Operation Safe Travel" and "Operation Tarmac*"

In the weeks following September 11, a task force consisting of several federal agencies,

including OIG/SSA, FBI, FAA, INS, DOT, U.S. Customs, and Homeland Security, initiated investigations designed to conduct audits of the social security numbers of security-badge holders at airports throughout the United States. This investigation, referred to as either "Operation Safe Travel" or "Operation Tarmac," (the names are interchangeable), was first initiated by SSA/OIG and INS at the Salt Lake City airport prior to the Winter Olympics. An audit of social security numbers at the airport revealed significant irregularities among holders of security badges with access to the tarmac and other sensitive areas of the airport. The investigation, labeled "Operation Tarmac," resulted in the indictment and arrest of sixty-nine individuals employed by private companies operating at the airport and providing services such as security screening, food services, aircraft fueling, cargo handling, cleaning/housekeeping services (inside the airport, the on-ramps leading to planes, and on the airplanes), airplane service and maintenance, and maintenance and construction in secure areas of the airport. Of the sixty-nine individuals indicted in the Operation Tarmac sweep, sixty-one individuals had Security Identification Display Area ("SIDA") badges that allowed them access to highly secure areas of the airport, including access to planes, runways, ramps leading to planes, and cargo areas. Three of those indicted were airport security screeners. The indictments charged violations of 42 U.S.C. §§ 408(a)(7)(B) and (C) (SSN misuse and using counterfeit or altered Social Security cards), 18 U.S.C. § 1001(a)(3) (false statements on government forms), and 18 U.S.C. § 1546(a)(3) (false statements on applications to INS). Other violations uncovered by the investigation included the use of false and counterfeit alien registration cards and numbers, making false representations about citizenship status to obtain employment and security badges, and making false statements to authorities about criminal history. All of those indicted were in the country illegally.

Since the initial sweep at the Salt Lake City airport, similar operations have been successfully undertaken at more than twenty airports in the United States, including Phoenix, Los Angeles, Miami, Boston, San Diego, Charlotte, Las Vegas, and San Francisco. These investigations have resulted in a significant number of indictments and arrests of individuals illegally living and operating under false identities in the United States, some of whom were fugitives from felony convictions. Each person indicted and arrested by agents involved in Operation Tarmac/Operation Safe Harbor possessed security badges with clearance to enter restricted and sensitive areas of each airport. Each person indicted was found to be using false identification documents, including false social security numbers. Particularly disturbing is the fact that, in Miami and Los Angeles, agents arrested individuals working as pilots and possessing false identification documents and bogus social security numbers. Further, agents arrested individuals during some sweeps who were employed as security screeners. In one particularly disturbing incident, an illegal used false identity documents to secure employment with an airline and to obtain a security badge allowing complete access to airport facilities. The subject failed to show up for work after obtaining the security badge, but the airline failed to cancel the badge. However, airport records show that the badge continued to be used to access the airport regularly. In each operation, the principal charge used to indict those using false identification documents was § 408(a)(7)(B).

The arrest of individuals utilizing false identities by Operation Tarmac/Operation Safe Harbor investigators has underscored the seriousness of the false identity problem faced by law enforcement and Homeland Security officials since the terrorist events of 9/11. In every airport security badge holder arrest, use of a false social security number proved to be the foundation block that supported the identity theft and enhanced the ease with which the individual was able to secure obscurity from law enforcement. It also helps explain why securing and using social security numbers was a critical element of the plans of the terrorists and their support cells in their preparation for the September 11 attacks. The indictments resulting from investigations implemented under Operation Safe Travel and Operation Tarmac also indicate the value and importance of using § 408(a)(7) as a tool for prosecuting such violations.

VII. Case study

Subject entered the United States legally in 1992, holding a French passport and using a visa waiver based on his French citizenship. Subject had been a pilot for a small middle-eastern airline for several years before coming to the United States. Subject applied for and legally secured a non-work SSN from SSA by presenting his French passport and a student ID card from a flight training school as identification. Subject used the SSN to lease an apartment, open bank accounts, attend flight training schools, secure an FAA certificate, obtain a cellular phone account, apply for credit cards, and apply for federal and state program funds to pay for his flight training (he was not successful!). Subject demonstrated no known source of income, but traveled frequently abroad using his French passport and visa waiver to enter and leave the United States virtually unchallenged. In 1998, using a variation of his true name, subject submitted an asylum application to the INS that contained material false statements and misrepresentations as to his identity, nationality, family, work history, and persecution at the hands of others. Subject also lied about his date of entry into the United States, representing that he had arrived by boat only four days before filing his asylum application. Based on his false statements and representations, INS granted subject's asylum application and issued him a green card and alien registration number. Subject presented the green card and INS alien number to SSA and applied for a new SSN using the false name from his asylum papers. On his application for a new SSN, subject represented that he had never before applied for or received an SSN. Based on subject's false representations and presentation of legitimate documents from the INS, SSA issued a new SSN in the name shown in subject's asylum papers. Subject used the new SSN to establish a new identity and to apply for employment with numerous domestic airlines and air-freight carriers. During this time, subject continued to travel extensively abroad using his French passport and true identity. At times, subject carried a pilot's case and represented himself as a pilot, thereby gaining admittance into the cockpit jump-seat of passenger aircraft. He also opened bank accounts and applied for credit cards using his new SSN, and worked periodically as an airport cab driver using his new identity and SSN to secure airport access. Within thirty weeks of receiving his new SSN, subject applied for, and secured a replacement social security card and continued his flight training using a "simulator club" at a local aviation school. Subject is known to have trained on the flight simulator at the same time as two of the 9/11 hijackers and other individuals associated with the events of 9/11.

VIII. Conclusion

The use of 42 U.S.C. § 408(a)(7)(A)-(C) to charge and detain suspects has already proven to be a particularly effective weapon in the domestic war against terrorism. Since September 11, prosecutors in several districts have used 42 U.S.C. § 408(a)(7) to indict individuals suspected of engaging in, or suborning, terrorist activities, and who have misused or misrepresented social security account numbers to secure positions at airports and other sensitive facilities. The elements of proof for each subsection of 42 U.S.C. § 408(a)(7) are more flexible than those required by other felony statutes such as 18 U.S.C. § 1028 (identity theft). The ease of charging § 408(a)(7)(B) makes it an increasingly popular tool for prosecutors.❖

ABOUT THE AUTHOR

❒**John K. Webb** is a Special Assistant United States Attorney, and is responsible for prosecuting federal crimes involving identity theft and Social Security number misuse. He is the Identity Theft Coordinator for the United States Attorney's Office (USAO) in Los Angeles, and divides his time between the USAOs for the District of Arizona and the Central District of California. Since September 11, 2001, he has served as a member of the Joint Terrorism Task Forces for the District of Arizona and the Central District of California, where he has participated in the indictment and prosecution of individuals related to events of 9/11 as well as the planning and implementation of Operation Tarmac/Operation Safe Harbor in Phoenix and Los Angeles.

Questions pertaining to in this article can be directed to SAUSA John K. Webb, 602-514-7544 (Phoenix) or 213-894-3518 (Los Angeles).✠

Hawala

David Marshall Nissman
United States Attorney
District of Virgin Islands

I. Introduction

Step back in time several hundred years and imagine that you are a merchant in China, India, or the Middle East. Picture a caravan crossing the desert on camel. You move between several destinations and need to carry money or gold on the Silk Road in order to purchase goods when you reach the marketplace. But gold is heavy and the criminal element knows that it is likely you are carrying valuables. Thus, you are an easy mark for highwaymen. In order to avoid these robberies, you and your colleagues develop your own banking system that became known by several different names such as "hawala", "hundi," or fei ch'ien. The key characteristics of this system are that it is based on trust and a network of connections.

II. How does Hawala work?

Here's how it works: Ahmed, who is in the United States, goes to his Hawala Broker and tells Broker #1 that he needs to get $10,000 in rupees to Mohammed, who is in Pakistan. Ahmed delivers $10,000 to Broker #1 and receives a receipt that may be nothing more than a scrap of paper. Broker #1 contacts his Pakistani counterpart, Broker #2, and tells him to deliver $10,000 to Mohammed. In fact, Broker #2 may actually give door to door service by having the funds delivered to the home of Mohammed (after a question and answer code verifies that Mohammed is the intended recipient). No money initially changes hands between Broker #1 and Broker #2. No money actually crosses a border. In many ways it is an invisible transaction. Each broker gets a small commission on the transaction. One of the brokers may make an additional profit on the foreign exchange rate between dollars and rupees, if there is a black market in one of the currencies exchanged. In most cases, the hawaladars give a better exchange rate to their clients than their clients would have received from the banks.

How does Broker #2 get compensated for the $10,000 he paid out to Mohammed? If there are frequent commercial transactions between the two brokers, over a period of time, an equalization of accounts may occur. If there is an unequal series of transactions, then the hawaladars must arrange something else to make the transactions right. One of the essential features of the hawala exchange system is that a myriad of different economic transactions, having no bearing to the original transaction, may be used to accomplish the equalization of accounts.

Unlike the original system in which contact between various brokers in different countries was difficult, some hawaladars use modern technology to assist them. The two brokers may use telephones, fax machines, or the Internet to make contact. Typically the transaction will be made by using various codes. Slips of paper may be generated while a transaction is pending. Thereafter, the records may be destroyed. However, in the West, the information age makes it easy to store records. In some cases in Europe and the United States investigators are finding that meticulous records of hawala exchanges are preserved.

Cash, Gold, diamonds, and tanzanite, as well as other precious stones, may be smuggled by courier between the two hawaladars. Wire transfers between accounts may also be used to square the transaction. One common method of equalization involves the use of padded invoices of goods. In *United States v. Ahmad,* 213 F.3d 805 (4th Cir. 2001), the Fourth Circuit described a hawala scheme in which defendant Ahmad received millions of dollars in cash payments from Pakistanis working in the United States who wanted to send money to their families. Ahmad structured all the transactions to avoid triggering currency reporting requirements. Ahmad then used the deposited money to structure bridge loans to a number of Pakistani companies. Ahmad had a Pakistani company inflate invoice prices for

surgical equipment shipped from Pakistan to a United States company, Falcon Instruments. Falcon would then request a discount on the surgical equipment, which Ahmad would grant. The invoices created false paperwork to disguise the other money being sent to Pakistan for the families of the hawala clients.

One of the foremost experts on hawala, Patrick Jost, formerly of the Financial Crimes Enforcement Network (FinCEN), recently testified before Congress and explained how this invoicing can work both ways:

> Another possibility is that the hawaladar has money in a country and cannot remove it due to measures designed to counter capital flight. These measures can be circumvented via hawala. The hawaladar accepts money in his current country of residence, and has an associate "drain" the supply of money in the other country until it is gone. Some hawaladars utilize invoice manipulation schemes to settle their debts. These schemes are often necessary because of remittance controls.
>
> For example, a hawaladar operating in the United States could send an associate $100,000 by purchasing $200,000 worth of goods that his associate wants. He ships the merchandise with an invoice for $100,000. The associate receives the merchandise and pays the first hawaladar $100,000. This payment appears to be legitimate because of the shipment and the invoice. The associate has $200,000 worth of merchandise for which only $100,000 was paid. This technique, known as "under invoicing" is one way of circumventing remittance controls as well as settling debts between hawaladars.
>
> The inverse of this, "over invoicing" also exists. It would, for example, be used to transfer money to the United States. A hawaladar operating in the United States would purchase $100,000 worth of goods that his associate wants. He would ship the goods with an invoice for $300,000. Payment of this amount would allow the associate to move $200,000 to the United States. Like "under invoicing", this technique can be used to circumvent remittance controls and settle debts between hawaladars.
>
> What might be termed "debt assignment" also takes place. If hawaladar A owes money to hawaladar B, and hawaladar B owes money to hawaladars C and D, hawaladar B might ask A to settle the debts with C and D, settling his debt with B.
>
> As with other aspects of hawala transactions, there is a great deal of flexibility. Hawaladars will use these settlement methods—or variations on them—as needed and dictated by circumstances."

Patrick Jost, testimony before United States Senate, Committee on Banking, Housing and Urban Affairs, Subcommittee on International Trade and Finance, November 14, 2001.

