**November 2001**
**Volume 49**
**Number 6**

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 Attorney's Bulletin is published pursuant to 28 CFR § 0.22(b)

The United States Attorney's 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 Attorney's Bulletin, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201

**Managing Editor**
Jim Donovan

**Assistant Editor**
Nancy Bowman

**Law Clerk**
Brian Burke

**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

# High Tech and Investment Fraud

**In This Issue**

## In Honor

This issue of the United States Attorneys' Bulletin is dedicated to Michael C. Messer, a senior attorney at the Social Security Administration (SSA). Mr. Messer was appointed a Special Assistant United States Attorney for the Northern District of Illinois on October 10, 2000 as part of SSA's Anti-Fraud Pilot Project, and was detailed to the Criminal Division of the Chicago United States Attorney's Office (USAO). On August 20, 2001, while attending a training conference at the National Advocacy Center (NAC), he was shot and killed in an attempted armed robbery while walking back to the NAC after dinner. Mike was a wonderful attorney and colleague who served his agency, the USAO, and his community with dedication and distinction. He is survived by his wife Susan, and their three children, Elizabeth, Zachary, and Joshua.

# Prosecuting Social Security Fraud: Protecting the Trust Fund for Present and Future Generations

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

**Introduction**

When I first arrived in the United States Attorney's Office in Portland, Oregon in 1997, as a Special Assistant United States Attorney on loan from the Social Security Administration (SSA), my new best friend (AUSA) in the office graciously offered to hand over his Social Security cases to help me get started. I don't recall his exact words, but the phrase "dog cases" comes to mind. He told me repeatedly that prosecuting elderly individuals with limited resources simply had no jury appeal.

Even though the AUSA enjoyed watching a rookie stumble about, he was a patient and thorough mentor. He enjoys reminiscing about how green I was and how he saved my career. I draw pleasure in reminding him just how wrong he was about the jury appeal of Social Security fraud cases. My experience is that Social Security fraud cases have immediate appeal to both a Grand Jury and a trial jury due to immediate name recognition. The Social Security nameplate has distinctive brand appeal – like an Intel processor, IBM computer, or RCA television. Can you name an American who isn't aware what Social Security means to his or her future? Can you name a politician who hasn't uttered the sacred words "Social Security – protect - future"? Two words best describe my own experiences with the jury appeal of Social Security fraud cases: "thief beware." I have yet to meet a Grand Jury or trial jury that has exhibited any tolerance for any Social Security offender, regardless of age, gender, or disability.

So, why are so many of our colleagues afflicted with prosecutorial reticence when faced with an agent bearing a prosecution report describing Social Security fraud? The answer, most likely, is fear of the unknown. The sheer number of benefits programs offered by SSA is enough to discourage some prosecutors, who fear a protracted learning curve just to get up to speed on Social Security laws. This fear of the unknown is misplaced, however, because most Social Security fraud cases can be prosecuted using familiar federal criminal law statutes found in Title 18, without relying on the two Social Security felony fraud statutes found in Title 42.

This article strives to demystify the misconceptions about the viability of prosecution of Social Security fraud cases, and discusses the application of the Social Security felony fraud statutes as prosecution tools. The article also identifies additional federal statutes that the government has traditionally used to prosecute fraud against SSA programs. Specifically, Section I explains why Social Security is frequently targeted for fraudulent conduct. Next, Section II provides an overview of the Social Security felony fraud statutes and their elements. Finally, Section III explains the relationship between the SSA felony fraud statutes and various other federal criminal statutes found in Title 18 of the United States Code.

**I. Impact of fraud on Social Security programs**

Social Security benefits are essential to the economic well-being of millions of Americans. The proof is in the numbers. SSA reported that about 152,000,000 people worked and contributed to the SSA trust funds in employment or self-employment covered by Social Security programs. *See* SSA *2001 OASDI Trustees Report*. According to the Trustees' Report, these cash benefits comprise over 4% of the nation's gross domestic product. Benefits are paid to about 90% of American citizens aged 65 or older, and serve as

the major source of income for 64% of Social Security beneficiaries.

Because of the sheer numbers of claimants seeking benefits from one or more SSA benefits programs, some fraud in the system is unavoidable. Moreover, the opportunity for fraud is enhanced because SSA is an agency that has, historically, made extraordinary efforts to ensure that its programs are promptly available to qualified Americans. SSA serves as a lifeline to many needy Americans who would be unable to survive without payments from one or more benefits programs. It is not surprising, then, that in recent years, Social Security fraud has increasingly attracted national attention. In fiscal year 2001, the Office of the Inspector General (OIG) for the Social Security Administration opened over nine thousand potential fraud cases nationwide. If current trends continue, hundreds of these cases will ultimately result in federal and/or state convictions for disability fraud, retirement fraud, theft of government property, and/or Social Security number misuse.

**II. Statutory framework: the Social Security fraud statutes**

One who wrongfully applies for and/or receives benefits payments under one of the programs administered by SSA may be subject to criminal liability under either 42 U.S.C. § 408(a), or 42 U.S.C. § 1383a, of the United States Code. The Social Security felony fraud statutes can be used separately, or in concert, with general Federal criminal statutes found in Title 18, to prosecute fraud in benefits programs. Neither Title 18 nor Title 42 provides the exclusive criminal remedy for prosecution of Social Security fraud. Indeed, in some instances, Title 18 may provide a more suitable remedy for prosecution.

**A. 42 U.S.C. § 408(a) – A Felony Provision Aimed at Title II Program Fraud, Disability Fraud, and/or SSN Misuse**

In 1981, Congress made Social Security fraud a felony, punishable by five years in prison and a fine up to $5000. (Pub. L. No. 97-123). This was subsequently increased to ten years in prison and a fine up to $10,000. The SSA felony fraud statute, 42 U.S.C. § 408(a)(1)-(8), contains the Social Security Act's primary criminal provisions. The statute is comprehensive, carefully spelling out restraints on fraud by specifying requirements for disclosure of specific events, and identifying facts that affect the right to payment of SSA benefits.

The statute is broadly written, and is paraphrased as follows:

> Section 408.
>
> Whoever . . .
>
> (2) makes or causes to be made any false statement or representation of a material fact in any application for any payment or for a disability determination . . . **or**
>
> (3) at any time makes or causes to be made any false statement or representation of a material fact for use in determining rights to payment . . . **or**
>
> (4) having knowledge of the occurrence of any event affecting (i) his initial or continued right to any payment . . . or (ii) the initial or continued right to any payment of any other individual in whose behalf he has applied for or is receiving such payment . . . **conceals or fails to disclose such event with an intent fraudulently to secure payment** either in a greater amount than is due or when no payment is authorized, **or**
>
> (5) having made application to receive payment . . . for the use and benefit of another, and having received such a payment, **knowingly and willfully** converts such a payment, or any part thereof to a use other than for the use and benefit of such other person,. . . **or**
>
> (6) willfully, knowingly, and with intent to deceive . . . [SSA] as to his true identity (or the identity of another person), furnishes or cause to be furnished, false information to [SSA with respect to earnings information]. . . **or**
>
> (7) for the purpose of causing an increase in any payment . . . when no payment is authorized . . . **or for any other purpose**–(A) willfully, knowingly, and with intent to deceive, uses a social security account number assigned by . . . [SSA on the basis of false

information] . . . **or** (B) with intent to deceive, falsely represents a number to be the social security account assigned by . . . [SSA] to him or to another person, when in fact such number is not the social security number [assigned by SSA] **or** (C) knowingly alters a social security card . . . or counterfeits a social security card, or possesses a social security card or counterfeit card with intent to sell or alter it, **or**

(8) discloses, uses, or compels the disclosure of the social security number of any person in violation of the laws of the United States,

shall be guilty of a felony and if convicted will be fined and imprisoned for five years or both.

42 U.S.C. § 408(a)(1)-(8) (emphasis added).

Social Security fraud cases can be quite diverse, ranging from clear false statements on benefit applications to concealment of material facts. Most fraud involving Social Security benefits programs is the result of deliberate deception, and arises when an applicant falsifies a document or record offered as proof of disability, or misrepresents material facts, such as paternity, on an application for benefits. Fraud can also be the result of an omission when a beneficiary fails to report a change in circumstance, or conceals a material event. Significant unreported events might include securing a new job, getting married, being incarcerated, or failing to report the death of a family member who is in active benefit status. A typical concealment scenario involves a disability beneficiary who conceals his full-time work from SSA.

The Third Circuit, in upholding a conviction for Social Security fraud in a concealment case charged under 42 U.S.C. § 408(a)(4), identified the following elements:

1. The defendant had knowledge of an event affecting his or her right to receive or to continue to receive payments;

2. The defendant knowingly concealed or failed to disclose this event to the Social Security Administration;

3. The defendant concealed or failed to disclose this event to the Social Security Administration with the intent to fraudulently secure payment of disability benefits in an amount greater than was due him or her or when no payment was authorized. *See United States v. Baumgardner*, 85 F.3d 1305, 1310-11 (1996) (setting out the elements for a prosecution under 42 U.S.C. § 408(a)(4)).

With respect to the first element, courts have construed the term "event" broadly to include essentially anything that would affect the right to payment. *Baumgardner*, 85 F.3d at 1310-1311; *see also United States v. Huckaby*, 698 F.2d 915 (8th Cir. 1982). The second element is self-evident and straightforward, requiring that the defendant must know of the event affecting their right to payment and knowingly conceal it. The third element requires that the concealment must have been "with an intent fraudulently to secure payment ... in an amount greater than was due." *Id*.

**B. 42 U.S.C. § 1383a – A Felony Provision Aimed at Prosecuting SSI Fraud**

In 1994, Congress passed the Social Security Independence and Program Improvements Act of 1994, which increased the penalties for Social Security Supplemental Security Income (SSI) fraud. The new amendments specifically provided that in SSI fraud cases, the offense will be punishable by a fine as determined under the general criminal fine statutes, and by a prison term of not more than five years, or both. This provision conformed the specific crime of SSI fraud to the criminal sanctions already found in 42 U.S.C. § 408(a).

SSI is awarded on the basis of financial need, as determined in relation to both "income" and "resources" (as those terms are defined for purposes of the Social Security Act). Eligibility for SSI monthly cash benefits depends upon the severity of the applicant's condition, and the amount paid to each SSI recipient depends upon: (1) how much other income an individual receives; (2) the living arrangements of the individual; and (3) other circumstances that affect an individual's financial needs. SSA's ability to properly determine a recipient's continuing eligibility, and the correct monthly benefit due that recipient, is directly dependent upon SSA's

ongoing access to accurate and current information regarding the recipient.