III. Why use Hawala?

It is important to understand how attractive hawala is to the average foreign born wage earner working in the United States. In a FinCEN publication entitled *The Hawala Alternative Remittance System and its Role in Money Laundering* by Patrick Jost and Harjtt Singh Sandhi, the authors illustrated the practicalities involved in an hawala transfer. A portion of that article is quoted, at length, below.

> An effective way to understand hawala is by examining a single hawala transfer. In this scenario, which will be used throughout this paper, Abdul is a Pakistani living in New York and driving a taxi. He entered the country on a tourist visa, which has long since expired. From his job as a taxi driver, he has saved $5,000 that he wants to send to his brother, Mohammad, who is living in Karachi. Even though Abdul is familiar with the hawala system, his first stop is a major bank.
>
> At the bank, he learns several things:

- The bank would prefer that he open an account before doing business with them;
- The bank will sell him Pakistani rupees (Rs) at the official rate of 31 to the dollar; and
- The bank will charge $25 to issue a bank draft.

This will allow Abdul to send Mohammad Rs 154,225. Delivery would be extra; an overnight courier service (surface mail is not always that reliable, especially if it contains something valuable) can cost as much as $40 to Pakistan and take as much as a week to arrive.

Abdul believes he can get a better deal through hawala, and talks to Iqbal, a fellow taxi driver who is also a part-time hawaladar.

Iqbal offers Abdul the following terms:

- A 5% "commission" for handling the transaction;
- 35, instead of 31, rupees for a dollar; and
- Delivery is included.

This arrangement will allow Abdul to send Mohammad Rs 166,250. As we will see, the delivery associated with a hawala transaction is faster and more reliable than in bank transactions. He is about to make arrangements to do business with Iqbal when he sees the following advertisements in a local "Indo-Pak" newspaper (such advertisements are very common):

MUSIC BAZAAR AND TRAVEL SERVICES AGENCY

•Cheap tickets to India,
Pakistan, Bangladesh, Sri Lanka, Dubai
•Great rupee deals (service to India and Pakistan)
•Large movie rental selection
•Video conversions
•Latest Hollywood hits on CD and cassette
•Prepaid international calling cards
•Pager and cellular activations (trade-ins welcome)
•Conveniently located in Jackson Heights
(718) 555-1111 ask for Nizam or Yasmeen
(718) 555-2222 [fax]
(718) 555-2121 [pager]

Abdul calls the number, and speaks with Yasmeen. She offers him the following deal:

- A fee of 1 rupee for each dollar transferred;
- 37 rupees for a dollar; and
- Delivery is included.

Under these terms, Abdul can send Mohammad Rs 180,000. He decides to do business with Yasmeen.

The hawala transaction proceeds as follows:

- Abdul gives the $5,000 to Yasmeen;
- Yasmeen contacts Ghulam in Karachi, and gives him the details;
- Ghulam arranges to have Rs 180,000 delivered to Mohammad.

Even though this is a simple example, it contains the elements of a hawala transaction. First, there is trust between Abdul and Yasmeen. Yasmeen did not give him a receipt, and her record keeping, such as it may be, is designed to keep track of how much money she owes Ghulam, instead of recording individual remittances she has made. There are several possible relationships she can have with Ghulam (these will be discussed later); in any case she trusts him to make the payment to Mohammad. This delivery almost always takes place within a day of the initial payment (a consideration here is time differences), and the payment is almost always made in person. Finally, in some scenarios, he trusts her to repay him the equivalent of either $5,000 or Rs 180,000.

Connections are of equal importance. Yasmeen has to be connected to Ghulam in Karachi to arrange this payment. As her advertisement indicates, she also offers service to India, so she either knows, or has access to, someone who can arrange payment there. Hawala networks tend to be fairly loose, communication usually takes place by phone or fax (but email is becoming more and more common).

To complete this discussion, there are two related issues to be addressed. The first is the relationship between Yasmeen and Ghulam, and the second is how Ghulam "recovers" the money that he paid to Mohammad on Abdul's behalf.

As was stated above, hawala works through connections. These connections allow for the establishment of a network for conducting the

hawala transactions. In this transaction, Yasmeen and Ghulam are part of the same network. There are several possible ways in which this network could have been constructed.

The first possibility is that Yasmeen and Ghulam are business partners (or that they just do business together on a regular basis). For them, transferring money is not only another business in which they are engaged but a part of their normal business dealings with one another. Another possibility is that, for whatever reason, Ghulam owes Yasmeen money. Since many countries make it difficult to move money out of the country, Ghulam is repaying his debt to Yasmeen by paying her hawala customers; even though this is a very "informal" relationship, it is quite typical for hawala. A third (and by no means the final) possibility is that Yasmeen has a "rupee surplus" and Ghulam is assisting her in disposing of it.

In the last two cases, Ghulam does not need to recover any money; he is either repaying an existing debt to Yasmeen, or he is handling money that Yasmeen has entrusted to him, but is unable to move out of the country. In the first case, where Yasmeen and Ghulam are partners, a more formal means of balancing accounts is needed.

One very likely business partner scenario is an import/export business. Yasmeen might import CDs and cassettes of Indian and Pakistani music and 22 carat gold jewelry from Ghulam, and export telecommunications devices to Ghulam. In the context of such a business, invoices can be manipulated to "conceal" the movement of money.

If Yasmeen needs to pay Ghulam the Rs 180,000 that he has given to Mohammad, she can do it by "under invoicing" a shipment to him. She could, for example, send him $20,000 worth of telecommunications devices, but only invoice him for $15,000. Ghulam pays Yasmeen $15,000 against this invoice. The "extra" value of goods, in this case $5,000 (the equivalent of Rs 180,000) is the money that she owes him.

In order to move money the other way (in this case, from Pakistan to New York), "over invoicing" can be used. For this example, it is assumed that Ghulam owes Yasmeen $5,000. She could buy $10,000 of telecommunications devices, and send it to Ghulam with an invoice for $15,000. Ghulam would pay her $15,000; this covers the $10,000 for the telecommunications devices as well as the other $5,000.

Since many hawala transactions (legitimate and illegitimate) are conducted in the context of import/export businesses, the manipulation of invoices, as discussed above, is a very common means of settling accounts after the transactions have been made.

IV. Hawala and terrorism

The use of precious stones, particularly diamonds and tanzanite, has been widely used by Al Qaeda to move and launder money and to finance terror attacks. The investigation into the 1998 African embassy bombings revealed that one of the convicted defendants, Wadih al-Hage, a bin Laden operative, formed Tanzanite King, a company used to launder money through tanzanite sales. According to an article that appeared in the Washington Post entitled “Al Qaeda's Road Paved With Gold,” by Douglas Farah (Washington Post Foreign Service Sunday, February 17, 2002) Al Qaeda appears to be in the conflict diamond trade. Conflict diamonds are diamonds mined, stolen, and illicitly sold by rebels. One group involved in the mining and sale of conflict diamonds in Sierra Leone is the Revolutionary United Front (RUF) which is on the State Department’s Immigration Only Terrorist Organization list (ITO) pursuant to 8 U.S.C. 1182(a)(3)(B)(vi). Various newspapers report that links between RUF and Al Qaeda go back to 1998. RUF denies that it sells diamonds to Al Qaeda. The use of diamonds as a commodity by Al Qaeda can take various forms. Al Qaeda operatives appear to have purchased diamonds at retail costs just prior to the 9/11 attacks, perhaps in anticipation that bank accounts would be frozen by the United States.

While the ancient hawala system may have had a noble purpose based in fact on crime prevention, the modern system has a far more complex genesis. Hawala is partially built on schemes to defraud governments of taxes and regulatory fees. It is a method of money laundering and it is sometimes used to move money between terrorists. Hawala techniques were used to move Al Qaeda and Taliban treasure from Afghanistan. But the hawala system is also a very efficient way in which wage earners can send money to family members in foreign countries without having to pay the high fees banks charge. In fact, it is cheaper, more secure, more convenient and faster than conventional methods. Hawaladars charge small commissions for people wanting to move money to family members because these transactions often help them move criminally derived proceeds for which they charge higher commissions. While hawala operates all over the world, it also operates in countries that have no modern banking or wire transfer services. In those places it isn't an alternative remittance system - it is the remittance system. The reasons for its continuing viability is that it is a cheap, fast, secure, and convenient network for people who need to send money to their families. While the majority of hawala customers are legitimate, it's a different question how much of the money is illegitimate.

Many of the existing hawala networks may have grown with gold smuggling operations that began in the 1960's between the Middle East and Asia. Gold smugglers began sending gold between the Gulf States and South Asia. After the gold was sold in South Asia, the smugglers needed a method to get the cash back to the Middle East. There were many Pakistanis and Indians working in the Middle Eastern Gulf States who typically sent money in regular intervals to their families in their home countries. The hawaladars essentially operated a money remitter business in which the foreign workers received favorable rates and low fees to "send" money to Pakistan, India and other points in South Asia. The workers physically gave their wages (or a part of them) to the hawaladars in the Gulf States thus paying for the gold sold in South Asia. The South Asians who held the proceeds for the gold sales then gave the money to the families of the wage earners while keeping their share of the profits from the gold smuggling. Instead of paying to transport the money they charged the wage earners a commission on the remitter transactions thus offering a second profit to the criminal organization.

The United Arab Emirates, Pakistan, and India form a hawala triangle that secretly moves money throughout the world. In Pakistan, two to five billion dollars move through the Pakistani hawala system annually which is more than the amount of the legitimate foreign transfers occurring in the banking system.

The system also operates all through the United States. Many foreign nationals come to the United States for the purpose of obtaining jobs that can be used to provide support for their families in impoverished nations. For example, a version of the hawala system was used by Somalis to send their earnings to their families in Somalia. In fact, Somalia doesn't have much of a conventional banking system and hawala operates in its stead. Hawala may also be used by check cashing businesses as the checks can be freely transported to areas in need of equalizing transactions. Couriers may move cash. Smuggling fees may be paid through hawala. For example smuggling operatives who move Chinese, Japanese and Russian aliens through the Caribbean to the United States sometimes get their fees from hawala transactions. It is not just the hawala triangle of Pakistan, Afghanistan and India - it's all over the world.

Note that countries without a banking system that handle foreign exchanges, countries that have restrictions on taking currency out of country (e.g. India), or countries that have embargoes imposed against them (e.g. Iraq), provide an opportunity for hawaladars to fill a need. It is decidedly low tech in many of these places. In some cases, Somalia hawaladars use the radio to notify recipients that money has arrived because phones are not in widespread use. The face of these systems may change as Internet usage increases in these parts of the world.

Hawala is described by the Financial Action Task Force (hereafter FATF) as an alternative remittance system for moving and laundering

money, and it has similarities with several other such schemes in place throughout the world. The Colombian Black Market Peso Exchange is an alternative remittance system in which drug dealers needing Colombian pesos, and Colombian businessmen needing dollars to purchase American made goods, operate through money brokers who collect fees on both sides of the exchange. In China, brokers use an ancient system called fei qian or "flying money" that is virtually identical to hawala.

Juan Zarate, Deputy Assistant Secretary, Terrorism and Violent Crime, Department of the Treasury, and formerly with TVCS, in testimony before the House Financial Services Subcommittee on Oversight and Investigations on February 12, 2002 stated that:

> FinCEN is forming an Alternate Remittance Branch [now called "non-traditional methodology section"] which will be responsible for the analysis of Bank Secrecy Act data and other information to identify mechanisms and systems used by criminal organizations to move operational funds in support of domestic and international activity. Analysis will focus initially on Informal Value Transfer Systems (IVTS) such as hawala, hundi and other Asian and South American systems as a potentially key but inadequately understood methodology for funds movement; development of indicators of IVTS use by criminal organizations to support law enforcement initiatives to combat criminal activity; and identification of policy implications of IVTS for law enforcement and financial regulators. Analysis will expand to include identification of the methods by which IVTS intersects with regulated funds transfer systems, and then identification of criminal funds movement methodologies based entirely on the legitimate financial industry.

While a pure hawala system is very hard to investigate due to the lack of records and the fact that the money doesn't actually move, there are several opportunities to penetrate hawalas, particularly in the United States. First of all, in the West, it is difficult for hawaladars to resist the convenience of modern technology. Fax machines, email, and wire transfers, have made their appearances in hawala transactions. Moreover, in the United States, it is more difficult to structure real estate transactions, commercial exchanges of goods, car purchases, and stock transfers, without the use of financial institutions.

The Al-Barakaat organization is an example of a hybrid hawala system turned modern. Somalis working in the United States used the Al Barakaat network to send money to their families in Somalia. Al Barakaat used financial institutions, and other modern methods of transfer, to send the funds to Somalia. Because this network used financial institutions, law enforcement was able to discover the transactions through the generation of Suspicious Activity Reports (SARS) produced by the banks pursuant to their obligations under the Bank Secrecy Act (BSA). There were a series of coordinated law enforcement actions in the Al Barakaat investigation. These actions were coordinated with Treasury's execution of blocking actions pursuant to the Executive Order against al Barakaat-related entities in Georgia, Minnesota, and Washington State.

The Grand Jury in Alexandria, Virginia recently indicted persons associated with Al-Barakaat for, among other things, structuring financial transactions to avoid the currency reporting violations. A portion of Count One of the indictment is included here to demonstrate how such networks work and one method for pleading such allegations:

The Grand Jury Charges That:

1. Title 31, United States Code, Section 5313 requires any financial institution that engages in a currency transaction (*i.e.*, a deposit or withdrawal) in excess of $10,000 with a customer to report the transaction to the Internal Revenue Service on Form 4789, Currency Transaction Report ("CTR"). These regulations also require that multiple transactions be treated as a single transaction if the financial institution has knowledge that they are by, or on behalf of, the same person, and they result in either currency received or disbursed by the financial institution totaling more than $10,000 during any one business day.

2. CTRs often are used by law enforcement to uncover a wide variety of illegal activities including narcotics trafficking and money laundering. Many individuals involved in these illegal activities are aware of such reporting requirements and take active steps to cause financial institutions to fail to file CTRs. These active steps are often referred to as "smurfing" or "structuring" and involve making multiple cash deposits, in amounts less than $10,000, to multiple banks and/or branches of the same bank on the same day or consecutive days. Structuring cash deposits to avoid triggering the filing of a CTR by a financial institution is prohibited by 31 U.S.C. § 5324(a).

3. Beginning in or about February 1998, and continuing thereafter up to on or about November 7, 2001, within the Eastern District of Virginia and elsewhere, the defendants, ABDIRAHMAN SHEIKH-ALI ISSE and ABDILLAH S. ABDI, did unlawfully and knowingly combine, conspire, confederate and agree with each other and others known and unknown to the grand jury, to cause domestic financial institutions to fail to file Currrency Transaction Reports required by law, and to structure transactions with domestic financial institutions, both for the purpose of evading the reporting requirements of section 5313(a) of Title 31, United States Code, in violation of Title 31, United States Code, Sections 5322 and 5324.

4. The primary purpose of the conspiracy was to transmit money through the United Arab Emirates and the Al-Barakat money transfer network to Somalia, Ethiopia, Kenya, and the Sudan without attracting the attention of the law enforcement authorities.

Ways, Manners, and Means

The ways, manner and means by which this purpose was carried out included the following:

5. Between 1997 and November 7, 2001, ABDIRAHMAN SHEIKH-ALI ISSE operated a money transmitting service, first from his residence at 4949 Manitoba Drive in Alexandria, Virginia, and later from the premises of Al-Barakat Rage Associates at 4810 Beauregard Street in Alexandria, Virginia. During that time, ABDIRAHMAN SHEIKH-ALI ISSE and his conspirators collected millions of dollars in cash from individuals wishing to transmit money to Somalia, Ethiopia, Kenya, and the Sudan. ABDIRAHMAN SHEIKH-ALI ISSE and his coconspirators deposited such monies in multiple branches of various banks in Northern Virginia, before wire transferring those monies to the Al-Barakat network in the United Arab Emirates for further transfer to Somalia, Ethiopia, Kenya, and Sudan, all without obtaining a money-transmittal license as required by Virginia and federal law.

6. The defendants collected monies from various individuals and aggregated those monies in their office before depositing such monies in domestic financial institutions.

7. Between December 1996 and June 1998, defendant ABDIRAHMAN SHEIKH-ALI ISSE directed deposits into First Union Bank account #3050001728626 in the name of Abdirahman Sheikh Ali Isse, 4949 Manitoba Drive, Apartment #711, Alexandria, Virginia, and the wire transfer from that account of more than $274,000 to Barako Trading Company at Emirates Bank International in the United Arab Emirates.

8. Between February and August 1998, defendant ABDIRAHMAN SHEIKH-ALI ISSE directed deposits into First Union Bank account #1050002756152, in the name of Abdallah Abdulkadir, 4949 Manitoba Drive, Apartment #303, Alexandria, Virginia, and the wire transfer from that account of more than $214,000 to Barako Trading Company, Emirates Bank International in the United Arab Emirates.

9. Between March 1998 and October 1999, defendant ABDIRAHMAN SHEIKH-ALI ISSE directed deposits into First Union Bank account #1020003281601, in the name of Abdirahman Sheikh Ali Isse, 4949 Manitoba Drive, Apartment #711, Alexandria, Virginia, and the wire transfer from that account of more than $469,000 to Barako Trading Company or the Al-Baraka Exchange at Emirates Bank International in the United Arab Emirates.

10. Between February 1998 and August 1999, defendant ABDIRAHMAN SHEIKH-ALI ISSE directed deposits into Bank of America account #4111357305 in the name of Abdirahman S. Isse, 4949 Manitoba Drive, Apartment #711,

Alexandria, Virginia, and the wire transfer from that account of more than $236,000 to Barako Trading Company or the Al-Baraka Exchange at Emirates Bank International in the United Arab Emirates.

11. Between June 1998 and December 1999, defendant ABDIRAHMAN SHEIKH-ALI ISSE directed deposits into Bank of America #004138600873 in the name of Abdisalam A. Ali, 4949 Manitoba Drive, Apartment #303, Alexandria, Virginia, and the wire transfer from that account of more than $287,000 to Barako Trading Company or the Al-Baraka Exchange at Emirates Bank International in the United Arab Emirates.

12. Between April and October 1999, defendant ABDIRAHMAN SHEIKH-ALI ISSE directed deposits into Chevy Chase Account #0683229508, in the name of Abukar A. Ali, 4949 Manitoba Drive, Apartment 303, in Alexandria, Virginia, and the wire transfer from that account of more than $84,000 to Al Baraka Exchange at Emirates Bank International in the United Arab Emirates.

13. Between August 2000 and January 2001, defendant ABDIRAHMAN SHEIKH-ALI ISSE directed deposits into First Union Bank account #1010036404449, in the name of Abdillah S. Abdi, 4949 Manitoba Drive, Apartment #303, Alexandria, Virginia, and the wire transfer from that account of more than $37,000 to Al Baraka Exchange at Emirates Bank International in the United Arab Emirates.

14. Between April 1999 and November 7, 2001, defendant ABDIRAHMAN SHEIKH-ALI ISSE directed deposits into Chevy Chase Bank account #0683229940 in the name of Abdirahman S. Isse, 4949 Manitoba Drive, Apartment #303, Alexandria, Virginia, and the wire transfer from that account of more than $175,000 to Al-Baraka Exchange at Emirates Bank International in the United Arab Emirates.

15. Between October 1999 and November 7, 2001, defendant ABDIRAHMAN SHEIKH-ALI ISSE deposited or directed deposits into Chevy Chase Bank Account #1554311173 in the name of Rage Associates, 4949 Manitoba Drive, Apartment #303, Alexandria, Virginia, and the wire transfer from that account of more than $4,400,000 to Al-Baraka Exchange at Emirates Bank International in the United Arab Emirates.

16. The defendants structured their deposits at First Union Bank, Bank of America, and Chevy Chase Bank into amounts less than $10,000 at a time to avoid the filing of a Currency Transaction Report that would report such deposits to the Internal Revenue Service by the domestic financial institutions into which such monies were deposited.

17. The defendants structured their deposits into various bank accounts at First Union Bank, Bank of America, and Chevy Chase Bank to avoid depositing more than $10,000 into one bank account in one day and thereby trigger the filing of a Currency Transaction Report reporting their deposits to the Internal Revenue Service.

18. The defendants structured their deposits into various branches of First Union Bank, Bank of America, and Chevy Chase Bank to avoid depositing more than $10,000 into one branch on one day and thereby trigger the filing of a Currency Transaction Report reporting their deposits to the Internal Revenue Service.

19. The defendants arranged for their deposits to be made by various individuals to avoid the appearance of depositing more than $10,000 in one day, and thereby trigger the filing of a Currency Transaction Report reporting their deposits to the Internal Revenue Service.

20. The defendants charged customers a 4% fee for any wire transfer, retained 1% themselves, and remitted the remaining 3% to the Al-Barakat network in the United Arab Emirates.

V. Patriot Act provisions

Attitudes about Informal Value Transfer Systems like Hawala have changed since 9/11. Prior to the terrorist attacks, nations hurt by the black market trade in currency, like India, were anxious to have the Western nations pass anti-Hawala rules. The West generally responded by suggesting those countries change their restrictive laws on currency exchange. Arguably, by making it a general intent crime to operate a money transmitting business without a license under state law, Section 373 of the USA Patriot Act signals

an attitudinal shift in our view of IVTS. *See* 18 U.S.C. § 1960. Moreover, the amended Bank Secrecy Act treats some underground banking systems as financial institutions and creates registration and reporting duties. Section 359 (b) adds a Suspicious Activity Report (SAR) reporting requirement by amending 31 U.S.C. § 5330(d)(1)(A) to include " any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system."

Section 361(F) of the USA Patriot Act directs FinCEN to assist federal, state, local, and foreign, law enforcement and regulatory authorities in combatting the use of informal, nonbank, networks and payment and barter system mechanisms that permit the transfer of funds or the equivalent of funds, without records and without compliance with criminal and tax laws.

The Treasury Department has commissioned a Temple University professor to perform a study on hawala and other informal value transfer techniques. Dr. Nikos Passas, a renowned expert on this subject and transnational crimes, is the author of INFORMAL VALUE TRANSFER SYSTEMS AND CRIMINAL ORGANIZATIONS: A STUDY INTO SO-CALLED UNDERGROUND BANKING NETWORKS (1999), which provides the most systematic look at these issues to date. This report, and the executive summary, may be downloaded from http://www.minjust.nl:8080/b_organ/wodc/publications/ivts.pdf. Dr. Passas is currently assisting in several investigations and is available to respond to questions from prosecutors. His telephone number is (215) 204-8605 and email: passas@temple.edu.

Dr. Passas emphasizes that not all hawala-type operations necessarily or knowingly assist terrorists, drug traffickers, or other serious criminals. In some parts of the world, these informal networks are still the only option people have to receive support from their relatives in the West.

Nonetheless, operating an unlicensed money remitting business is now a crime. Where money or financial instruments actually leave the United States, there are tools law enforcement can use to investigate the transaction. In some cases, money leaving the United States has been skimmed to avoid paying taxes and the transactions have been structured to disguise the skimming. Moreover, when more than $10,000 in cash or in financial instruments is transported from the United States to any foreign destination, the courier or sender must report this event or face a five-year felony. *See* 31 U.S.C. §§ 5316 (a)(1)(A) and 5324(b).

VI. Suggestions for conducting hawala investigations:

(1) Conduct educational and compliance training of all affected industries including banks, brokerage houses, wire services, coin dealers, commodities brokers, real estate conglomerates and precious stone dealers, to alert the industries to the use and operation of hawala. This will spark the generation of SARS and other tips to law enforcement.

(2) Conduct a community-wide survey to identify the money remitters in the community. Determine whether these entities are required to have licenses under state law. Determine whether the hawala broker is an unlicensed money remitter in violation of 18 U.S.C. § 1960. Note that the USA PATRIOT ACT now makes § 1960 a general intent crime and the prosecution does not have to prove that the remitter knew that there was a state licensing requirement. There is no requirement that the funds transmitted be from an otherwise illegal source.

(3) Examine whether required reporting statutes are followed. Review the new requirements under the USA PATRIOT Act. For example, coin dealers are now required to file reports pursuant to 31 U.S.C. § 5331. Bulk cash smuggling is a crime. 31 U.S.C. § 5332. Securities brokers will also be required to file SARS.

(4) Examine whether false statements are made on required customs forms in violation of 18 U.S.C. § 1001. This was the case in *United States v. Ahmad,* 213 F.3d 805 (4th Cir. 2001) discussed earlier.