The SSI felony fraud statute is broadly written, and is paraphrased as follows:

> § 1383a. Fraudulent acts; penalties; restitution.
>
> (a) Whoever–
>
> (1) knowingly and willfully makes or causes to be made any false statement or representation of a material fact in any application for any benefit . . .,
>
> (2) at any time knowingly and willfully makes or causes to be made any false statement or representations of a material fact for use in determining rights to any such benefit,
>
> (3) having knowledge of the occurrence of any event affecting (A) his initial or continued right to any such benefit, or (B) the initial or continued right to any such benefit of any other individual in whose behalf he has applied for or is receiving such benefit, conceals or fails to disclose such event with an intent fraudulently to secure such benefit either in a greater amount or quantity than is due or when no such benefit is authorized, or
>
> (4) having made application to receive any such benefit for the use and benefit of another and having received it, knowingly and willfully converts such benefit or any part thereof to a use other than for the use and benefit of such other person,
>
> shall be fined under Title 18, United States Code, imprisoned not more than 5 years, or both.

42 U.S.C. § 1383a(a)(1)-(4).

The elements for a conviction under the SSI felony fraud statute are:

> 1. The defendant knowingly and willfully made or caused to be made a false statement or representation of a material fact in an application for a benefit;
>
> 2. The defendant knowingly concealed or failed to disclose this event to the Social Security Administration;
>
> 3. The defendant concealed or failed to disclose this event to the Social Security Administration with the intent to fraudulently convert it to her own use.

While there is no case authority setting forth the elements for 42 U.S.C. § 1383a(a), these elements are similar to those found in *Baumgardner*, 85 F.3d at 1310-11, outlining the elements for 42 U.S.C. § 408(a)(4). The statute is intended to reach a person who knows that he or she is making a false statement in the first instance, and then knowingly and willfully conceals it. In effect, the statute requires disclosure of a specific event or facts that affect the right to a particular payment. In other words, not only the event, but the specific claims or payments, must be identified.

**III. Application of Title 18 to Social Security fraud cases**

The existence of specific criminal penalties in the Social Security Act does not preclude prosecution under more general criminal statutes found in Title 18. For example, a prosecutor may find it advantageous, in some circumstances, to charge an individual who has committed Social Security fraud under the more general statute dealing with conversion/theft of government property (18 U.S.C. § 641). This statute does not require fraud as a necessary element, whereas under the Social Security felony fraud statute fraud is a necessary element. Sentencing issues might also be a consideration in deciding whether to charge an individual under Title 18 or Title 42. Restitution is also a consideration that might determine whether an individual is charged with Title 18 or one of the Social Security felony fraud statutes, because Title 42 does not incorporate provisions relating to the Mandatory Victims Restitution Act of 1996, Pub. L. No. 104-132. Thus, an individual accepting a plea agreement based on 42 U.S.C. § 408(a)(4) might be ordered to pay significantly less in restitution to the victim (SSA) than someone entering a plea based upon 18 U.S.C. § 641.

Other general criminal statutes are available and useful in prosecuting Social Security fraud matters, and may be used in conjunction with, or independent of, the Social Security felony fraud statutes. Prosecutors should remember that the

SSA felony statute is not limited in use to Social Security program fraud cases. For example, an individual using a false Social Security number when filing a fraudulent bankruptcy petition can be charged with both 18 U.S.C. § 152 and 42 U.S.C. § 408(a)(7)(B). Similarly, an individual charged with identity theft (18 U.S.C. § 1028(a)) can also be charged with Social Security Number misuse (42 U.S.C. § 408(a)(7)(B)). In fact, any crime in which a false Social Security Number has been used to misrepresent or conceal the identity of an individual may be charged using 42 U.S.C. § 408(a)(7)(B).

The following is a (non-inclusive) list of general criminal statutes found in Title 18 that may prove useful in charging matters involving Social Security fraud. Similarly, when charging a case using one of the Title 18 criminal statutes, a provision of 42 U.S.C. § 408(a) might prove beneficial.

- 18 U.S.C. § 152. Bankruptcy fraud; Concealment of assets; false oaths and claims;
- 18 U.S.C. § 286. Conspiracy to defraud the United States with respect to claims;
- 18 U.S.C. § 287. False, fictitious, or fraudulent claims;
- 18 U.S.C. § 371. Conspiracy to defraud or commit an offense against the United States;
- 18 U.S.C. § 495. Altering, forging, or counterfeiting documents to receive money from the United States, deliberately submitting or passing such documents with an intent to defraud the United States;
- 18 U.S.C. § 506. Altering or counterfeiting the seal of a United States Agency, or the knowing use or possession of an altered or counterfeited seal;
- 18 U.S.C. § 641. Embezzling, stealing, or converting a record, money, or anything of value of the United States, or the receiving of such property with the knowledge that it was embezzled, stolen, or converted;
- 18 U.S.C. § 712. Misusing names or seals of an agency of the United States on an emblem or insignia to convey a false impression that the business represents the United States;
- 18 U.S.C. § 1001. Knowingly and willfully concealing a material fact or making a false statement or representation in a manner within the jurisdiction of a department or agency of the United States;
- 18 U.S.C. § 1002. Possession of false papers to defraud the United States;
- 18 U.S.C. § 1028(a). Knowingly transferring stolen or false identification documents;
- 18 U.S.C. § 1341. Using the mails for a scheme to defraud;
- 18 U.S.C. § 1342. Use of the mails for an unlawful business, where a false name or address is used;
- 18 U.S.C. § 1343. Using the wires for a scheme to defraud;
- 18 U.S.C. § 1542. False statement in application and use of a passport;
- 18 U.S.C. § 1546. Fraud and misuse of visas, permits and other documents;
- 18 U.S.C. § 1621. Perjury;
- 18 U.S.C. § 1622. Causing another to commit perjury.

Criminal penalties under the statutes listed above include substantial fines, restitution, and prison terms ranging from five to twenty years. Each of them has the potential for use in charging fraud involving Social Security. In many instances, the only federal charge available to a prosecutor is misuse of a Social Security number (42 U.S.C. § 408(a)(7)(B)). It is a common felony committed by criminals who try to hide their identities or create false documents in concert with other types of fraud.

Social Security fraud schemes range from the simple to the elaborate. Some are crimes of opportunity, while others are well-conceived and conducted with military precision and attention to detail. Most involve some form of false statement and fraudulent claim for payment, while others are conceived using false identities, multiple Social Security numbers, and fictitious injuries or health issues. Remember, the jury will love you for protecting their retirement.❖

**ABOUT THE AUTHOR:**

❑**John K. Webb** is a Special Assistant United States Attorney, detailed to the United States Attorney's Offices for the District of Arizona and the Central District of California by the Office of the Counsel to the Inspector General/Social Security Administration. He has successfully prosecuted more than 100 cases involving fraud in Social Security benefits programs during the past four years. Prior to his current assignments in California and Arizona, he served as a SAUSA in both the Western District of Washington and the District of Oregon.✠

# The Mail and Wire Fraud Statutes

*Michael L. Levy*
*Assistant United States Attorney*
*Chief, Computer Crimes*
*Eastern District of Pennsylvania*

## I. Introduction

This article is written to give an overview of issues that can arise in the prosecution of fraud cases under the mail and wire fraud statutes. Although this article focuses upon mail fraud and wire fraud, the operative words of those statutes show up in many crimes. Congress has used the terms "scheme and artifice to defraud" and "to obtain money and property by means of false and fraudulent pretenses, representations and promises" in many statutes. *E.g.*, 7 U.S.C. § 60 (fraud by commodity trading advisors); 15 U.S.C. §§ 77q (fraudulent interstate securities transactions), 78jjj (securities fraud), 80b-6 (prohibited transactions by investment advisors), 1703 (fraud in interstate land sales); 18 U.S.C. §§ 157 (bankruptcy fraud), 514 (fictitious obligations), 1031 (major fraud against the United States), 1341 (mail fraud), 1343 (wire fraud), 1344 (bank fraud), 1347 (health care fraud), 2314 (interstate transportation of fraudulently obtained property). Consequently, issues discussed in this article may also be matters of concern under these other statutes. The article is not intended as the final word on these issues. I have written it to alert prosecutors to some recurring issues under the mail and wire fraud statutes and to give a starting point for research. The mail and wire fraud statutes are wonderful tools. By criminalizing "fraud" Congress gave prosecutors a tool far broader than the earlier crimes such as larceny, embezzlement or misapplication. One former Assistant United States Attorney, now a judge, wrote of the mail fraud statute that it is "our Stradivarius, our Colt .45, our Louisville Slugger, our Cuisinart – and our true love." Jed S. Rakoff, The Federal Mail Fraud Statute (Pt.1), 18 Duq. L. Rev. 771 (1980). Were he writing today, he would probably also call it our Tech 9 and our Uzi.

**II. A unitary statutory structure**

The elements of mail fraud are as follows:

a. The defendant devised or intended to devise a scheme or artifice

1) to defraud, or

2) to obtain money or property by means of false or fraudulent pretenses, representations or promises, and

b. for the purpose of executing the scheme or artifice or attempting to do so,

c. the defendant

1) placed in an authorized depository for mail matter any matter or thing to be sent or delivered by the Postal Service, or

2) took or received from an authorized depository for mail matter any matter or thing, or

3) knowingly caused to be delivered by mail or by any private or commercial interstate carrier any matter or thing

a. according to the direction thereon; or

b. at the place at which it is directed to be delivered by the person to whom it is addressed; or

4) deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier.

Wire fraud has identical elements, except that instead of mailings, there must be a wire transmission that passes in interstate commerce. The wire fraud statute is based exclusively on the Commerce Clause of the Constitution, Article I, Section 8, Clause 3. The mail fraud statute looks to the Commerce Clause and the Post Office Clause, Article I, Section 8, Clause 7. Note that while a mailing may be "for the purpose of executing the scheme or attempting to do so," wire fraud has no "attempting" language.

Although the mail fraud statute appears to have two prongs and to prohibit both schemes to defraud *and* schemes to obtain money and property by means of false and fraudulent pretenses, representations and promises, the Supreme Court has held that these are merely two ways of saying the same thing. *McNally v. United States*, 483 U.S. 350, 358-59 (1987); *Cleveland v. United States*, 531 U.S. 12, 17 (2000). Both cases pointed out that the statutory history of mail fraud demonstrated that the "false and fraudulent" phrase was added merely to codify the result in *Durland v. United States*, 161 U.S. 306 (1896). *Durland* held that the term scheme to defraud covered not only a misrepresentation as to some existing fact, but also misrepresentations as to the future. In *Cleveland* the Court said of the possibility of construing the statute to have two independent clauses, "[b]ut we rejected that construction of the statute [in *McNally*], instead concluding that the second phrase simply modifies the first. . . ." *Cleveland,* 531 U.S. at 27.