(5) Examine whether transactions are structured to avoid reporting requirements in violation of 31 U.S.C. §§ 5313, and 5324(a)(3). *See also United States v. Ahmad,* 213 F.3d 805 (4th Cir. 2001).

(6) If more than $10,000 cash is smuggled to equalize hawala transactions consider using Title 31 U.S.C. § 5332, the bulk cash smuggling statute.

(7) If the hawala transaction is for a criminal purpose, the commission may be significantly higher than the average .5- 1.5% percent charged on most hawala transactions. Investigators that encounter high commissions may wish to scrutinize the transaction closely. (8) Also look for aggregation of small sums as opposed to large single sum transactions. The collection method may be different when there is a criminal purpose. If the hawaladar and client meet on the side of the road and a bag of cash is thrown into the trunk of a car, somebody ought to be filing a SAR.

VII. Conclusion

It is important to understand how hawala works so that we are able to stop the use of this system to finance terrorism and other criminal enterprises. At the same time it is equally important to be sensitive to the fact that there are many innocent people who use the system to send help to family members in places where there is no banking system or reasonable alternatives. Nonetheless, the hawaladars have an obligation to license their businesses and to comply with the requirements of the Bank Secrecy Act. If they choose not to comply with the law, it is not the United States government that is prohibiting immigrants from sending needed help to family members, but the hawaladars themselves.❖

ABOUT THE AUTHOR

❑**David M. Nissman** is the United States Attorney for the District of Virgin Islands. He is also the author of PROVING FEDERAL CRIMES (2001) and the former Editor in Chief of the UNITED STATES ATTORNEYS' BULLETIN.✠

Forfeiture of Terrroist Assets Under the USA PATRIOT Act of 2001

Stefan D. Cassella
Deputy Chief, AFMLS
Criminal Division

The USA PATRIOT Act (hereafter "Patriot Act"), Pub. L. 107-56, 115 Stat. 272, contains a number of provisions that may be used by federal law enforcement authorities to seize and forfeit the assets of terrorist organizations, assets that are derived from terrorist acts, and assets that are intended to be used to commit terrorist acts in the future. Some of the new provisions are specifically intended to be used in, and are limited to, the terrorism context. Others apply more generally, but will undoubtedly be used in terrorism cases.

I. 18 U.S.C. § 981(a)(1)(G)

Title 18, United States Code, section 981, is the general-purpose civil forfeiture statute applicable to most federal crimes. Among other things, it authorizes the forfeiture of property involved in money laundering cases (18 U.S.C. § 981(a)(1)(A)), property derived from and used to commit certain foreign crimes (18 U.S.C. § 981(a)(1)(B)), and the proceeds of any offense designated as a "specified unlawful activity" (18 U.S.C. § 981(a)(1)(C)).

Section 806 of the Patriot Act added a new provision to section 981 that is obviously a response to September 11. Section 981(a)(1)(G) authorizes forfeiture of all assets belonging to anyone engaged in terrorism, any property

affording any person a "source of influence" over a terrorist organization, and any property derived from or used to commit a terrorist act.

This language is extraordinarily broad. Unlike the money laundering statute, which authorizes the forfeiture only of property "involved in" the money laundering offense (18 U.S.C. § 981(a)(1)(A)), or the drug statute, which authorizes forfeiture only of property derived from or used to commit the drug offense (21 U.S.C. § 881(a)), section 981(a)(1)(G) does not require any nexus between property and a terrorism offense. To the contrary, once the Government establishes that a person, entity, or organization is engaged in terrorism against the United States, its citizens or residents, or their property, the Government can seize and ultimately forfeit *all assets*, foreign or domestic, of the terrorist entity—whether those assets are connected to terrorism or not.

The only parallel in federal law is to the Racketeer Influenced and Corrupt Organizations (RICO) statute, which permits the forfeiture of all interests a person has in a RICO enterprise or any property affording that person a source of influence over the enterprise, whether the forfeited property was tainted in any way by the racketeering activity or not. *See* 18 U.S.C. § 1963(a)(2). In fact, the "source of influence" language that appears in the RICO statute is repeated in section 981(a)(1)(G).

Enactment of section 981(a)(1)(G) was necessary because the law previously had no forfeiture provisions tailored to terrorism.

A. Civil vs. Criminal forfeiture

Section 981(a)(1)(G) appears in the general purpose civil forfeiture statute, but it is really both a civil and criminal forfeiture provision. That is because federal law now provides that any forfeiture that can be done as a civil forfeiture can also be done as a criminal forfeiture. *See* 28 U.S.C. § 2461(c). Thus, if the Government apprehends and prosecutes a terrorist, it can seek forfeiture of all assets in the criminal case under the new statute, provided that the act giving rise to the forfeiture occurred after October 21, 2001, when the new law took effect. But the true utility of section 981(a)(1)(G) is likely to be in the civil forfeiture context, because in civil forfeiture cases the Government can proceed against the assets even if it does not apprehend the defendant because he or she is dead or remains a fugitive from justice.

B. Procedure for civil forfeiture

In most respects, a forfeiture under section 981(a)(1)(G) will work just like any other civil forfeiture action under federal law. The Government can seize property based on probable cause. Generally the seizure must be pursuant to a warrant, but warrantless seizures are authorized in exigent circumstances. *See Florida v. White*, 526 U.S. 559, 119 S. Ct. 1555 (1999). But the seizure of property is only the beginning of the process. Seized property may be under Government control, but it still belongs to the property owner. *See United States v. A Group of Islands*, 185 F. Supp. 2d 117, 121 n.7, (D.P.R. 2001) (seizure may be based on probable cause to believe the property will ultimately be proved forfeitable, but it entails only taking possession and control; to become the owner of the property, *i.e.*, to transfer title to the property to the United States, the Government must commence a forfeiture action). To convert a seizure into a forfeiture—that is, to take title to the property permanently away from the property owner and transfer it to the Government—the Government must commence a formal forfeiture action.

The provisions of the Civil Asset Forfeiture Reform Act (CAFRA) of 2001 set forth the procedure for converting a seizure into a forfeiture. *See* 18 U.S.C. § 983. In short, the Government has 60 days from the date of the seizure to send notice of the forfeiture action to all interested parties (section 983(a)(1)). If no one files a claim challenging the forfeiture in 30 days (section 983(a)(2)), the Government can declare the property forfeited by default (19 U.S.C. § 1609). If someone does challenge the forfeiture, however, the Government has 90 days to return the property or to commence either a civil or criminal forfeiture action in federal court (section 983(a)(3)).

All of that is standard civil forfeiture law. It would work the same way in a terrorism case as in any other case. In other words, if the Government

seizes a terrorist's assets under section 981(a)(1)(G), the case could be in federal court, before a jury in less than six months. The only concession Congress has made to the unique nature of terrorism cases concerns the procedure at trial. Under section 316 of the Patriot Act, if the case goes to trial under section 981(a)(1)(G), and the property involves the assets of "suspected international terrorists," the normal burden of proof is reversed: Once the Government makes its initial showing of probable cause, the claimant has the burden of proving by a preponderance of the evidence that his or her property is *not* subject to confiscation. In almost all other forfeiture cases, of course, the Government has the burden of proving the forfeitability of the property. *See* 18 U.S.C. § 983(c). Moreover, in the forfeiture trial, hearsay is admissible if the evidence is reliable, and compliance with the normal Rules of Evidence "may jeopardize the national security interests of the United States." But these two exceptions aside, the forfeiture of terrorist assets under section 981(a)(1)(G) would proceed along a very short timetable, would likely involve a full-blown jury trial if contested, and could result in the payment of attorneys' fees to the claimant if the Government fails to prevail. *See* 28 U.S.C. § 2465.

C. Relationship to IEEPA

For whatever reason, there have been few instances since September 11 in which the Government has sought to seize or forfeit terrorist assets under the new statute. The fact is that the Department of the Treasury has separate authority to freeze and confiscate terrorist assets under the International Emergency Economic Powers Act (IEEPA) that is specifically exempted from CAFRA and from virtually all of the other evidentiary and due process requirements of federal forfeiture law. *See* 18 U.S.C. § 983(i). Thus, all the stories in the media about the President freezing bank accounts of terrorists since September 11 have been IEEPA cases, not cases brought by the Department of Justice under section 981(a)(1)(G).

Under IEEPA, Treasury—that is, the Office of Foreign Asset Control (OFAC)—can freeze (*i.e.*, seize) suspected terrorist assets indefinitely based on a presidential order. And if Treasury ultimately decides to convert its blocking order into a forfeiture (or "confiscation," which is the same thing), it would not be bound by any of the CAFRA procedures, except for the right of the property owner to contest the forfeiture by filing a claim in federal court. *See* section 316(a) of the Patriot Act.

On the other hand, Treasury could decide to refer a case to the Department of Justice for formal forfeiture of the property under section 981(a)(1)(G). The Department of Justice stands ready to pursue any such case if it is referred.

II. Forfeiture of Property Intended To Be Used To Commit Terrorism

There are some other provisions in the Patriot Act that are actually much more likely to be used to confiscate assets from terrorists. The key is to understand the interrelationship between the asset forfeiture and money laundering statutes.

Under section 981(a)(1)(A), the Government can forfeit any property involved in a money laundering offense. That can be either "clean" or "dirty" property, as long as it is involved in the money laundering. *See United States v. McGauley*, 279 F.3d 62, 76 n.14 (1st Cir. 2002) (collecting cases and citing legislative history).

The problem has always been that the money laundering statutes are "backward looking." Most of them focus on what the criminal is doing with the proceeds of a crime that has already been committed. *See*, *e.g.*, 18 U.S.C. § 1956(a)(1)(B)(i) (concealing or disguising the proceeds of a prior crime). Terrorism cases, however, usually deal not with someone who is trying to hide the proceeds of a past crime, but someone who is moving money into or through the United States with the intent to use it to commit a crime—a terrorist act—in the future. This is called "reverse money laundering."

Only two federal money laundering statutes address reverse money laundering, but the Patriot Act has expanded both of them considerably. Under 18 U.S.C. § 1956(a)(2)(A), it is an offense for anyone to bring any money—tainted or untainted—into the United States for the purpose of using it to commit any specified unlawful activity. That's not new. What is new is that the

Patriot Act greatly expanded the list of specified unlawful activities to include approximately 47 offenses generally associated with terrorism, such as assassination, attack with biological weapons, or sabotage of a nuclear facility. The complete list is in 18 U.S.C. § 2332b(g)(5)(B), which has been incorporated into the RICO statute (18 U.S.C. § 1961(1)), which in turn is incorporated into the list of specified unlawful activities. *See* 18 U.S.C. § 1956(c)(7)(A).

So here's where this new authority will be used: If someone brings money not derived (as far as it is known) from any criminal offense into the United States with the intent to use it to commit one of the acts of terrorism listed in section 2332b(g)(5)(B), that is a section 1956(a)(2)(A) violation, and the money is immediately subject to civil or criminal forfeiture because it was involved in a money laundering offense.

III. 18 U.S.C. § 1960

The other reverse money laundering statute is found in a newly-enacted subsection of 18 U.S.C. § 1960. Section 1960 was enacted in 1992 to make it a crime to conduct a money transmitting business without a license. It was little used because it was too hard to prove that a defendant knew that operating without a license was a crime. The Patriot Act amended section 1960 to allow the prosecution of a money remitter in three situations:

- When he or she operates without a license, whether he or she knows that doing so is a crime or not;
- When he or she operates in violation of the Treasury regulations on money transmitters; and
- When he or she transfers money knowing that the funds being transmitted are derived from a criminal offense or are intended to be used for an unlawful purpose.

Note that the third alternative does not require proof that the business was unlicensed. Someone who sends money for a living, knowing it came from a criminal act *or* that it is intended for a future criminal act, is guilty of an offense under section 1960.

Note also the conjunction "or." If the money remitter is sending money that he or she knows is intended to be used to commit a criminal act, he or she does not have to know—indeed, it is unnecessary to prove—that the money was derived from an unlawful source. The act of sending clean money with the intent to commit any unlawful act is sufficient. This is obviously a better law enforcement tool than, say, section 1956, the general money laundering statute, because section 1956 requires proof that the money is dirty *and* that the launderer intends to use it to commit another unlawful act. *See* 18 U.S.C. § 1956(a)(1)(A)(i).

Moreover, the Patriot Act provides forfeiture authority for section 1960 violations. *See* 18 U.S.C. § 981(a)(1)(A). Money being transmitted for an unlawful purpose is subject to forfeiture as property involved in the section 1960 offense. The only problem is that section 1960 only applies to persons in the business of being money remitters. What is really needed is a domestic counterpart to section 1956(a)(2)(A) so that the Government can prosecute anyone engaged in reverse money laundering in the United States whether he or she is a money remitter or not, and whether the money crosses an international border or not. It appears that right now only the State of Florida has such a domestic reverse money laundering statute.

IV. 18 U.S.C. § 981(k)

Finally, there is one other new tool relating to asset forfeiture in the Patriot Act that is worth mentioning. Historically, it has been very difficult for the United States to recover forfeitable property that has been deposited into a foreign bank. The federal courts have jurisdiction to enter forfeiture orders against funds in foreign banks if the act giving rise to the forfeiture occurred in the United States (28 U.S.C. § 1355(b)), but the forfeiture still requires the cooperation of the foreign government. Sometimes that cooperation is forthcoming, and sometimes it is not.

Congress addressed this in the Patriot Act by enacting a new provision at 18 U.S.C. § 981(k). Under that statute, if the Government can show that forfeitable property was deposited into an account at a foreign bank, the Government can now recover the property by filing a civil

forfeiture action against the equivalent amount of money that is found in any correspondent account of the foreign bank that is located in the United States. It is not necessary to trace the money in the correspondent account to the foreign deposit; nor does the foreign bank have standing to object to the forfeiture action. Only the customer who made the deposit of the forfeitable funds into the foreign bank has standing to contest the forfeiture.

The theory is that when the U.S. forfeiture action results in the forfeiture of a given sum of money from the correspondent account of the foreign bank, the bank will then debit the customer's account abroad, leaving the bank in a wash situation, and depriving the foreign customer of the funds that have been forfeited to the United States. This solves the problems that occur when a foreign bank objects to the forfeiture of funds in its correspondent account, claiming that the money belongs to the bank, not its customer, and raising the innocent owner defense. Because this will be controversial, however, forfeitures under section 981(k) require approval from the Department of Justice.❖

ABOUT THE AUTHOR

❑**Stefan D. Cassella** is the Deputy Chief of the Asset Forfeiture and Money Laundering Section (AFMLS). He has been a prosecutor since 1979. He came to the Department of Justice in 1985 and has been involved in forfeiture and money laundering issues since 1989. He handles civil and criminal forfeiture cases, lectures at training conferences on many aspects of money laundering and forfeiture law, and is responsible for legal advice, policy, and legislative issues for the Department. He handled the criminal forfeiture of the assets of Bank of Credit and Commerce International, for which he received the John Marshall Award. He has published four law review articles on forfeiture and is the editor of *Quick Release*, the Department's forfeiture newsletter. From 1978-89, he served as Senior Counsel to the United States Senate Judiciary Committee, working directly for the committee Chairman, Senator Joseph Biden, Jr.✠

This article is an edited version of a presentation made by the author at the symposium on "Financial Aspects of the War on Terror" at Georgetown University Law Center on March 18, 2002.

International Terrorism, the Internet, and the USA PATRIOT Act

Leonard Bailey
Computer Crimes and Intellectual Property Section
Department of Justice

I. Introduction

On December 21, 1989, an explosion brought down a New York-bound 747 Jumbo Jet over Lockerbie, Scotland, killing 259 passengers (189 of which were U.S. citizens) and 11 people on the ground. The downing of Pam Am Flight 103 was, until then, the largest mass killing of U.S. citizens in a single terrorist event. It prompted Congress to pass the Antiterrorism Act of 1990 and the Department of Justice to create the Terrorism and Violent Crime Section in the Criminal Division. Unfortunately, it also ushered in a new era of lethal terrorist attacks against U.S. citizens, government workers, and military personnel, that were a harbinger to the tragic terrorist attacks of September 11th.

Like the bombing of Pan Am 103, the September 11 terrorist attacks have resulted in the passage of new legislation intended to better equip law enforcement to combat terrorism. Unlike the 1990 legislation, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act augmented the government's ability to use electronic surveillance techniques (such as wiretaps, pen registers, and trap and trace devices) to interdict terrorism. Many of these USA PATRIOT Act amendments were intended to updated federal statutes to improve the government's capacity to combat terrorism in the electronic age.

II. How terrorists use computers and the Internet

During the last decade, computers have become increasingly commonplace in our society. According to a recent U.S. Commerce Department report (*A Nation Online: How Americans Are Expanding Their Use Of The Internet*, February 2002) the number of U.S. households with a computer increased from 24.1 percent in 1994 to 56.5 percent in 2001. Just as significant is the fact that most of those computers are being used to access the Internet. The same Commerce Department report found that over half of U.S. households have Internet-access. The Internet has permeated all facets of our society. We have become dependent on it for a broad array of purposes, from entertainment to business to academic research.

Unfortunately, the increase in Internet usage in our society has also been accompanied by a concomitant increase in use of the Internet to commit and facilitate crime. During the last several years, there has been a precipitous increase in the commission of crimes related to the Internet. The Internet is being used to commit conventional crimes such as fraud, extortion, and theft. It is also being used to facilitate less common crimes, such as terrorism. Below is a brief discussion of the purposes for which terrorists are exploiting computers and the Internet.

A. Proselytizing

The Internet's global reach renders it the perfect means of disseminating a message to a large community. A web site posted on a server in Beijing is accessible from Algiers, London, La Paz, or Peoria. The business community has exploited the Intemet's global reach to advertise its wares. So have savvy terrorist organizations.

Some of the most notorious terrorist organizations in the world are using the Internet to proselytize. Several terrorist groups that have been designated by the State Department as "foreign terrorist organizations" because they engage in terrorist activity as defined in Section 212 (a)(3)(B) of the Immigration and Nationality Act (8 U.S.C. §1182), maintain web sites on the Internet: *e.g.*, the Revolutionary Armed Forces of

Colombia; the military wing of the Colombian Communist Party responsible for the 1999 kidnaping and execution of three U.S. Indian rights activists on Venezuelan territory; Hamas which pursues the goal of establishing an Islamic Palestinian state in place of Israel through use of terrorist attacks, including large-scale suicide bombings against Israeli civilian and military targets; the Liberation Tigers of Tamil Eelam, a separatist terrorist group that seeks an independent state in areas in Sri Lanka inhabited by ethnic Tamils and has used conventional, guerrilla, and terror tactics, including some 200 suicide bombings; and Hezbollah, which is a Lebanese group of Shiite militants that opposes the West, seeks to create a Muslim fundamentalist state modeled on Iran, and is a bitter foe of Israel.

If web hosting services in the United States posted such web sites, they would be potential targets for prosecution under 18 U.S.C. §2339B, which renders it unlawful to provide material support to designated terrorist organizations. "Material support" is defined broadly under 18 U.S.C. §2339A(b) to include "expert advice or assistance, ... communications, ..., and other physical assets, except medicine or religious materials." However, the servers that host these web sites are outside the United States, probably beyond the reach of U.S. law notwithstanding the fact that the web sites are accessible from the United States.

B. Intelligence gathering

Increasingly, information is being made available online as a service to the public. While making information accessible via the Internet can be extremely convenient for both those responsible for disseminating information and those seeking to obtain it, it can also pose risks depending on the type of information involved. A review conducted by a computer security firm of information available to the public via the Internet found that an alarming amount of data was available that could be used to stage terrorist attacks on key U.S. assets. The ability to retrieve such information anonymously via the Internet is a boon to individuals who would use it to commit a criminal act such as a terrorist attack.

Indeed, searches performed on the residences of the perpetrators of the September 11 terrorist attacks revealed that the terrorists used public sources to gather intelligence on various potential targets for terrorist attacks. Similar information was attainable via the Internet, prompting the FBI to disseminate an advisory in February 2002, regarding possible attempts by terrorists to use U.S. municipal and state web sites to obtain information on local energy infrastructures, water reservoirs, dams, highly enriched uranium storage sites, and nuclear and gas facilities.

C. Communicating

For many in the United States, e-mail is among their primary modes of communication, second only to the telephone and perhaps conventional mail. If one has reliable access to the Internet, communicating via e-mail has a host of obvious advantages, especially for purposes of international communications: a message can be transmitted almost instantaneously anywhere in the world via e-mail; sending an e-mail to distant countries is far cheaper than conventional mail; e-mail may be more reliable than some countries' domestic postal services; most e-mail can now be used to transmit photos, audio, and video files; and some web-based e-mail accounts are accessible from anywhere on the planet that has Internet access.

E-mail can be sent virtually anonymously and be difficult to trace, especially in regard to international communications. These characteristics of e-mail render it the ideal means for international terrorist groups to communicate with cell members in other countries. Free web-based e-mail accounts like Hotmail, which do not authenticate customer information, have increasingly been used in relation to criminal activity, including terrorism. Indeed, there are indications that international terrorists have already discovered the utility of e-mail as a mode of communication. Many of the nineteen hijackers maintained e-mail accounts. Furthermore, during recent terrorists incidents, terrorists have sent messages to the public and the news media through the Internet. For example, Al Hayat, a Pan-Arab daily newspaper published in London, claims to have received and authenticated an e-mail from Taliban leader Mullah Omar urging

the Palestinians to fight on against America and Israel. Furthermore, ransom demands related to the kidnaping and murder of journalist Daniel Pearl were transmitted by his captors via e-mail.

D. Fundraising

While most charities have laudable goals, some serve as fronts for terrorist organizations. Such charities are perceived by innocent donors to be legitimate. However, these charities typically use fraudulent representations to lure donors into contributing and do not disclose all the purposes for which the donated money is used. Donated funds can be converted by terrorist organizations to plan future terrorist acts, recruit persons to carry out attacks, and support families of terrorists injured or killed. On December 4, 2001, acting under the authority of Executive Order 13224 (Blocking Terrorist Property), the Administration froze the assets of three charities because they were Hamas-controlled organizations that finance terror.

Some of these charities also operate web sites on the Internet that collect funds. In May 2002, the Department alleged that Benevolence International Fund had links to al-Qaeda. Specifically, the Department charged that al Qaeda leader Usama bin Laden used Benevolence International's ten offices worldwide to transfer money to al Qaeda associates. Al-Qaeda members would withdraw funds that were purportedly sent to build schools or provide food for the poor from bank accounts held by the charity, providing a legitimate cover for the movement of funds that financed terrorism. The Benevolence Foundation maintained a web site that permitted contributions online through credit cards or electronic banking systems. It even permitted contributors to make monthly contributions that could be auto-debited to their credit card or bank account on an appointed date.

As discussed above, providing material support to an international terrorist organization (*i.e.*, an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act) is a violation of §2339B. Currently, the State Department has designated twenty-eight organizations as "international terrorist organizations."

III. The USA PATRIOT Act and terrorism investigations related to the Internet

The USA PATRIOT Act amended immigration, money laundering, and anti-terrorism statutes. It also altered statutes governing the interception and tracking of electronic communications in order to improve the government's anti-terrorism capabilities. For purposes of investigating terrorism and terrorism-related activities facilitated by computers, the amendments to statutes governing the tracking and interception of electronic communications were particularly important. Many of them were drafted before the advent of the Internet. Consequently, they did not adequately address some of the issues that arise when applying these statutes to such new technology. As discussed below, the USA PATRIOT Act amendments have vastly improved law enforcement's ability to collect electronic evidence and will undoubtedly assist law enforcement to wage the "War on Terrorism."

A. Using the Pen Register/Trap and Trace Statute to identify a subscriber or user

The pen register and trap and trace statute (the "pen/trap" statute) governs the prospective collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone. Since the telephone was the primary means of communicating electronically in 1986 when the pen/trap statute was drafted, the statute was written using telephone-specific language referring to "local and long distance telephone toll billing records," "numbers dialed," and a "telephone line."

Internet communications are now being used like telephonic communications, by terrorists and other criminals, to plan and coordinate their activities. Accordingly, federal prosecutors have, in the last few years, used pen/trap orders to obtain Internet Protocol (IP) addresses for computers that access e-mail accounts related to criminal activity. IP addresses, much like telephone numbers, are unique numeric identifiers assigned to a computer while it is connected to the Internet. It is possible to use an IP address to determine the location of a computer from which

an e-mail account was accessed, just like a telephone number can be traced to a particular residence.