One of the issues not considered by *Cleveland*, which was an issue in *United States v. Frankel*, 721 F.2d 917 (3d Cir. 1983), is the distinction between a fraud committed by a material omission and one committed by a material misrepresentation. *Frankel* was concerned with the deposit of bad checks in a check-kiting scheme. The Supreme Court held in *Williams v. United States*, 458 U.S. 279 (1982), that a check is not a statement under 18 U.S.C. § 1014. Thus, it could not be a "representation" under the fraud statutes. In *Frankel* the Court held that the use of a bad check could not be prosecuted under the false representation prong of the mail fraud statute, because a bad check is not a representation. The *Frankel* Court did clearly suggest, however, that such misconduct could be prosecuted under the scheme to defraud prong. *Accord*, *United States v. Rafsky*, 803 F.2d 105, 107 (3d Cir. 1986). The distinction between the two parts of the mail fraud statute is that a scheme to defraud includes material omissions and a scheme by false representations does not. The distinction is clearly illustrated by the bank fraud statute, 18 U.S.C. § 1344. The legislative history of the bank fraud statute made it clear that Congress intended for this statute to cover check

kites and to get around the *Williams* decision. S.Rep. 98-225, at 663-68 (1983). Congress accomplished this through the same "scheme or artifice" language it had used in the mail fraud statute. See *United States v. Schwartz*, 899 F.2d 243, 247 (3d Cir. 1990).

**III. Success irrelevant**

It is not necessary for the defendant to gain, or for the scheme to succeed, in order to convict the defendant. *United States v. Frey*, 42 F.3d 795, 800 (3d Cir. 1994); *United States v. Williams*, 728 F.2d 1402, 1405 (11th Cir. 1984); *United States v. Curtis*, 537 F.2d 1091, 1095 (10th Cir. 1976); *United States v. Pollack*, 534 F.2d 964, 978 (D.C. Cir. 1976); *Pritchard v. United States*, 386 F.2d 760, 765-66 (8th Cir. 1967). The victim does not have to have suffered a loss, because the crime consists merely of devising the scheme and executing or attempting to execute it. *United States v. Copple*, 24 F.3d 535, 544 (3d Cir. 1994).

**IV. Scheme defined**

Congress did not define "scheme or artifice to defraud" when it first coined that phrase, nor has it since. Instead that expression has taken on its present meaning from 111 years of case law. *United States v. Lemire*, 720 F.2d 1327, 1335 (D.C. Cir. 1983).

"The law does not define fraud; it needs no definition; it is as old as falsehood and versable as human ingenuity." *Weiss v. United States*, 122 F.2d 675, 681 (5th Cir. 1941).

A scheme to defraud is not defined according to "technical standards." "The scheme need not be fraudulent on its face, but must involve some sort of fraudulent misrepresentations or omissions reasonably calculated to deceive persons of ordinary prudence and comprehension." *United States v. Pearlstein*, 576 F.2d 531, 535 (3d Cir. 1978). See discussion below regarding *Neder v. United States,* 527 U.S. 1 (1999).

**V. Intent to defraud is required**

Mail fraud is a specific intent crime. The specific intent required, however, relates only to the intent to defraud. "Under the mail fraud statute, it must be shown that the defendants possessed the requisite intent to defraud. Proof is required of specific intent and the defendants must either have devised the fraudulent scheme themselves, or have willfully participated in it with knowledge of its fraudulent nature." *Pearlstein*, 576 F.2d at 537. (Citations omitted)

As the court in *United States v. Cusino*, 694 F.2d 185, 188 (9th Cir. 1982), put it, regarding the wire fraud statute: "The specific intent requirement under 18 U.S.C. § 1343 pertains to the scheme to defraud ... not to the causing of wire transmissions."

The mail fraud and wire fraud statutes are to be read *in pari materia*. The principles which apply to one apply to the other. *E.g., United States v. Tarnapol*, 561 F.2d 466, 475 (3d Cir. 1977); *United States v. Computer Sciences Corp.*, 689 F.2d 1181, 1188 n. 14 (4th Cir. 1982), *overruled on other grounds*, *Busby v. Crown Supply, Inc.*, 896 F.2d 833 (4th Cir. 1990); *United States v. Feldman*, 711 F.2d 758, 763 n. 1 (7th Cir. 1983); *United States v. Lemire*, 720 F.2d 1327, 1334 n. 6 (D.C. Cir. 1983). *See also Carpenter v. United States*, 484 U.S. 19, 25 n.6 (1987).

Specific intent can be proven by circumstantial evidence. In the case of a lower level person in a scheme, evidence of continuing personal or professional relationships with the architects of the scheme, excessive financial gain or extravagant expense accounts, and the defendant's role in the operation (supervisor vs. "gofer"), are relevant factors. *Pearlstein*, 576 F.2d at 541-42. A specific intent to deceive may be found from a material misstatement made with reckless disregard of the facts. *United States v. Boyer*, 694 F.2d 58 (3d Cir. 1982); *United States v. Hannigan*, 27 F.3d 890, 892, n.1 (3d Cir. 1994).

Although "good faith" is the opposite of having an intent to defraud, once the court has given a jury proper instructions on the elements of the offense, it is not required to give a further charge on good faith. *United States v. Gross*, 961 F.2d 1097 (3d Cir. 1992).

**VI. Intent to use mails not necessary**

It is not necessary that the scheme contemplate the use of the mails as an essential element, nor is it necessary for the government to

show that the defendant mailed anything, as long as he caused it to be mailed. *Periera v. United States*, 347 U.S. 1 (1954). The defendant does not actually have to know that the mails were used and, *a fortiori*, *the mailing does not have to be willful* (devising the scheme is the willful act). "Where one does an act with knowledge that the use of the mails will follow in the ordinary course of business, or where such use can reasonably be foreseen, even though not actually intended, then he 'causes' the mails to be used." *United States v. Periera*, 347 U.S. at 8-9.

Where one devises a scheme which will involve the use of attorneys to make claims and file law suits, the use of the mails to forward claims to insurance carriers and to send pleadings to opposing counsel is reasonably foreseeable. *United States v. Lebovitz*, 669 F.2d 894 (3d Cir.1982); *United States v. Sturm*, 671 F.2d 749 (3d Cir. 1982). Similarly, where one expects a payment from an insurance carrier, the mailing of a check from the insurance company is reasonably foreseeable. *United States v. Tiche*, 424 F.Supp. 996 (W.D.Pa.), *aff'd. mem.,* 564 F.2d 90 (3d Cir. 1977). It is important to emphasize that *Periera* held that there are two ways to meet the knowledge requirement of the statute: first, by showing that the defendant had actual knowledge that the mails would be used (subjective proof); or, second, by showing that, regardless of the defendant's actual knowledge, it was reasonably foreseeable that the mails would be used (objective proof). The same standard applies with respect to wire fraud. *United States v. Bentz*, 21 F.3d 37, 40 (3d Cir. 1994).

**VII. The "in furtherance" requirement**

The mailing involved must be "in furtherance" of (or in the language of the statute – "for the purpose of executing") the scheme. The use of the mails need not, itself, be an essential element of the scheme. It is enough that the use of the mails merely furthers the scheme. *United States v. Maze*, 414 U.S. 395, 400 (1974).

> We do not wish to be understood as intimating that, in order to constitute the offense, it must be shown that the letters so mailed were of a nature calculated to be effective in carrying out the fraudulent scheme. It is enough if, having devised a scheme to defraud, the defendant, with a view of executing it, deposits in the post office letters, which he thinks may assist in carrying it into effect, although, in the judgment of the jury, they may be absolutely ineffective therefor.

*Durland v. United States*, 161 U.S. 306, 315 (1896); *United States v. Cardall*, 885 F.2d 656, 680 (10th Cir.1989)*; United States v. Finney,* 714 F.2d 420, 422-23 (5th Cir. 1983)*; United States v. Lea,* 618 F.2d 426, 430 (7th Cir. 1980)*; United States v. Adamo,* 534 F.2d 31, 36 (3d Cir. 1976)*; United States v. Street,* 529 F.2d 226, 228 (6th Cir. 1976).

Mailings which are purely incidental, however, are not covered. *United States v. Tarnapol*, 561 F.2d 466 (3d Cir. 1977). In *Tarnapol* the Court held that the regular mailing of invoices which would have occurred anyway were not mailings "in furtherance." *See also*, *United States v. Cross,* 128 F.3d 145 (3d Cir. 1997).

Mailings which are done after the scheme is completed are not covered. *United States v. Maze,* 414 U.S. 395 (1974). In *Maze* the Court held that where the defendants used a stolen credit card, the mailings of the credit card slips by the merchant to the bank after the sale had been completed were not "in furtherance," because they were done after the defendants had completed the scheme. They had gotten what they wanted and did not care what the merchant did with the credit card slip afterward. However, as long as the mailing is part of the execution of the fraud, or closely related to the scheme, a mail fraud charge will lie. *United States v. Brown*, 583 F.2d 659 (3d Cir. 1978).

Thus, two pitfalls to look out for are mailings done after the scheme has succeeded and mailings which would have been made anyway and which did not further the scheme. There are two ways in which mailings done after the perpetrator has obtained the money can be in furtherance. The first is in a continuing scheme, where each mailing furthers the fraud. The second is a lulling letter.

**A. Continuing scheme**

In *Schmuck v. United States*, 489 U.S. 705 (1989), the mailings of title work to the state bureau of motor vehicles to obtain new titles, sent after the sale of vehicles on which the odometers had been rolled back, were held to be covered by the statute, because of the continuing nature of the fraud. This distinguished the case from *Maze* because the deal was not really complete until the purchaser received the completed new title from the state motor vehicle bureau. If the purchaser did not get the new title, the scheme would have collapsed.

In *United States v. Morelli,* 169 F.3d 798 (3d Cir. 1999), the defendants established a "daisy chain" to avoid the payment of the diesel fuel excise tax. (Diesel fuel and home heating oil are the same. The government taxes diesel fuel, but exempts home heating oil from taxation. This tax structure requires certifications of the ultimate disposition of the fuel and the payment of the excise tax when home heating oil is sold for diesel fuel.) A daisy chain consists of a number of companies that sell the fuel. The conspirators designate one company to pay the excise tax (the "burn company") and that company fails to do so. There was a series of payments up the chain. The defendants argued that any exchanges up the chain before the "burn company" were not in furtherance of the fraud, because the fraud did not occur until the "burn company" failed to pay the taxes. The Third Circuit held that because the entire program constituted one large ongoing fraud scheme, each wiring furthered the tax scheme and helped to create the proceeds in each succeeding series of transactions.