While the use of the pen/trap statute to obtain IP addresses was relatively common before passage of the USA PATRIOT Act, no federal district or appellate court had explicitly ruled on its lawfulness. The USA PATRIOT Act amended the pen/trap statute to make it expressly apply to Internet communications. For example, the amended definition of a pen register under section 3127 permits installation of pen register and trap and trace devices that obtain all "dialing, routing, addressing, and signaling information" used in the processing and transmitting of wire and electronic communications. This includes IP addresses, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the *content* of a communication, such as words in the "subject line" or the body of an e-mail. Interception of content requires a Title III order.

The USA PATRIOT Act also amended federal law to give trap/trace orders nationwide effect. Previously a USAO seeking to obtain pen/trap authority would be required to obtain an order from the jurisdiction where the pen/trap device was installed, which could be a distant district where the Internet service provider's (ISP) servers were located. Under the USA PATRIOT Act amendments, courts are now permitted to authorize the installation and use of pen/trap devices in other districts. Thus, for example, if a terrorism or other criminal investigation based in Virginia uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order.

B. Identifying customers with subpoenaed information

Under 18 U.S.C. 2703(c)(1)(C), the government, using a subpoena, can obtain "basic subscriber information" for an Internet account. Prior to passage of the USA PATRIOT Act, basic subscriber information included name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber. Unfortunately, this was sometimes not sufficient to actually identify an account subscriber because a user may register with an ISP using a false name and address. A terrorist or other criminal would be particularly likely to engage in such obfuscation.

The USA PATRIOT Act expanded the information that could be obtained with a subpoena to identify an account subscriber under section 2703(c)(1)(C). Subscriber information now includes information about the credit card or bank account used to pay for an account. Such information cannot be falsified if that card or account were actually used to pay for Internet service. Thus, information about payments may be an essential means of determining the true identity of someone seeking to conceal their identity. This information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users' biographical information. The USA PATRIOT amendments also provide for disclosure of "telephone connection information," "temporarily assigned network address," and "records of session times and durations" with a subpoena. Such information can also furnish fertile leads to help identify a customer and valuable evidence of identity at trial.

C. Life and limb disclosure provision

Before passage of the USA PATRIOT Act, ISPs were only allowed to voluntarily disclose stored customer content under narrow circumstances. For example, 18 USC §2702(b)(5) permitted voluntary disclosure of customer content to protect the ISP's rights and property. None of the exceptions allowed disclosure in emergency circumstances. In the event that an ISP independently learned that one of its customers was imminently planning to commit a terrorist attack, none of the voluntary disclosure provisions clearly provided the ISP with authority to disclose that information to law enforcement. Section 2702(b)(6) permitted disclosure of information that appeared to pertain to the commission of a crime, but only if that information was "inadvertently obtained" by the ISP. If an ISP disclosed information in violation of section 2702, it could have been sued civilly.

The USA PATRIOT Act amended subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications to uncover imminent dangers. However, an ISP may now disclose a customer's communications if it discovers communications that it reasonably believes constitute an emergency that requires disclosure without delay involving immediate danger of death or serious physical injury to any person.

D. Section 220 nationwide search warrants for e-mail

Under section 2703(a) the government is required to use a search warrant to compel a provider to disclose unopened e-mail less than six months old. But Rule 41 of the Federal Rules of Criminal Procedure requires that the "property" to be obtained be "within the district" of the issuing court. Accordingly, some courts have declined to issue section 2703(a) warrants for e-mail located in other districts. Unfortunately, this refusal has placed an enormous administrative burden on those districts in which major ISPs are located, such as the Eastern District of Virginia and the Northern District of California, even though these districts may have no relationship with the criminal acts under investigation. In addition, requiring investigators to obtain warrants in distant jurisdictions has slowed time-sensitive investigations. In the aftermath of September 11, the U.S. Attorneys' Offices for the Eastern District of Virginia and the Northern District of California were swamped with requests for search warrants for e-mail accounts related to the terrorist attacks.

The USA PATRIOT Act amended section 2703(a) (and parallel provisions elsewhere in section 2703) to allow investigators to use section 2703(a) warrants to compel records outside of the district in which the court is located, just as they use federal grand jury subpoenas and orders under section 2703(d). This change enables courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of agents, prosecutors, and judges, in the districts where major ISPs are located.

IV. Conclusion

Congress amended the authorities discussed above specifically to bolster the government's ability to combat terrorism. These amendments have already proven helpful and have been used in the PENTTBOMB investigation of the September 11 terrorists attacks. However, these USA PATRIOT Act amendments have not exclusively benefitted terrorism investigations. Indeed, investigations of all manner of criminal conduct with a nexus to the Internet have benefitted from these amendments.

Because of concerns over the expansion of law enforcement's authorities, Congress made many of the USA PATRIOT Act's amendments (such as the emergency voluntary provider disclosure and nationwide search warrant provisions) "sunset" on December 31, 2005. If they are not re-authorized by Congress, they will be automatically repealed. Congress' decision to re-authorize them will likely rest upon whether they have proven effective for law enforcement and whether they have been abused. The Criminal Division's Computer Crime and Intellectual Property Section is prepared to assist any U.S. Attorney's Office with questions about these amendments and their application.❖

ABOUT THE AUTHOR

❑**Leonard Bailey** is a trial attorney in the Computer Crime and Intellectual Property Section. He has been at the Department of Justice since 1991 and has worked as a trial attorney in the Terrorism and Violent Crime Section and as Special Counsel to the Department of Justice's Inspector General.✠

Immigration and Naturalization Service's Role in Fighting Terrorism

Daryl F. Bloom, Assistant District Counsel
United States Department of Justice
Immigration and Naturalization Service
Philadelphia District/York Field Office

In the wake of the September 11, 2001 attacks on America, I, along with countless others, was dispatched to Washington, D.C., to staff the Federal Bureau of Investigation, George Bush Strategic Information and Operations Center (SIOC). The SIOC was the heart of the Pentagon/Twin Towers Bombing (PENTTBOM) investigation. The SIOC is a Secure Compartmental Information Facility (SCIF) located on the fifth floor of the FBI building. Gaining access to the SIOC requires a special compartmentalized, as well as a top-secret, clearance. The main room is a large open space surrounded by numerous smaller breakout rooms and offices. There are no windows in any of the rooms. The room was designed to divide into many sections and is capable of handling several events at one time. In January, the SIOC was sectioned off and used to prepare for the Super Bowl and the Winter Olympics.

During the PENTTBOM investigation, virtually every United States federal law enforcement agency was represented in the room. Military personnel, law enforcement agents, attorneys, and support staff, occupied every inch of the forty thousand square foot space. In some instances two individuals, on the same shift, shared a desk despite the fact that the room was equipped with more than one hundred desks, computers, and monitors and contained a maze of computer and telephone wires. Dozens of fax machines occupied almost an entire wall. CNN Headline News, C-SPAN, and CNBC could be viewed on two, five by fifteen foot video screens, which provided up-to-date news reports. In addition to the charts and diagrams, dozens of enlarged photographs of the hijackers and the damage from the September 11 attack were displayed throughout the room as a constant reminder of the seriousness of the task.

The Director of the FBI, Robert Mueller, and Attorney General John Ashcroft frequently passed through the room providing greetings and encouragement to the staff. In addition, the room was often buzzing with official visitors, including President Bush, Vice President Cheney, the Director of Homeland Security, Tom Ridge, and numerous high-ranking military officials, Senators, and Congressman. The President, Vice President, and Director of Homeland Security thanked us for our dedication and hard work and assured us that the responsible parties would be brought to justice.

The dedication that we felt in the room was an extraordinary testament to the task force's commitment to public service. Even though many members were away from their homes and families for significant periods of time and living in hotels, they were honored to serve. Everyone in the room was helpful to the fullest extent possible. In addition, the support of the public was overwhelming. For example, several businesses and organizations donated snacks for the personnel who were working during late night and early morning hours. Elementary school students sent a thank-you note, which was displayed in a break room and encompassed almost an entire wall. Some of the local restaurants extended their hours to stay open for the personnel working at the FBI headquarters, despite the fact that tourism was down, and they would not likely have other customers during those hours. An FBI agent's parents donated a full dinner, rivaling most families' Thanksgiving Day dinners, for the dozens of employees at the SIOC one Sunday afternoon.

I represented the Immigration and Naturalization Service (INS) at the SIOC, answering legal questions related to immigration arrests, detentions, searches, and other evidentiary matters. Originally, INS attorneys from Boston,

Pennsylvania, New Jersey, and Washington, D.C., were assigned to the SIOC in twelve-hour shifts, twenty-four hours a day and seven days a week. After two weeks, the shifts were reduced to eight hours and weekend shifts were eliminated. The reality was twelve-hour business days and only a few hours on the weekends. The dedication and energy felt throughout the room eased the long hours spent at the SIOC, and the hectic pace made the time pass quickly. The field attorneys with which I dealt and the staff at the National Security Law Unit at the INS Headquarters and FBI Headquarters greatly assisted with the heavy caseload.

All national security and terrorist-related cases are assigned to special, designated attorneys in the district and field offices, who receive special training in the handling of these types of cases. The appropriate Office of the Regional Counsel for the particular region and INS Headquarters' Office of the General Counsel monitor the cases. A staff attorney in the office of the General Counsel will serve as the liaison between the CIA, FBI, Department of State, the National Security Agency, and other federal agencies.

Although tremendous progress in the investigation and a large number of immigration arrests were being made, the task force needed to address the hundreds of immigration cases related to the investigation. A unique working group was quickly established to deal with the aliens, defined as any person who is not a citizen or national of the United States, linked to the attack or contacted due to a PENTTBOM lead.

The working group consists of representatives from the INS, FBI, Office of Immigration Litigation (OIL), Terrorism and Violent Crime Section (TVCS) and the Deputy Attorney General's Office. The group's primary responsibility is to liaise with the FBI, INS, and United States Attorneys' offices in the field and at the headquarters offices, to facilitate information and evidence sharing. The group also coordinates the cases to ensure that those aliens linked with the attack are not released until they can be criminally prosecuted or removed from the United States. The cooperation between these agencies is unparalleled.

Once an individual is encountered, based on a PENTTBOM lead, INS agents initiate an investigation to determine his or her immigration status. Such cases are generated internally by the INS, subject to concurrence by the FBI, or generated by a referral from the FBI to the INS. The TVCS and the United States Attorney's Office for the Eastern District of Virginia and Southern District of New York determine if material witness warrants should be issued based on information they may provide to a grand jury. Criminal charges are prepared by the United States Attorney's office in the controlling district, in the event that an alien might be placed in immigration removal proceedings and ordered released on an immigration bond by an Immigration Judge. Many of the individuals arrested by the INS based on PENTTBOM leads were eligible for release on bond because they were not removable based on a terrorist ground of removal. The Immigration Judge may not redetermine the custody conditions with respect to an alien who has been charged with a terrorism ground of removal.

The authority of the Immigration and Nationality Act allows INS agents to arrest and detain aliens on immigration matters while the investigation continues, with the goal of bringing those responsible for assisting in the September 11 attack to justice. Although some of the individuals could not be criminally prosecuted for the attack, they could be removed from the United States, which helps neutralize or eliminate possible future threats. The law enforcement community and others quickly became aware that the INS is a valuable asset to law enforcement.

Many of the people working outside of the INS are not familiar with the ever-evolving and complex immigration statutes and regulations that may be helpful. The Immigration and Nationality Act is a labyrinth of laws, exceptions, and waivers. Therefore, when asked to write this article about my experience at the SIOC, I determined that it was a perfect opportunity to provide a basic guide to the INS's handling of terrorist cases and immigration laws in general.

The INS, through its designated employees, has expanded search powers, which proves helpful in the investigation. Authorized INS

officers and employees have the power to conduct a search, without a warrant, of any person, and of the personal effects in the possession of any person, seeking admission to the United States. The officer must have reasonable cause to suspect that grounds exist, which would be disclosed by the search, for denial of admission to the United States under the INA. Authorized INS officers have the power to board and search for aliens on any vessel within the territorial waters of the United States, and any railway car, aircraft, conveyance, or vehicle within a reasonable distance from any external boundary of the United States.

INS officers also have extended interrogation and arrest authority. Authorized officers and employees of the INS have the power, without warrant, to interrogate any alien or person believed to be an alien, as to his or her right to be, or to remain, in the United States. The officers and employees also have the power to arrest any alien in the United States if there is reason to believe that the alien is in the United States in violation of law and is likely to escape before a warrant can be obtained for his arrest.