> More precisely, each wiring, including those that occurred before a particular transaction, made it more difficult for the government to detect the entire fraudulent scheme or any particular fraudulent transaction or series of transactions. In sum, the money gained in each series of transactions (save the initial one) was the proceeds of wire fraud because the money was the proceeds of a fraud that was furthered by the prior wirings.

*Id.* at 807 (footnote omitted).

**B. Lulling letters**

The second type of post success mailing that is "in furtherance" is the lulling letter. Letters which are sent after the scheme has been completed, but which "were designed to lull the victims into a false sense of security, postpone their ultimate complaint to the authorities, and therefore make the apprehension of the defendants less likely than if no mailing had taken place," *United States v. Maze*, 414 U.S. at 403, are mailings in furtherance. *See also*, *United States v. Lane*, 474 U.S. 438 (1986); *United States v. Lebovitz*, 669 F.2d 894 (3d Cir. 1982). Letters promising to repay money to victims can be lulling letters, if done to avoid lawsuits and complaints which could jeopardize the scheme. *United States v. Otto*, 742 F.2d 104 (3d Cir. 1984).

In *United States v. Ashman*, 979 F.2d 469 (7th Cir. 1992), brokers on the Chicago Board of Trade worked together to fix the prices of commodities and defeat the open market system. The mailings were the confirmations of the purchases and sales which served as representations that the trades had been executed in the open market. The court held that these mailings were in furtherance, even though the fraud was already completed, because they prevented customers from checking whether they got the best price available.

**VIII. Mailing requirement**

It is necessary to prove that the item which was sent was, in fact, mailed. With the number of private courier services available today, it is not sufficient to have a witness say that the item was "sent." Such a statement, without further clarification, does not meet the mailing requirement. *United States v. Hart*, 693 F.2d 286 (3d Cir. 1982). In addition, "[a]lthough circumstantial evidence may be used to prove the elements of mailing essential to conviction under § 1341, reliance upon inferences drawn from evidence of standard business practice without specific reference to the mailing in question is insufficient." *United States v. Burks*, 867 F.2d 795, 797 (3d Cir. 1989). In *Burks* the testimony of a secretary that 99% of the items were mailed was held to be insufficient. The continuing validity of *Burks* was called into question by *United States v.*

*Hannigan*, 27 F.3d 890 (3d Cir. 1994). Because *Hannigan* was not an *en banc* decision, it could not overrule *Burks*. In *Hannigan,* a witness was able to testify about the specific document and show that the records of the company demonstrated that it had been sent to the mail room to be mailed and was not to be picked up. According to the Court, this cured the failure in *Burks* of not having testimony about the specific mailing. However, in *Hannigan* the witness did not testify about mail room procedures and could not say if someone had come to the mail room to pick up the document. Thus, there was no testimony about general business practice with respect to the mail room.

In *United States v. Cohen*, 171 F.3d 796 (3d Cir. 1999), the bookkeeper for Butler Foods testified that after invoices were prepared, they were placed in envelopes, run through the postal meter, and put in a United States mail bin which one of the defendants took to the post office in his car. She testified that Butler Foods never used any delivery method other than the United States mail for any of its invoices, and that the invoices at issue were handled in the normal manner. A manager at the company testified that it was standard practice to pick up the invoices in the mail bin and drop them off at the post office, and that he himself did this on occasion. Finally, an accountant for the Thriftway stores testified that it was normal business practice for his company to receive Butler Foods' invoices through the United States mail. The court held that this testimony provided sufficient evidence that Butler routinely delivered its invoices through the United States Mails and was sufficient proof of the mailing.

For fraud schemes starting after, or continuing after September 13, 1994, this concern about how an item was sent will be lessened. Congress added the words "or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier...." to the mail fraud statute. (P.L. 102-322). The effect of this amendment is to give the mail fraud statute two constitutional bases — the Postal clause (Article I, Section 8, Clause 7, "Congress shall have the Power . . . To establish Post Offices and post Roads . . . .") and the Commerce Clause. (Article I, Section 8, Clause 3, "Congress shall have the Power ... To regulate Commerce . . . among the several States . . . .") This amendment, however, will not solve all problems in this area. Prosecutors still have to prove that the carrier was either the Postal Service or some other carrier which is involved in interstate commerce. A person picking up the document or the use of some carrier not involved in interstate commerce will not satisfy even the expanded mail fraud statute. It is unlikely that the government would have won *Hart*, *Burks* or *Hannigan* even with this amendment. In none of those cases did the government establish how the item was delivered. However, since Congress made the crime delivery by an interstate commercial carrier, and not interstate delivery, intrastate deliveries are covered whether the item was sent by the Postal Service or by a commercial carrier. *United States v. Photogrammetric Data Services, Inc.*, 259 F. 2d 229, 246-49 (4th Cir. 2001); *United States v. Marek*, 238 F.3d 310, 318 (5th Cir. 2001)(en banc), *cert. denied* __ U.S. __, 2001 WL 410327 (10/1/2001).

It is not necessary that the false representations themselves were transmitted by mail or that the mailings went to or from the intended victim. *Periera v. United States* 347 U.S. 1 (1954).

**IX. The materiality requirement**

In *Neder v. United States*, 527 U.S. 1 (1999), the Supreme Court held that materiality is an element of a scheme to defraud. *Neder* involved the interpretation of the mail, wire and bank fraud statutes. The Court held that the term fraud had a common law meaning that required that the misrepresentation or omission be material. The amorphous language that sometimes appears in cases must be read in light of this limitation. For example, in *United States v. Goldblatt*, 813 F.2d 619, 624 (3d Cir. 1987), the court wrote: "The term 'scheme to defraud,' however, is not capable of precise definition. Fraud instead is measured in a particular case by determining whether the scheme demonstrated a departure from fundamental honesty, moral uprightness or fair play and candid dealings in the general life of the community."

After *Neder,* there must be some material misrepresentation or omission in order to have a crime. *Compare*, *United States v. Frankel*, 721 F.2d 917, 921 (3d Cir. 1983)(Sloviter, J., concurring). This should not be a problem in most cases. For example, in a bad check case, while the depositing of a check is not a statement, *Williams v. United States*, 458 U.S. 279 (1982); *United States v. Frankel*, 721 F.2d at 917, the depositing of a bad check clearly involves a material omission – the failure of the depositor to tell the bank that the check will be dishonored. Thus, *Neder* should not have any effect upon our ability to charge the cases that we usually charge.

*Neder* will also have an impact upon our jury instructions. Because materiality is an element of fraud, it is a matter for the jury to decide. *Neder*; *United States v. Gaudin*, 515 U.S. 506 (1995). We must submit a proposed jury instruction on the issue. *Gaudin* stated that a false statement is material if it has a "natural tendency to influence, or is capable of influencing, the decision of the decision-making body to which it was addressed." (Internal quotations and citations omitted). *Gaudin*, 515 U.S. at 509.

*Neder,* 527 U.S. at 22, quoted the Restatement (Second) of Torts, § 538 (1976) to define materiality, saying that a matter is material if:

> (a) a reasonable man would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question; or
>
> (b) the maker of the representation knows or has reason to know that its recipient regards or is likely to regard the matter as important in determining his choice of action, although a reasonable man would not so regard it.

*Neder* will have no impact upon the traditional drafting of fraud indictments. *Neder* only holds that materiality is an element of fraud and that when we use the term "fraud" in an indictment, we are necessarily alleging the concept of materiality. *Neder* does not say that we need to allege that the misrepresentation or omission was material.

Finally, at least in theory, *United States v. Wells*, 519 U.S. 482 (1997) (holding that materiality is not an element of 18 U.S.C. § 1014), may have an impact upon some charging decisions. *Wells* held that when Congress used the term "false" in § 1014, it did not include a requirement of materiality. Any false statement in a loan application is covered by the statute, whether the statement is material or not. This could mean that if the defendant is charged with devising or executing a scheme and artifice to obtain property by means of false (but not fraudulent) representations, materiality is not an element. This "cute" drafting was certainly implied in *Neder*, 527 U.S. at 23 n. 7, but it has not yet been tested in court.

**X. Status of victim**

The victim's negligence is not a defense. However, there is a debate about whether it was reasonable for the victim to be deceived. For example, the following quotes show one side of the argument:

> The victim's negligence is not a defense to criminal conduct. The truth about virtually every scheme to defraud could be obtained if the gull were clever and diligent enough. The truly careful are, perhaps, never defrauded because they are not deceived by the artifice. The laws protecting against fraud are most needed to protect the careless and the naive from lupine predators, and they are designed for that purpose.

*United States v. Kreimer*, 609 F.2d 126, 132 (5th Cir. 1980).

> To the extent that [defendant] is arguing that the victim was negligent in ignoring Johns' advice and in failing to review the Schedules A, we reject the relevance of those allegations, even if true. The negligence of the victim in failing to discover a fraudulent scheme is not a defense to criminal conduct.

*Id. United States v. Coyle,* 63 F.3d 1239, 1244 (3d Cir. 1995). *See also*, *United States v. Maxwell*, 920 F.2d 1028, 1036 (D.C. Cir. 1990); *United States v. Brien*, 617 F.2d 299, 311 (1st Cir. 1980); *Lemon v. United States*, 278 F.2d 369, 373

(9th Cir. 1960). On the other hand, some cases say that the scheme must be calculated to deceive persons of ordinary prudence. *E.g., United States v. Pearlstein*, 576 F.2d at 535 ("The scheme need not be fraudulent on its face, but must involve some sort of fraudulent misrepresentations or omissions reasonably calculated to deceive persons of ordinary prudence and comprehension."); *United States v. Brown*, 79 F.3d 1550, 1557-62 (11th Cir. 1996). In *United States v. Masten*, 170 F.3d 790, 795 (7th Cir. 1999), the Seventh Circuit explained that the reasonable person analysis is relevant only where the defendant claims that he did not intend to deceive anyone. In that special case, the reasonable person standard helps a jury to determine if the defendant had the intent to defraud. The facts of the Eleventh Circuit case, *Brown*, would support this interpretation of the reasonable person requirement.

*Neder*'s definition of materiality may provide some guidance. *Neder* adopts the Restatement's language that the fraudulent representation or omission must be such as to deceive a reasonable person. However, if the defendant knows that his listener is relying upon the representation, then even if a reasonable person would not consider the point material, the statement is material. By analogy, a scheme has to be such as to deceive a reasonable person. Nevertheless, where the defendant knows that his victim is being taken in, it does not matter if no reasonable person would be deceived.

**XI. Failure to disclose**

Neither *Neder* nor *Cleveland* changed existing law regarding non-disclosure. The courts have long said that fraud may be found not only where there is an affirmative misrepresentation, but also where there has been a deceitful concealment of material facts. *United States v. Olatunji*, 872 F.2d 1161, 1167 (3d Cir. 1989); *United States v. Pearlstein*, 576 F.2d at 535 (3d Cir. 1978); *United States v. Bush*, 522 F.2d 641, 651 (7th Cir. 1975) .

> We find no case law in this circuit to substantiate a claim that the misrepresentation must be active. Instead, we find that an essential element of mail fraud is that the defendant possess the specific intent to defraud, and that the intent to defraud be evidenced in any way, including non-action on the part of the defendant. Fraud, for purposes of a mail fraud conviction, may be proved through the defendant's non-action or non-disclosure of material facts intended to create a false or fraudulent representation.

*United States v. O'Malley*, 707 F.2d 1240, 1247 (11th Cir. 1983). *See United States v. Neder*, 197 F.3d 1122, 1125, 1130 (11th Cir. 1999) (discussing Neder's concealment of material facts and affirming the conviction after remand from the Supreme Court). The Supreme Court's opinion in *Neder* specifically referred to fraud as being committed by material misrepresentations or omissions. *Neder*, 527 U.S. at 22 (1999).

**XII. Generally no need to cite 18 U.S.C. § 2**

Both the mail and wire fraud statutes have their own causing language. Relying upon this language instead of the "willfully caused" language of 18 U.S.C. § 2, obviates the need to have the jury instructed on the issue of willfulness, which can become a problematic issue. *See e.g.*, *United States v. Curran*, 20 F.3d 560 (3d Cir. 1994).

**XIII. Single vs. multiple schemes**

One should be aware of the danger of charging multiple schemes in a single mail fraud. The concept is similar to that of single vs. multiple conspiracies. A mail fraud scheme is different from a conspiracy, however, because a conspiracy requires an agreement, while a fraud scheme only requires that the defendants participated in the same scheme, even if they had no agreement. *United States v. Camiel*, 689 F.2d 31, 35 (3d Cir.1982)("A conspiracy requires the existence of an agreement among the alleged co-conspirators, but the federal mail fraud statute requires only that the co-schemers participate in a common scheme. Thus, it is the existence of a common scheme, and not any agreement among the parties to participate in it, that is critical."); *United States v. Maker*, 751 F.2d 614, 625 n.8 (3d Cir. 1984)("a single scheme is shown when the evidence showed 'a common goal, operations carried out in virtually identical manner, and an overlapping of participants. . . .'" No requirement

that the entire scheme be planned at the outset, nor is the scope of the scheme determined by the defendant's state of mind at the initial alleged incident of mail fraud. Fact that more than one insurance company defrauded does not make this multiple schemes.). In *Camiel*, two different groups vied for control of the Philadelphia Democratic City Committee. One ousted the other. However, at different times, both ran a no-show state job scheme for party loyalists. The Third Circuit reversed the convictions, holding that although the indictment charged all defendants in one scheme, the schemes were separate.

**XIV. Withdrawal**

As noted above, a conspiracy requires an agreement while a scheme does not. *United States v. Bibby*, 752 F.2d 1116, 1124 (6th Cir. 1985); *Camiel*, 689 F.2d at 35; *United States v. Read*, 658 F.2d 1225, 1238 (7th Cir.1981). One consequence of this distinction is that some courts have held that withdrawal is not a defense to a scheme charge, although it is a defense to a conspiracy charge. The rationale is that a conspiracy requires an agreement from which one can withdraw. Since a fraud scheme does not require agreement, withdrawal is not possible. *Read*, 658 F.2d at 1238:

> The elements of the offenses are, however, different. The predicate for liability for conspiracy is an agreement, and a defendant is punished for his membership in that agreement. Mail and securities fraud, on the other hand, punish the act of using the mails or the securities exchanges to further a scheme to defraud. No agreement is necessary. A party's "withdrawal" from a scheme is therefore no defense to the crime because membership in the scheme is not an element of the offense. Spiegel is liable for mail fraud as a principal or as an aider and abettor, not a conspirator. As an aider and abettor, Spiegel need not agree to the scheme. He need only associate himself with the criminal venture and participate in it.

*But see United States v. Lothian*, 976 F.2d 1257, 1263 (9th Cir.1992):

> Although we find the Seventh Circuit's rationale in *Read* instructive in determining the proper contours of the withdrawal defense when a fraudulent scheme is charged, we do not find it entirely applicable to Lothian's offenses. In our view the liability for substantive fraud offenses is based on participation in a fraudulent scheme, for in this circuit a defendant who is a "knowing participant" in such a scheme is vicariously liable for co-schemers' uses of the mails or wires. *[United States v.] Dadanian*, 818 F.2d [1443] at 1446 [(9th Cir. 1987, *modified,* 856 F.2d 1391 (1988). Withdrawal ends the defendant's knowing participation, and therefore can negate the element of use of the mails or wires. At the same time, however, withdrawal will not shield a defendant from liability for uses of the mails of wires that are an inevitable consequence of actions taken while a participant in the scheme. Thus in *Read*, for example, the defendant was liable despite his resignation because he had "directed the inventory inflation scheme which largely contributed to the false statements contained in the mailings.... The mailings ... were an inevitable consequence of his actions.

**XV. Multiple counts**

Although the statute was designed to punish frauds, the gist of the offense is the use of the mails. *United States v. Tarnapol*, 561 F.2d 466, 471 (3d Cir. 1977); *United States v. Brown*, 583 F.2d 659, 664 (3d Cir. 1978). Thus, each mailing is a separate offense and should be charged in a separate count of the indictment. *Badders v. United States*, 240 U.S. 391 (1916); *United States v. Ledesma*, 632 F.2d 670, 678 (7th Cir. 1980); *United States v. Stull*, 743 F.2d 439, 444 (6th Cir. 1984); *United States v. Saxton*, 691 F.2d 712, 714 (5th Cir. 1982).

**XVI. Venue**

Mail fraud has its own venue paragraph in 18 U.S.C. § 3237(a) which provides:

> Any offense involving the use of the mails, transportation in interstate or foreign commerce, or the importation of an object or person into the United States is a continuing offense and, except as otherwise provided by enactment of Congress, may be inquired of and prosecuted in any district from, through, or into which such commerce, mail matter, or imported object or person moves.

In *United States v. Brennan*, 183 F.3d 139 (2d Cir. 1999), however, the court held that this statute does not apply to the mail fraud statute. The court held that the crime is committed by the depositing or the delivery of an item. In *Brennan* the mail was sent from Manhattan in the Southern District of New York, but the crime was charged in the Eastern District of New York on the theory that the mail had been sent out of either Kennedy or LaGuardia airports. Analyzing the history of the statute and the constitutional venue protections, the court held that venue was not proper in the Eastern District.

**XVII. The deceived and the defrauded**

If the defendant lies to A to get money from B, is there a violation of the mail fraud statute? The circuits are split on this. In *United States v. Blumeyer*, 114 F.3d 758 (8th Cir. 1997), the defendants gave false financial information to the state's Division of Insurance which allowed the company to remain in business and to avoid closure due to insolvency. This permitted the company to stay open and continue to collect premiums. The court held that "a defendant who makes false representations to a regulatory agency in order to forestall regulatory action that threatens to impede the defendant's scheme to obtain money or property from others is guilty of conducting a scheme or artifice ... for obtaining money or property by means of false or fraudulent pretenses, representations, or promises." *Id.* at 768. Thus, lying to the government, which permitted the defendants to keep the license which allowed them to collect premiums from the policy holders, was held to be a violation of the statute. The same result was reached in *United States v. Cosentino*, 869 F.2d 301, 307 (7th Cir. 1989).

In *United States v. Lew*, 875 F.2d 219, 221 (9th Cir. 1989), on the other hand, a lawyer who submitted false information to the government regarding his immigration clients was charged with defrauding his clients of the money they paid for fees. The court read *McNally v. United States,* 483 U.S. 350 (1987), to require that the intent must be to obtain money or property from the one who is deceived. Since the deception was made to the government, while the money came from the clients, the court reversed the conviction. In *United States v. Sawyer*, 85 F.3d 713, 734 n.18 (1st Cir. 1996), the court wrote, "In any event, Sawyer's deceptive conduct toward Hancock, alone, cannot form the basis of this honest services fraud conviction. Rather, the alleged victims of the mail fraud – here, the state and the public – must be the ones deceived." This split was noted most recently, but not resolved, in *United States v. Frost*, 125 F.3d 346, 360 (6th Cir. 1997)(collecting cases).

**XVIII. Honest services**

The mail fraud statute also covers the defrauding another of the "intangible right of honest services." 18 U.S.C. § 1346. This was once referred to as the "loyal and faithful services" theory of mail fraud and it had been considered a valid mail fraud theory for over forty years. Then the Supreme Court decided *United States v. McNally*, 483 U.S. 350 (1987), and eliminated this theory as a valid basis for a mail fraud prosecution. On November 18, 1988, 18 U.S.C. § 1346 went into effect, partially restoring this concept. *Cleveland v. United States*, 531 U.S. 12 (2000). Thus, for schemes devised and completed prior to November 18, 1988, loyal and faithful services is not a valid theory. For schemes completed prior to that date, an indictment must charge a loss of money or property. Lost intangible rights are not sufficient. However, loss of rights in intangibles which constitute property will suffice. *United States v. Carpenter*, 484 U.S. 19 (1987)(right of Wall Street Journal to have information gathered remain confidential until publication; writer of Journal's "Heard on the Street" column gave tips he had gained as a reporter to friends to trade in the market before the information was published in the Journal; held while the statute did not

protect the Journal's intangible right to the writer's "loyal and faithful" services, it did protect its right to keep this information confidential until the Journal was ready to publish it); *United States v. Zauber*, 857 F.2d 137 (3d Cir. 1988). This distinction is important to keep in mind as a scheme may not be an "honest services" scheme (discussed in the following paragraphs), but may still be a scheme to deprive someone of a property right.

Even if you charge a case as an intangible rights case and it does not fit into the § 1346 honest services category, you may still be able to win if you can show that the scheme necessarily involved financial loss to the victim. *United States v. Asher*, 854 F.2d 1483, 1496 (3d Cir. 1988); *United States v. Perholtz*, 842 F.2d 343, 365-67 (D.C. Cir. 1988); *United States v. Richerson*, 833 F.2d 1147, 1156-57 (5th Cir. 1987); *United States v. Wellman*, 830 F.2d 1453, 1461-64 (7th Cir. 1987); *United States v. Fagan*, 821 F.2d 1002, 1010, n.6 (5th Cir. 1987).