The INS must make a determination within forty-eight hours of arrest, unless voluntary departure is granted, whether the alien will be continued in custody, released on bond or recognizance, and whether to issue an NTA. An exception to the forty-eight-hour rule occurs in the event of emergency or other extraordinary circumstances, in which case the INS must make such determinations within an additional, reasonable period of time. This exception was created in response to the terrorist attacks. In many cases, obtaining the necessary information within forty-eight hours is nearly impossible, and the country was in a President-declared state of emergency. The difficulty in determining identity is compounded by the fact that documents from many countries have poor security features. In addition, a vast network exists of false documentation, passports, driver's licenses, and birth certificates. Determining identity within forty-eight hours in every case is virtually impossible.

If appropriate, the INS places the individuals in removal proceedings under Title II of the Immigration and Nationality Act (INA). Removal proceedings are initiated by the issuance and filing of a charging document called a Notice to Appear (NTA), which sets forth the factual and legal basis for attempting to remove the alien from the United States.

Individuals, placed in removal proceedings, are either charged with inadmissibility or deportability grounds of removal. An alien is inadmissible if he or she is attempting to enter the United States, or is present in the United States, without being lawfully admitted or paroled. An alien is deportable if he was lawfully admitted into the United States but has failed to maintain his immigration status, overstayed his visa, or engaged in qualifying unlawful conduct. Most federal and state convictions can form the basis of a charge of removal and many may also bar the individual from various waivers and forms of relief, which would allow the individual to lawfully remain in the United States, notwithstanding certain criminal convictions.

Engaging in terrorism renders an alien subject to removal. Filing a terrorism charge of removal requires the approval of the INS HQ National Security Law Unit under the Office of the General Counsel and the National Security Unit under Field Operations. A terrorism charge can be filed for any alien that engages in, is likely to engage in, or has engaged in, terrorist activity; incited terrorist activity; is a representative of a foreign terrorist organization; or, is a member of a foreign terrorist organization which the alien knows or should have known is a terrorist organization. Terrorist activity is defined in INA section 212(a)(3)(B)(ii) and includes:

- hijacking or sabotage of any conveyance;
- seizing or detaining and threatening to kill, injure, or continuing to detain another individual in order to compel a third person or government to do or abstain from doing some act;
- a violent attack upon an internationally protected person;
- an assassination;
- and, the use of any biological agent, chemical agent, nuclear weapon, explosive device or

firearm with the intent to endanger the safety of others or cause substantial damage to property.

Terrorist activity also includes any threat, attempt or conspiracy to do any of the foregoing.

"Engage in terrorist activity" means to commit, as an individual or as a member of an organization, an act of terrorist activity or an act that provides material support to any individual, organization or government in conducting a terrorist activity. "Engage in terrorist activity" is defined in INA section 212(a)(3)(B)(iii) and includes:

- the preparation or planning of a terrorist activity;
- the gathering of information on potential targets for terrorist activity;
- the providing of any material support (including a safe house, transportation, communications, funds, false documentation, weapons, explosives, or training) to any individual the actor knows, or has reason to believe, has committed or plans to commit a terrorist activity;
- the soliciting of funds or other things of value for terrorist activity or a terrorist organization and;
- the solicitation of any individual for membership in a terrorist organization or to engage in a terrorist activity.

The Department of State publishes a list of entities that are designated as foreign terrorist organizations. The list also includes other names the group has used or is known by, abbreviations to the name of the group and acronyms. In order for the entity to be subject to designation as a "foreign terrorist organization" under the Anti-Terrorism and Effective Death Penalty Act (AEDPA), the Secretary of State must find that an entity is a foreign organization engaging in terrorist activities that threaten the national security of the United States. Nonetheless, it is important to note that an alien may still be a terrorist even if he or she is not affiliated with any organization included in the list of terrorist organizations, and a group can be a terrorist organization even if not so designated by the Secretary of State. Thus, an alien, who is a member of a nondesignated terrorist organization, or who is otherwise believed to have engaged or is likely to engage in terrorist activity, may still be inadmissible or deportable from the United States.

After a decision is made to proceed under Title II removal proceedings and to issue an NTA, the charging document is then filed with the Immigration Court. The Immigration Court is an administrative body under the authority of the Attorney General of the United States. Immigration Courts are trial level tribunals, which determine whether an individual is in the United States in violation of United States law and, if so, whether there is any waiver or benefit available to the individual that would allow them to remain in the United States lawfully. An INS Assistant District Counsel represents the INS at the hearings. Aliens have the right to be represented by counsel, but at no expense to the government.

In removal proceedings, the alien must show the time, place, and manner of his or her entry into the United States. The INS must establish the individual's alienage and removability by clear, convincing, and unequivocal evidence. The burden then shifts to the respondent to establish nonremovability. When an alien makes an application for a visa or other entry document, he or she must prove that he or she is eligible to receive such a visa or document, and that he or she is not inadmissible under any provision of the Immigration and Nationality Act.

The federal rules of evidence do not apply in immigration removal proceedings. To be admissible, evidence need only be relevant, probative, and its use must be fundamentally fair. Hearsay evidence has no per se objection. An alien has the right to examine the evidence against him and to cross-examine witnesses presented by the government. However, an exception exists with respect to classified material presented by the INS to rebut applications for relief or support the respondent's inadmissibility to the United States. The 1996 antiterrorism bill that followed the Oklahoma City bombing and first World Trade Center bombing specifically authorized the use of classified evidence in some immigration proceedings. However, the use of classified

evidence in immigration proceedings has existed since at least 1956.

The Service has the ability to present classified evidence in an *in camera* and *ex parte* proceeding. The use of classified evidence requires the approval of INS Headquarters and the Deputy Attorney General's office. Therefore, the request should be made as soon as possible. Statutory provisions authorizing the use of classified evidence appear primarily in INA sections 235(c) and 240(b) No provision allows for the review or confrontation by the alien (or his representative). The respondent is only provided access to an unclassified summary of the material, and then only if the agency providing the material deems that it can safely be provided. Removal proceedings are civil in nature. Therefore, the procedural safeguards prescribed for criminal cases are not applicable. In a federal civil case, plaintiffs have no right to classified information.

The Supreme Court has affirmed the use of classified information in Title II proceedings where the disclosure of such information would be prejudicial to the public interest, safety, or security, of the United States. However, classified information should only be used when absolutely necessary in order to protect the information from unnecessary disclosure. Other ways to obtain the same information through unclassified means or sources should be used when available. The reliability of the evidence is always questioned and must be addressed at the forefront.

Some federal courts have ruled against the government in "secret evidence" cases. In one of the first decisions concerning the use of classified evidence under the 1996 legislation, a federal district court ruled that the use of classified information against an alien accused of having links with terrorists was unconstitutional and violated the alien's right to due process. *Kiareldeen v. Reno*, 71 F.Supp. 2d 402 (D. N.J. 1999).

The plain language of the Act bars the use of classified evidence to establish deportability, as opposed to inadmissibility, in removal proceedings. Classified evidence may be used only in opposition to the alien's admission or once deportability is established. The Act provides for the use of classified evidence in opposition to applications for discretionary relief. If the government wishes to use classified evidence to establish deportability, it must invoke the Title V procedures through the Alien Terrorist Removal Court (ATRC).

The ATRC was established to adjudicate special removal proceedings where the INS seeks to remove an alien terrorist under a terrorism charge. The ATRC is comprised of five United States District Court judges appointed by the Chief Justice of the United States Supreme Court. A single judge presides over the individual special removal proceeding. Before this court, the government has the burden of establishing, by a preponderance of the evidence, that the alien is a terrorist. The sole issue in such a proceeding is whether the alien is removable. The alien is entitled to legal representation at government expense if he or she is unable to afford private counsel. Although Title V of the Immigration and Nationality Act provides these special courts, it has generally been found that the public interest is better served by charging such aliens in ordinary expulsion proceedings under Title II of the INA.

A common fallacy is that the INS can detain aliens based solely on their illegal presence in the United States. Although aliens arriving in the United States are not eligible for bond, there must be a justification for the detention of aliens already present in the United States. This requires some individualized inquiry. Mandatory custody provisions exist for some aliens who are present in the United States and removable for terrorism and certain criminal grounds. The United States Supreme Court holds that the Due Process Clause applies to all persons within the United States, including aliens, whether their presence in the United States is lawful, unlawful, temporary, or permanent. Some federal district courts have held that the mandatory custody provisions contained in the Immigration and Nationality Act are unconstitutional. *Patel v. Zemski*, 275 F.3d 299 (3d Cir. 2001) (holding that § 236(c) of the INA improperly deprived the subject respondent his constitutional due process rights).

The INS makes the initial custody determination, either setting a bond amount or finding that the alien is a flight risk and/or danger to the community and holding that bond be

denied. If the alien remains in INS custody, he may apply to the Immigration Judge for a change in his custody status at any time before his removal order becomes administratively final. Immigration judges do not have the authority to conduct bond redeterminations for arriving aliens, which includes aliens paroled into the United States, certain criminal aliens, and aliens charged with a terrorism ground of removal. Bond decisions are subject to appeal to the Board of Immigration Appeals, the appellate body for the Immigration Court. The INS has the ability to stay the bond decision of an Immigration Judge until an appellate decision can be rendered where the INS initially set a bond at $10,000 or more.

The Immigration Judge's decision on bond need only be based upon "information" provided by the alien or the INS, rather than the traditional requirement of evidence. The INS attorney may simply narrate relevant factors without witnesses or introducing documentary evidence.

One purpose of the working group was to gather evidence that could be used in the bond and removal hearing. Because of the significance of the PENTTBOM cases, affidavits were prepared for the hearings and signed by senior FBI agents. Although the affidavits were as specific as possible, the group is mindful of revealing too much information that might jeopardize the investigation, disclose a confidential source, or otherwise be detrimental to the case. In addition, the investigation is in the developmental and initial stages. Therefore, it is difficult to obtain all of the facts for the hearings.

The attack on America resulted in several new amendments in the law to combat terrorism. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (2001), was passed in response to the September 11 attacks. The USA Patriot Act expanded the terrorism grounds of inadmissibility in § 212(a)(3)(B) and renders inadmissible:

- a representative of a political, social or other similar group whose endorsement of acts of terrorist activity the Secretary of State has determined undermines United States efforts to reduce or eliminate terrorist activities;
- an individual who has used his or her position of prominence within any country to endorse or espouse terrorist activity, or persuade others to support terrorist activity or a foreign terrorist organization, in a way that the Secretary of State has determined undermines United States efforts to reduce or eliminate terrorist activities; and
- the spouse or child of an alien inadmissible under this section, if the activity that rendered the alien inadmissible occurred within the last five years.

The Patriot Act also expanded the definition of "terrorist activity." Another amendment grants the Attorney General or the Commissioner of the INS authority to certify cases of aliens if they are described in national security or terrorism grounds of removal and allows them to be held for up to seven days before charging the alien criminally or placing them in removal proceedings. Effective September 17, 2001, the period of time in which the INS must make custody and charging determinations was extended from twenty-four hours after arrest to forty-eight hours, unless voluntary departure is granted, or a "reasonable period of time" in the event of emergency or other extraordinary circumstances. This open-ended provision was implemented in order to provide more time to establish identity, check domestic, foreign and international databases, and liaise with law enforcement in the United States and abroad. The amendments are a great addition to the counter-terrorism measures already in place.

However, the best way to combat terrorist activity is intelligence. A battle is lost every time a terrorist attack occurs. The object is not simply to arrest and ultimately convict those responsible for the terrorist activity. The object is to stop acts of terrorism before they occur, even if the effort does not result in a conviction. Arresting terrorists disrupts terrorist networks. Therefore, the INS, FBI, and other law enforcement agencies need to continue to coordinate their efforts in the investigation of individuals suspected of terrorist activity.