**A. Honest services – public corruption**

In the area of public corruption, the honest services theory has a long and honored history. The defraud clause of the conspiracy statute, 18 U.S.C. § 371, has long been used in public corruption cases. In discussing the predecessor of § 371, the Supreme Court said in *Hammerschmidt v. United States*, 265 U.S. 182, 188 (1924):

> To conspire to defraud the United States means primarily to cheat the government out of property or money, but it also means to interfere with or obstruct one of its lawful governmental functions by deceit, craft or trickery, or at least by means that are dishonest. It is not necessary that the government shall be subjected to property or pecuniary loss by the fraud, but only that its legitimate official action and purpose shall be defeated by misrepresentation, chicane, or the overreaching of those charged with carrying out the governmental intention.

Applying these concepts, the defraud clause has been applied to conspiracies to bribe congressmen, *United States v. Johnson*, 383 U.S. 169 (1966), Agriculture Department officials, *Haas v. Henkel*, 216 U.S. 462, 480 (1910), and United States Attorneys, *Glasser v. United States*, 315 U.S. 60 (1942). However, in *McNally v. United States*, 483 U.S. 350, 358 n.8 (1987), the Court held that the defraud clause of § 371 is broader than the defraud concept of mail fraud.

In passing § 1346, Congress did not restore the law completely to its state before *McNally*. Rather it only reinstated a "right to honest services." *Cleveland v. United States*, 531 U.S. 12, 18 (2000) ("Significantly, Congress covered only the intangible right of honest services, even though federal courts, relying on *McNally*, had dismissed for want of any monetary loss to any victim, prosecutions under § 1341 for diverse forms of public corruption, including licensing fraud.").

The theory of honest services in the public corruption area is based upon the concept that, "In a democracy, citizens elect public officials to act for the common good. When official action is corrupted by secret bribes or kickbacks, the essence of the political contract is violated." *United States v. Jain*, 93 F.3d 436, 442 (8th Cir. 1996). Put another way, "Public officials inherently owe a fiduciary duty to the public to make governmental decisions in the public's best interest." *United States v. DeVegter*, 198 F.3d 1324, 1338 (11th Cir. 1999).

In the public corruption area, there are several pre-*McNally* cases that are of interest, for they still may be good law after the adoption of § 1346. Cases involving self-dealing, or conflict of interest are well illustrated by *United States v. Bush*, 522 F.2d 641 (7th Cir. 1975), and *United States v. Keane*, 522 F.2d 534 (7th Cir. 1975)(the cases were argued on the same day and decided by the same panel). In *Bush* a press secretary to the mayor, in violation of the city's conflict of interest rules, held an interest in a company which was bidding on a city contract. He pushed members of the administration to award the contract to his company and either failed to disclose his interest, or affirmatively misrepresented that he had no interest. He filed false disclosure forms with the city. The court found that this was an honest services mail fraud scheme. It held that breaching a fiduciary duty alone is not sufficient, but when combined with a

material misrepresentation of interests, his conduct constituted a violation. *Id.* at 647-48. Because the city did suffer a pecuniary injury (the city could have negotiated a contract in which the profits which went to the defendant could have been retained by the city), it did not opine whether, in the absence of pecuniary injury, a mail fraud violation would have been shown.

In *Keane* a city alderman voted to have the city compromise liens on property without disclosing to his fellow alderman that he had an interest in the property. The court held that the active concealment of his personal financial interest while voting on the matter was sufficient to show a mail fraud violation. *Keane* also held that a specific violation of state law is not necessary for a mail fraud conviction. *See also United States v. States*, 488 F.2d 761, 767 (8th Cir. 1973); *United States v. Edwards*, 458 F.2d 875, 880 (5th Cir. 1972); *United States v. Clapps*, 732 F.2d 1148 (3d Cir. 1984).

There are currently different theories in the public corruption area on honest services. The first is set forth in *United States v. Sawyer*, 85 F.3d 713 (1st Cir. 1996), and *United States v. Woodward*, 149 F.3d 46 (1st Cir. 1988). In those cases, the First Circuit held that there are two ways to violate the duty of honest services: (1) taking a bribe or gratuity for some official acts; (2) failing to disclose a conflict of interest, resulting in personal gain. Quoting *United States v. Mandel*, 591 F.2d 1347, 1362 (4th Cir.), *aff'd in relevant part en banc*, 602 F.2d 653 (4th Cir. 1979), the court in *Sawyer,* 85 F.3d at 724, said:

> [T]he fraud involved in the bribery of a public official lies in the fact that the public official is not exercising his independent judgment in passing on official matters. . . . When a public official has been bribed, he breaches his duty of honest, faithful and disinterested service. . . . [T]he official has been paid for his decisions, perhaps without even considering the merits of the matter. Thus, the public is not receiving what it expects and is entitled to, the public official's honest and faithful service. [Citations omitted.]

As to undisclosed conflict of interests, the court said, *id*. at 724:

> A public official has an affirmative duty to disclose material information to the public employer. When an official fails to disclose a personal interest in a matter over which she has decision-making power, the public is deprived of its right either to disinterested decision making itself or, as the case may be, to full disclosure as to the official's potential motivation behind an official act. Thus, undisclosed, biased decision making for personal gain, whether or not tangible loss to the public is shown, constitutes a deprivation of honest services.

Note that with regard to the failure to disclose fraud, one must show a failure to disclose the personal interest plus some official action. It would appear that the court would not approve a mail fraud based solely upon a failure to disclose a conflict of interest or payment where the public official or employee took no official action. Such a holding would likely conflict with the plain language of the statute. In addition, if a public official or employee failed to disclose a conflict (on a required disclosure form, for example), but took no official action that would implicate any conflict of interest, such a failure to disclose does not seem to meet the materiality requirement of *United States v. Neder,* 527 U.S. 1 (1999).

Thus, there must be an undisclosed conflict of interest coupled with some type of official action that benefits the defendant. The court was careful to note that the concept of honest service requires the exercise of a discretionary or decision-making duty. If the public employee takes a tip (gratuity) for doing a completely non-discretionary act (such as issuing a permit), there is no deprivation of honest services, citing *United States v. McNeive*, 536 F.2d 1245 (8th Cir. 1976). In addition, if the public employee performs a service which is not an official act (*e.g.* making an introduction without more), there is no dishonest service performed, because the service performed was not part of a service that was owed to the public, citing *United States v. Rabbit*, 583 F.2d 1014 (8th Cir. 1978).

*Sawyer* and *Woodward* involved the prosecution of a lobbyist for paying, and of a legislator for taking, gratuities. It is clear that the state suffered no pecuniary loss in these cases. Nevertheless, the breach of the duty of honesty was held to constitute a violation of the mail and wire fraud statutes. The *Sawyer-Woodward* reasoning has been accepted in the Eleventh Circuit, *see United States v. Lopez-Lukis*, 102 F.3d 1164, 1169 (11th Cir. 1997).

One significant part of the *Sawyer-Woodward* decisions is that, "[i]n general, proof of a state law violation is not required for conviction of honest services fraud." *Sawyer*, 85 F.3d at 726. This stands in stark contrast to another theory of public corruption honest services fraud set forth in *United States v. Brumley*, 116 F.3d 728 (5th Cir. 1997). *Brumley* holds that the term "honest services" is to be defined under state law and, therefore, the government must prove "that conduct of a state official breached a duty respecting the provision of services owed to the official's employer under state law." *Id.* at 734. Under *Brumley*'s analysis, *id.* at 734, ". . . if the official does all that is required under state law, alleging that the services were not otherwise done 'honestly' does not charge a violation of the mail fraud statute." "If the employee renders all the services his position calls for, and if these and all other services rendered by him are just the services which would be rendered by a totally faithful employee, and if the scheme does not contemplate otherwise, there has been no deprivation of honest services." *Brumley* holds that the mail fraud statute does not protect the right of citizens to honest government.

*Brumley,* which concerned a charge against an executive branch employee, also holds that the duty of honest services is owed to the state as employer and not to the public in general. "Despite its rhetorical ring, the rights of the citizens to honest government have no purchase independent of rights and duties locatable in state law." *Id.* at 735. It is unclear what the Eleventh Circuit would say about an elected official.

The distinction between the *Sawyer-Woodward* line and *Brumley* can have significant consequences for charging. Under the former theory, it follows that by passing § 1346, Congress has uncoupled honest services mail fraud from state law and created a federal right to honest services. *United States v. Sawyer*, 239 F.3d 31, 41-42 (1st Cir. 2001). *See also, Badders v. United States*, 240 U.S. 391, 393 (1916) ("The overt act of putting a letter into the post-office of the United States is a matter that Congress may regulate. Whatever the limits to the power, it may forbid any such acts done in furtherance of a scheme that it regards as contrary to public policy, whether it can forbid the scheme or not.")(Citations omitted.) Thus, with the passage of § 1346, there is a statutory duty created by Congress to render honest services. Under *Brumley*, this argument is not viable.

One of the consequences of this uncoupling is that it is not necessary to rely upon state law to find the source of the right. Thus, even in a state which has no bribery or gratuity statute, if a legislator took a payment to vote on a particular bill or an executive branch employee took money for the exercise of his discretion, he would violate the federally created right of honest services. If an "in furtherance" wiring or mailing could be found, he could be prosecuted for mail or wire fraud. Similarly, even if a state had no disclosure law, taking a payment from an interested party, failing to disclose it and voting on a measure would violate the right to honest services. It is not yet clear if the *Sawyer-Woodward* line will go this far. However, the court did emphasize that to violate the mail fraud statute, on this theory, the government had to prove that the defendant acted "with two kinds of intent: that she intended to deprive the public of her honest services, and that she intended to deceive the public. *See Sawyer*, 85 F.3d at 729; *see also Woodward*, 145 F.3d at 55." *United States v. Sawyer*, 239 F.2d at 40-41.

### B. Honest services – private employer

While the right to honest services in the public sector is based upon the compact theory of government, "[e]nforcement of an intangible right to honest services in the private sector, however, has a much weaker justification because relationships in the private sector generally rest upon concerns and expectations less ethereal and more economic than the abstract satisfaction of receiving 'honest services' for their own sake." *United States v. Frost*, 125 F.3d 346, 365 (6th Cir.

1997); *United States v. deVegter*, 198 F.3d 1324, 1328 (11th Cir. 1999) ("On the other hand, such a strict duty of loyalty ordinarily is not part of private sector relationships. Most private sector interactions do not involve duties of, or rights to, the 'honest services' of either party.") Generally, these cases involve employer-employee relationships, although they can also involve outside contractors. Clearly, a *sine qua non* of an honest services case is a duty to provide honest services. Thus, for example, dishonesty between the salesman and the customer in the sale of a used car is never going to fit under an honest services theory.

Because many of the cases speak of the need for a fiduciary duty, some general agency principles are worth noting. In general, Restatement 2d, Agency (hereafter "Restatement") § 1, defines agency as "the fiduciary relation which results from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act." "An agent is a fiduciary with respect to matters within the scope of his agency." Restatement, § 13. Comment (a) provides in pertinent part:

> Among the agent's fiduciary duties to the principal is the duty to account for profits arising out of the employment, the duty not to act as, or on account of, an adverse party without the principal's consent, the duty not to compete with the principal on his own account or for another in matters relating to the subject matter of the agency, and the duty to deal fairly with the principal in all transactions between them.

Restatement, § 387 provides, "Unless otherwise agreed, an agent is subject to a duty to his principal to act solely for the benefit of the principal in all matters connected with his agency." Finally, "Unless otherwise agreed, an agent who makes a profit in connection with transactions conducted by him on behalf of the principal is under a duty to give such profit to the principal." Restatement, § 388. Comment (b) says that an agent can retain gratuities, if it is the custom in the business or if the employer agrees. *See United States v. Joselyn*, 206 F.3d 144, 149, 154 and n.10 (1st Cir. 2000), discussing this concept in general and noting that in the case of a corporation, the fact that management has condoned the practice may not be a defense, because the shareholders of the corporation may not have agreed.

> An agent who acquires confidential information in the course of his employment or in violation of his duties has a duty not to use it to the disadvantage of the principal, see § 395. He also has a duty to account for any profits made by the use of such information, although this does not harm the principal.

*Carpenter v. United States*, 484 U.S. 19, 27-28 (1987). Citing to an earlier case, the Court stated, "we noted the similar prohibitions of the common law, that 'even in the absence of a written contract, an employee has a fiduciary obligation to protect confidential information obtained during the course of his employment.'" *Id.* at 27.

While these principles are useful, the violation by an agent of any duty under common law or statute does not automatically become a crime. Violations of general agency principles, or even ethical principles, do not automatically make a mail or wire fraud case.

However, these principles provide a necessary (though not a sufficient) basis for understanding honest services fraud. It is essential that there be a violation of the principle that no man can serve two masters, before you can have an honest services fraud violation. The second master can be an outsider to the relationship (the person who pays a bribe or kickback) or the second master can be the agent's own personal interests, which he is supposed to subordinate to those of his master. In the absence of such a showing, an honest services fraud cannot be proven.

Generally, the courts use the same standards for a private honest services mail fraud as they do for one involving a public official. That is, there needs to be some potential financial benefit to the dishonest employee (either by bribe, kickback or embezzlement), a failure to disclose this "dishonest" relationship (conflict of interest) and some realistic potential for harm to the principal/employer. For examples of honest

services violations accomplished by a failure to disclose under the bank fraud statute, 18 U.S.C. § 1344, *see United States v. Harvard*, 103 F.3d 412 (5th Cir. 1997); *United States v. Mangone*, 105 F.3d 29, 31 (1st Cir.1997); *United States v. Pribble*, 127 F.3d 583 (7th Cir.1997). The advantage of an honest services bank fraud prosecution against bank employees and directors is that there is no need to find a mailing or wiring that is "in furtherance."

*United States v. Lemire*, 720 F.2d 1327 (D.C. Cir. 1983), gives a good illustration of this concept. Lemire was an employee of Raytheon Corp., which had a conflict of interest policy and required employees to certify annually that they were in compliance with the policy. Lemire gave information to a bidder seeking to do business with Raytheon which permitted the bidder to achieve inflated profits, while still submitting the lowest bid on a contract. Lemire got a kickback from the bidder for his efforts. Needless to say, Lemire did not disclose this conflict to Raytheon. The court first held that "an intentional failure to disclose a conflict of interest, without more, is not sufficient evidence of the intent to defraud an employer necessary under the wire fraud statute. There must be something which in the knowledge or contemplation of the employee poses an independent business risk to the employer." *Id.* at 1337 (citation omitted).

> Accordingly, our holding does not remove from the ambit of wire fraud undisclosed conflicts that, accompanied by activity on the part of the employee, carry a significant risk of identifiable harm to the employer apart from the loss of his employee's loyalty and fidelity. So long as the jury finds the non-disclosure furthers a scheme to abuse the trust of an employer in a manner that makes an identifiable harm to him, apart from the breach itself, reasonably foreseeable, it may convict the employee of wire fraud. The crucial determination must be whether the jury could infer that the defendant might reasonably have contemplated some concrete business harm to his employer stemming from his failure to disclose the conflict along with any other information relevant to the transaction.

*Id.*

In *United States v. Sun-Diamond Growers of California*, 138 F.3d 961 (D.C. Cir. 1998), *aff'd,* 526 U.S. 398 (1999), the court held that the potential for damage to the reputation of a public relations firm if an illegal corporate contribution was discovered was a serious economic risk. The court went on to say that the government does not have to prove that the defendant intended to cause economic harm, only that he had an intent to defraud. The court noted, "But *Lemire* did not go so far as to say that economic harm must be part of the defendant's intent in a private-sector "honest services" case – only that economic harm be within the defendant's reasonable contemplation." *Sun Diamond*, 138 F.3d at 974.

A slightly different, but more generalized expression of the test is found in *United States v. deVegter*, 198 F.3d 1324, 1328-29 (11th Cir. 1999), discussed more fully below, where the court said that "the breach of loyalty by a private sector defendant must in each case contravene – by inherently harming – the purpose of the parties' relationship." This phrasing may be more useful for the breach of loyalty by an employee or agent working for an organization that is not in business for profit. Hurting the purpose of the relationship for dishonest reasons should also violate the mail fraud statute.

In *United States v. Frost*, 125 F.3d 346 (6th Cir. 1997), the defendants were professors at the University of Tennessee, who allowed students to pass off material written by others as their own thesis or dissertation, and who concealed from the oral examination committees that the thesis or dissertation under review was not the student's own work. The students were employees of NASA and were involved in the awarding of government contracts. The professors had side businesses which sought government contracts. The scheme, at its core, involved a swap of degrees for government contracts. While the court upheld the conviction, it placed a strange reading on the honest services theory. The court, ostensibly following *Lemire,* held that:

> The prosecution must prove that the employee intended to breach a fiduciary duty, and that the employee foresaw or reasonably should have foreseen that his employer might suffer an economic harm as a result of the breach.

The court effectively held that the "concrete business harm" requirement of *Lemire*, 720 F.2d at 1337, was economic harm. In doing this the court recognized that, "Despite the literal terms of § 1346, we therefore have construed the intangible right to honest services in the private sector as ultimately dependent upon the property rights of the victim." *Frost*, 125 F.2d at 369. This construction would seem to be at odds with the general principle that a court "must give effect, if possible, to every clause and word of a statute." *Williams v. Taylor*, 529 U.S. 362, 364 (2000); *Gade v. National Solid Wastes Management Ass'n*, 505 U.S. 88, 100 (1992). By requiring that the employer be defrauded of property, the court effectively reads § 1346 out of existence. The Supreme Court has recognized in *Cleveland v. United States,* 531 U.S. 12 (2000) that Congress passed § 1346 to partially overrule *McNally*, which had held that the mail fraud statute protected only property.

The court in *Frost* found that the degree issued by the University was property and, therefore, upheld the convictions. It is not clear if this rationale survives *Cleveland v. United States*. In *Cleveland*, the Court held that a license is not property under the mail fraud statute as the issuing of a license is part of a state's regulatory scheme and not property in the hands of the state. Whether this rationale will also apply to a degree issued by a university (state owned or private) is unclear.

To avoid considering the "degree as property" issue, the court could have used two different lines of reasoning. First, as in *Sun Diamond*, the court could have held that the actions of selling advanced degrees could have injured the reputation of the University. This would have affected the ability of the University to attract students, faculty and grants. Thus, the University would have suffered some economic harm as a result of this conduct.

Second, the court could have held that the conflict of interest went to the core reason that the professors were hired by the University. A university hires professors to teach and test students and it gives them the authority to grant the one tangible thing that the university offers its students – a degree. A professor who "sells" degrees defeats that purpose. Using the standard articulated in *deVegter* – a breach of loyalty that inherently harms the purpose of the parties' relationship – would cover this situation.

Honest services require that the employee have the potential to get something of value in return for depriving his employer of honest services. The employee must violate the "two masters" rule, either by serving someone else's interest or by serving his own to the detriment of the employee's principal. Comment a to Restatement § 13 says:

> Among the agent's fiduciary duties to the principal is the duty to account for profits arising out of the employment, the duty not to act as, or on account of, an adverse party without the principal's consent, the duty not to compete with the principal on his own account or for another in matters relating to the subject matter of the agency, and the duty to deal fairly with the principal in all transactions between them.

At its core an "honest services" violation needs a violation of one of these duties. In *Frost*, the scheme involved the students helping the professors get contracts, while the professors helped them get their degrees. Thus, the professors got something of value for lowering the degree requirements.

*United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), demonstrates this principle well. Czubinski was an IRS employee who had access to the IRS computer system which he was supposed to use in performing his official duties. However, he also used the system to view the files of other people, when he had no legitimate reason to do so. He did not transmit this information to anyone else and the government had no proof that he intended to disclose this information to anyone else. The court held that the IRS was not

defrauded of property because, although information can be property, *see Carpenter v. United States*, 484 U.S. 19 (1987), either some articulable harm has to befall the holder of the information as a result of the employee's activities, or the person getting the information has to make some gainful use of it. Czubinski neither caused harm, nor gained anything. The court also rejected an honest services theory for three reasons. First, Czubinski "was not bribed or otherwise influenced in any public decision-making capacity. Nor did he embezzle funds. He did not receive, nor can it be found that he intended to receive, any tangible benefit." *Czubinski*, 106 F.3d at 1077. Second, the mail fraud statute is not some means of enforcing personnel regulations. Third (sounding like *United States v. Brumley*, 116 F.3d 728 (5th Cir. 1997), but not citing to *Brumley*), "Although he clearly committed wrongdoing in searching confidential information, there is no suggestion that he failed to carry out his official tasks adequately, or intended to do so." *Id.* at 1077.

On the other side of this equation is the issue of harm and how tangible it must be. In *United States v. Jain*, 93 F.3d 436 (8th Cir. 1996), a doctor took kickbacks from a hospital based upon patient referrals. The government had no evidence of tangible harm to the patients and there was no claim of unnecessary care or excessive hospitalization. The court did not decide if this was a violation of the patients' right to honest services, but held that "the essence of a scheme to defraud is an intent to harm the victim," *id.* at 442, and the patient-victims suffered no harm. While there was a breach of a duty to disclose the kickbacks, there was no harm.