ABOUT THE AUTHOR

❑**Daryl F. Bloom** has served as an Assistant District Counsel for the Immigration and Naturalization Service for seven years after being hired through the Attorney General's Honors Program. Mr. Bloom is currently a designated "special interest" and terrorist related case attorney for the Philadelphia District and his current duty station is the York Field Office in York, Pennsylvania.✠

Victim-Witness Services in a World Faced with Terrorism

Jennifer Parks-Abbott
Victim-Witness Specialist
United States Attorney's Office
Eastern District of Virginia

I. Introduction

Every American citizen, and many citizens of foreign countries, became crime victims on September 11, 2001, when terrorists struck on American soil. Whether by loss of loved ones, friends, businesses, occupations, or real estate, the victim count is massive. Government agencies have come to the realization that the world has changed and will likely involve more and more terrorists attempts here and abroad, be it by weapons of mass destruction or by biological and chemical weapons. Consequently, many agencies are creating service units to provide immediate assistance to crime victims and witnesses so as to alleviate, as much as possible, the pain and suffering caused by such senseless acts.

Terrorism is premeditated to cause deaths and injuries, which result in an atmosphere of shock and dismay. Recovering from such devastation can take a lifetime. The destruction of life and property causes us to pause and reflect on where we have been and where we are headed in the future. Our priorities with victims and witnesses have become more defined as we have seen firsthand how our humanity, self-sacrifice, compassion, endurance, and unselfishness, can bring about unity and help those who are suffering. This assures them that they are not alone and that immediate help is available for them.

A Decade of Terrorism

Pam Am Flight 103 – December 21, 1988
Airplane explodes over Lockerbie, Scotland.

New York City - February 26, 1993
Massive bombs explode below the World Trade Center.

Tokyo, Japan - March 20, 1995
Terrorists release sarin gases in subway trains.

Oklahoma City - April 19, 1995
Truck bomb explodes at the Alfred P. Murrah Federal Building.

Khobar Tower Bombing – June 25, 1996
Truck carrying bomb explodes outside a U.S. military housing facility.

Kenya and Tanzania - August 7, 1998
U.S. Embassies bombed.

USS Cole – October 12, 2000
Bombing of a U.S. Navy Ship in port at Yemen.

Just days after the September 11 tragedy, women gave birth to children whose fathers were killed in the World Trade Center, the Pentagon, and the Pennsylvania plane crash. Unless one has been in such a situation, knowing the deep pain and grief these women must have gone through during delivery is impossible. These women need the immediate support of victim specialists who can assist them in obtaining the services they require while rebuilding their lives.

Thousands of children were left without one or both parents on that tragic day. These children will need counseling and other services, perhaps for the rest of their lives, as they grow up without a parent or parents. Daily life will constantly remind them of their losses as they participate in school and athletic activities. They will suffer emotionally and psychologically and require adequate services and support systems to let them know that they are not alone.

Following the September 11 attacks, Americans were faced with an anthrax scare. All Americans became crime victims because of feelings of being under siege by the daily delivery of their mail. As if the loss of life and limb in the terrorists attacks was not enough, terrorists claimed several other victims and caused human suffering and death from inhaling anthrax.

Numerous victims of terrorism look to us for support, and we must answer the call. Many victims are merely trying to cope, but some of the problems are too serious for mere coping skills. We must seek out those who will eventually, if they are not already, be faced with post traumatic stress, suffer flashbacks, nightmares, anxiety attacks, anger, upsets, and difficulty sleeping and concentrating. Lives have dramatically changed and will continue to change as the reality of what is happening in America sets in. Our government continuously reminds us that this will probably not be the last time that we will be faced with terrorists acts against American citizens.

II. Coping with the aftermath of terrorism

A critical aspect of the aftermath is dealing with the destruction caused to loved ones. Out of the ashes of the World Trade Center, the Pentagon, and the Pennsylvania crash, came mangled bodies and, in many cases, no body will ever be found. Therefore, families are unable to have funeral services and have grave sites to visit. For many, these absences prevent them from experiencing closure. This fact alone has very devastating effects on the families. Also hard hit will be the survivors who will constantly ask themselves why they were spared when so many of their friends and coworkers were not.

Victim-Witness Specialists are able to assist these individuals with the help of other government agencies. Various offices and units, providing a variety of services, are in place. While we try to understand the depths of the despair that crime victims face, we will also attempt to help them through the process by assuring them that we can ease their pain and suffering and provide them with information needed to rebuild and carry on with their lives. In 2001, the Office for Victims of Crime (OVC), under the umbrella of the Department of Justice, prepared a handbook, titled *OVC Handbook for Coping After Terrorism; A Guide to Healing and Recovery*, which is very useful. Victim-Witness Specialists should make this publication a part of the caring package that they provide to crime victims. This handbook provides valuable information to victims which will help their recovery efforts.

Practical Coping Ideas

- **"Give yourself time to get through the most hectic times and to adjust before making decisions that will affect the rest of your life." OVC HANDBOOK FOR COPING AFTER TERRORISM 6.**
- **Discuss the experience with a counselor, clergy member, friend, family member, or other survivors about what happened. Sharing your experience over and over can be helpful. *See* OVC HANDBOOK FOR COPING AFTER TERRORISM 7.**
- **Ask questions. Begin to restore order in your world by reestablishing old routines. *See* OVC HANDBOOK FOR COPING AFTER TERRORISM 7.**

- **Avoid using alcohol and other drugs. They may temporarily block pain, but will not help with the healing. "You have to experience your feelings and look clearly at your life to recover from tragedy." OVC HANDBOOK FOR COPING AFTER TERRORISM 7.**

The victims and witnesses of the September 11 tragedy, and all crime victims, must be given every opportunity to express their feelings whenever the need arises. To that end, Victim-Witness Specialists should work with local, state, and federal agencies to set up support groups, psychological services, and other means of support so that the victims do not feel that they are alone in their grief. All victims of crimes need to feel secure and safe, knowing that they can receive emotional and physical assistance.

The way victims cope may depend on the information provided by Victim-Witness Specialists and the manner in which they are treated during the investigation and prosecution stages of the case. Victims should always feel that they have support and compassion. The goal should always be to restore some type of security and control to their lives. This instills trust and cooperation because victims realize that we are looking out for their best interest. Victim-Witness Assistants should also realize the full extent of victims' physical and emotional needs, making such determinations on a victim-by-victim basis, and not attempt to group all victims' needs into one category.

III. Services offered to victims and witnesses in the face of terrorism

Terrorist activity brings about great loss of life and is a major concern of the United States and other nations. Those who can provide comfort and hope to victims and witnesses rely on the service providers to give them help and direction. Victim-Witness Assistants provide:

- a listening ear;
- needed services, such as referrals to local, state and federal agencies;
- notification of court proceedings;
- opportunity for victims to speak to the court by way of victim impact statements.

Victim-Witness personnel are trained to respond quickly to the needs of crime victims. Following terrorists attacks, they will become intensely involved in the lives of those affected. The victims of the World Trade Center and Pentagon attacks are not only those who had relatives killed or injured, but also those who had the task of rescuing, recovering, identifying, and notifying family members. These individuals, will come to suffer in the aftermath of the rescue and recovery operations, just as the relatives of those who were killed.

The type of terror a victim or witness experiences does not matter as the aftermath is always the same. Victims are faced with shock, numbness, sorrow, grief, fear, guilt, anger, resentment, loneliness, depression, isolation, physical symptoms of distress, panic, the inability to resume normal activities, and often delayed reaction to the terrors. Victim-Witness personnel become invaluable to the well-being of these individuals. First and foremost, the Victim-Witness personnel must gain the trust and confidence of victims by treating all victims with faimess, dignity, and respect. The Specialist also has a responsibility to ensure that the victims are aware of the services available to them. The Victim-Witness Protection Act (VWPA) sets forth services that must be provided to every crime victim.

In many cases, agencies such as the Department of Housing and Urban Development (HUD) have been contacted to assist in providing temporary housing for victims. In one case, a mother of five children, ranging in age from three to twenty-one years, received a long-term prison sentence after entering a plea of guilty to federal drug offenses and agreed to cooperate with federal authorities and testify against co-defendants. Her children, after her arrest, were living with a friend of some of the other co-defendants, thereby making them potential subjects of retribution for the mother's cooperation. After several attempts at finding reasonable housing for the children, the Victim-Witness Specialist requested and received housing assistance from HUD for

semipermanent housing and vouchers. This enabled the children to remain together as a family and continue with their education and afterschool care in familiar surroundings.

Services Provided by Victim Witness Personnel

- **Inform victims where they may receive emergency medical and social services. *See* 42 U.S.C. § 10607(c)(1)(A) (2001).**
- **Inform victims "of any restitution or other relief to which [they] may be entitled," and inform them of the "manner in which such relief may be obtained." 42 U.S.C. § 10607(c)(1)(B).**
- **Inform victims of public and private programs that are available "to provide counseling, treatment, and other support." 42 U.S.C. § 10607(c)(1)(C).**
- **Assist victims in contacting persons who are responsible for providing services and relief. *See* § 42 U.S.C. 10607(c)(1)(D).**
- **Arrange for victims to receive reasonable protection from suspected offenders and persons "acting in concert with or at the behest of the suspected offender[s]." 42 U.S.C. § 10607(c)(2).**

The Department of Health and Human Services (HHS) is another unit that provides much needed mental health services to terrorism victims. Many local and state level agencies also assist in providing services to victims.

Since terrorist crimes often involve large numbers of victims, many agencies and Victim-Witness personnel work together to help the victims make the transition from the agency that is investigating the criminal act to another that has the responsibility to prosecute the case. This effort requires communication and coordination skills on the part of all persons involved. This is a crucial part in making and keeping the victim informed.

New and innovative ways to combat terrorism are emerging. The offices and agencies that provide services to victims and witnesses must be involved in the initial stages of planning and development so that they are able to create and update programs and services that assist victims and witnesses when tragedy occurs. Programs such as the Victim Notification System (VNS) enable victims to receive information regarding upcoming trial proceedings. This system also keeps them informed, on a regular basis, by an automated telephone system.

During the investigation and prosecution of crimes, Victim-Witness personnel are required to provide notice to victims regarding:

(1) the status of the investigation of the crime, to the extent that it will not interfere with the investigation;

(2) the arrest of a suspected offender;

(3) the filing of charges against a suspected offender;

(4) the scheduling of each court proceeding that the witness is either required to attend or is entitled to attend;

(5) the release or detention status of an offender or suspected offender;

(6) the acceptance of a guilty plea or nolo contendere or the rendering of a verdict after trial; and

(7) the sentence imposed on an offender, including the date on which the offender will be eligible for parole. *See* 42 U.S.C. § 10607(c)(3)(A)-(G).

During court proceedings, Victim-Witness Specialists ensure that the victim is provided a waiting area removed from, and out of the sight and hearing of, the defendant and defense witnesses. *See* § 10607(c)(4). After trial, the victim is provided with notice of:

(1) the scheduling of a parole hearing for the offender;

(2) the escape, work release, furlough, or any other form of release from custody of the offender; and

(3) the death of the offender, if the offender dies while in custody. *See* § 10607(c)(5)(A)-(C).

Crime victim compensation is available in all fifty states, the District of Columbia, U.S. Virgin Islands, and Puerto Rico. These funds provide financial assistance, such as lost wages, medical care, and funeral and counseling services if needed, to victims of crime. Out-of-state compensation agencies provide financial aid when all other means are exhausted.

The tragic loss of human life is the most obvious result of terrorism. Terrorism affects all of us by influencing the way we live our daily lives, and by the choices we make when we travel.

Tragedies like those in New York, Pennsylvania, and Northern Virginia have caused us to think about our priorities. Victim-Witness Specialists are responsible for ensuring that victims are given an opportunity to "come back whole" and to receive appropriate services at a time when they most need them. We cannot allow victims of terrorism to be retraumatized.

As we heal from the traumas of September 11, we must recognize the importance of those individuals who sacrifice their lives, their time, and their resources, by observing "National Crime Victims' Rights Week" April 21-27, 2002. This year's theme is "Bringing Honor to Victims of Crime."❖

ABOUT THE AUTHOR

❑**Jennifer Parks-Abbott** is the Victim-Witness Specialist for the United States Attorney's Office, Eastern District of Virginia, Norfolk and Newport News Divisions. She began her government service in September, 1978. She has received numerous awards and recognition from various federal agencies for her services to victims and witnesses. She has provided assistance to federal, state and local agencies, helping them with their victim-witness programs. She has served on various committees with the Executive Office for United States Attorneys LECC/Victims-Witness Unit.✠

Notes

UPCOMING PUBLICATIONS

July, 2002 - Civil

Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' **BULLETIN** to all 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 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 803-544-5158. Your cooperation is appreciated.