In *United States v. DeVegter*, 198 F.3d 1324 (11th Cir. 1999), the defendant was hired by a county to advise it on which investment banker it should hire as the underwriter for a bond refunding. The defendant manipulated the process in favor of one investment bank in return for money. He gave that bank copies of a competitor's proposal and had them analyze it and help him write his report to tilt the scales of the decision-making process. The court held that "the breach of loyalty by a private sector defendant must in each case contravene – by inherently harming – the purpose of the parties' relationship." *Id.* at 1328-29. The court found that "Corrupting the process by which this recommendation was made poses a reasonably foreseeable risk of economic harm to Fulton County because the best underwriter might not be recommended." *Id.* at 1331. Note that the court said "might not be recommended." *Jain* required actual harm; *DeVegter* only required a reasonable possibility. While the injury in *DeVegter* was economic, the injury in *Jain* could have been physical. Kickbacks from hospitals create a reasonably foreseeable risk that patients will be hospitalized that do not need treatment. Other patients could be sent to a hospital that would not be as well equipped to treat them because of the doctor's financial incentive. It is not possible to harmonize *Jain* and *deVegter*.

Where a third party is paying an employee, believing that he is depriving the employer of honest services, it does not matter if the payee does not have an actual fiduciary relationship with the entity defrauded of honest services. The important factor is that the defendant engages in a scheme to deprive the employer of the employee's honest services. If that is done, then the statute is violated. *United States v. Sancho*, 157 F.3d 918, 920 (2d Cir. 1998)(per curiam), *cert. denied*, 525 U.S. 1162 (1999); *United States v. Middlemiss*, 217 F.3d 112, 120 (2d Cir. 2000).

Finally, a prosecutor should be aware of the "sound business judgment rule." A good faith, unconflicted business decision by an employee will not be second guessed by the courts and cannot be the subject of a mail fraud prosecution. *United States v. D'Amato*, 39 F.3d 1249, 1258 (2d Cir. 1994); *United States v. Wallach*, 935 F.2d 445, 464 (2d Cir. 1991). Thus, a case in which a business leader has run a business into the ground, causing the shareholders and creditors to lose money, will be a very difficult one to prove in the absence of clear proof of a financial conflict of interest.❖

**ABOUT THE AUTHOR**

❑**Michael L. Levy** is an Assistant United States Attorney (AUSA) for the Eastern District of Pennsylvania and is currently Chief of the Computer Crimes Division. Previously he served

as Acting United States Attorney, Deputy Chief of the Criminal Division, and First Assistant.

Mr. Levy has been an AUSA since 1990, after previously serving in the same capacity from 1980-83. Mr. Levy also has engaged in private practice and served as Special Attorney for the Philadelphia Strike Force.

Mr. Levy is an Adjunct faculty member, James E. Beasley School of Law, Temple University and has lectured frequently at the National Advocacy Center in Columbia, South Carolina.

The views and opinions expressed in this article are those of the author only and not the official position of the Department of Justice. This memo was originally written for attorneys in the Eastern District of Pennsylvania and, as a result, the citations may show a particular bent toward the Third Circuit. I have tried in many instances to add citations from other circuits. However, to the extent that I have not done so, the citations should give an attorney a beginning point for research in his or her own circuit.

I would like to thank Ronald H. Levine, Chief of the Criminal Division and Robert A. Zauzmer, Chief of Appeals, in my office for their suggestions and encouragement. My special thanks to Assistant United States Attorney Gregory A. Paw with whom I debated the merits of whether, and how, to charge a political corruption case under the mail fraud statute. It was these debates that introduced me to the subtleties of the honest services mail fraud theory that is discussed above.

# Identity Theft

*Beth Moskow-Schnoll*
*Assistant United States Attorney*
*District of Delaware*

Identity theft, the misappropriation of an individual's personal identification information, has emerged as a significant law enforcement and public concern. The Identity Theft Subcommittee of the Attorney General's Council on White-Collar Crime is responsible for the development of identity theft enforcement policy and coordination with the FBI, Treasury Department, Secret Service, Postal Inspection Service, Federal Trade Commission, Social Security Administration and other regulatory and law enforcement agencies.

Through the Identity Theft Subcommittee, the Department has expanded its reach in combating identity theft by joining forces with our state and local counterparts, including the International Association of Chiefs of Police, the National Sheriffs Association, the National Association of Attorneys General and the National District Attorneys Association. The Subcommittee has organized and participated in various training programs and conferences that disseminate information on trends, patterns of crimes and enforcement strategies aimed at state and local law enforcement agencies, which often act as the first line of defense in the battle to curb identity theft. In addition, the Subcommittee, chaired by the Criminal Division's Fraud Section, has been instrumental in promoting local and regional task forces and working groups to address identity theft.

The Subcommittee is interested in learning more about strategies, including the formation of task forces and other specialized units, that are being used by United States Attorneys' Offices to combat identity theft. If your office has developed an identity theft enforcement program, we ask that you share your office's experiences with the Subcommittee by calling the telephone number listed below. Additionally, as part of a government-wide initiative, United States Attorneys' Offices recently have been requested to

provide information about ongoing identity theft investigations to the Fraud Section, which is conducting a survey of all offices to determine the current inventory of identity theft cases.

The Subcommittee and the Fraud Section have prepared resource materials focusing on identity theft and the related crime of pretext calling or "pretexting" - - obtaining financial institution customer information by means of false pretenses. These materials are currently being distributed by the White-Collar Crime Council and include a form indictment and model jury instructions for Section 1028(a)(7) offenses, which also will be available on USA Book. For additional information and assistance on identity theft and pretexting matters, please call the Fraud Section at 202-514-0890.

**I. An overview of the identity theft problem**

In late 1998 and early 1999, investigators in the Army Criminal Investigations Division began receiving complaints from high ranking officers that someone had obtained credit in their names. Unbeknownst to the Army, during the same time period, similar complaints from high ranking officers were pouring into the criminal investigations divisions of the Navy, Air Force and Marines. Meanwhile, First USA Bank was uncovering fraudulent accounts and account applications in the names of military officers at an alarming rate.

When the investigators compared notes, they learned that the hundreds of fraudulent accounts were related. How had someone managed to obtain the personal information of the officers and then use that information to apply for credit in the officers' names? It turned out to have been all too easy.

The perpetrator was not some criminal mastermind, but a petty crook with a fifth grade education and some minimal computer skills named Lamar Christian. Christian had learned of the "scam", as he called it, through a friend of his in Florida who had shown him a Web site that contained the names, ranks and social security numbers of persons who had been promoted either to, or within, the officer ranks of the armed forces. The information on the Web site had been copied from the Congressional Record where the promotions had been published.

Using the information downloaded from the Web site, Christian applied for credit cards via the Internet from Wingspan Bank and First USA Bank's Internet bank. He also applied for credit via the Internet from Gateway Computers and then used the Gateway accounts to purchase computers and other electronic equipment. Christian's co-conspirator, Ronald Stevens, a/k/a "Squeaky", fenced the items that had been purchased with the fraudulent credit to members of his, e.g. Stevens', drug organization. As Stevens proudly admitted in a misguided effort to minimize his involvement in the offense, "I am a drug dealer. I don't know nothing about computers." With this scheme, Christian and Stevens obtained goods and cash worth several hundred thousand dollars and compromised the credit and good name of over three hundred military officers.

This is only one example of how easily an identity theft scheme can be perpetrated. Yet while these schemes may easily be executed, their results can be devastating. Such schemes cause monetary loss to the financial institutions and are devastating to the victims whose identities are stolen and whose credit is ruined. Therefore, we need to understand these schemes and learn what tools we have to combat and prosecute them.

Identity theft cases in the financial institution realm primarily involve account takeovers and fraudulent applications. An account takeover occurs when someone obtains a victim's identity information and uses it to take over an existing account held by the victim, usually by asking the bank to change the address on the account to an address under the thief's control and further requesting that an additional credit card be sent to the new address. Those who steal identities target dormant accounts in this type of scheme so that the true account holder will not notice that his or her monthly statement has not arrived.

A fraudulent application case occurs when someone obtains a victim's identity information and uses it to apply for new credit and/or open new accounts. This type of scheme is much more invidious in that the victim generally does not

learn that he or she has been victimized until their credit already has been harmed.

Both types of schemes are easily perpetrated because each requires only a few basic ingredients: (1) sources of personal or identity information; (2) fraudulent addresses to which credit cards and bank statements can be sent; and (3) fake identification in the victim's name to be used for bank and other in person transactions. While the need for fraudulent addresses and identification may be obvious, the sources of account information may not be.

There are myriad sources of personal information. In several cases that I have prosecuted, bank employees sold credit card account holders' personal information to others for as little as $15 per account. Similarly low paid employees of credit bureaus, doctor's offices, car rental agencies, and building management companies also have access to customers' names, social security numbers, dates of birth, and employment information and have compromised this information for a minimal price.

Mail theft, dumpster diving, and pretext calling are three low tech means of obtaining personal information. Theft of mail can range from a person stealing individual credit cards and convenience checks out of mailboxes to the theft of entire shipments of mail. Dumpster diving is where a person sorts through the trash outside a car rental agency or doctor's office, etc. and collects discarded papers containing customers' names, addresses, and social security numbers.

As exemplified by the Christian case, the Internet can be a source of identity information as well. While the Web site used by Christian no longer contains the personal information of the officers, a search using the term "social security number" turns up many sites that purport to be able to track down anyone's social security number and personal information for a fee. The Internet also hosts many sites discussing and/or offering fake ID's. An example is the "Hactivist" which bills itself as the "Ultimate Fake ID Reference Page."

**II. Investigative techniques**

There are many investigative techniques with which to combat these schemes. First, most financial institutions track the "footprints" of their employees, e.g. they have a record of every time an employee views customer account information. When the bank learns that certain accounts are fraudulent, their investigators can review the logs to determine if any of the accounts were viewed by the same employee. In this way, the bank hopefully can learn whether one of its employees was the point of compromise. In the best case scenario, once identified, the "dirty" bank employee will agree to cooperate against the person to whom they sold the information.

Second, many financial institutions use caller ID information to track telephone calls that come in on accounts. A subpoena for the telephone billing records and subscriber information for the subject telephones often provides valuable information as to the identity of the perpetrator of the fraud.

Third, in their investigations, many financial institutions use "link analysis", i.e. bank investigators enter the information pertaining to fraudulent accounts, such as addresses and telephone numbers, and run a search to determine whether the accounts are linked. If the financial institution does not keep such information, the agent investigating the case should be urged to perform the same type of analysis. While some of the information derived from this type of analysis may not lead to evidence of the defendant's guilt beyond a reasonable doubt, it is invaluable at sentencing when arguing that the additional linked accounts should be included as relevant conduct under U.S. Sentencing Guidelines Manual §1B1.3 (2000).

Fourth, if an account is opened online, you **may** be able to trace the email account used to open the account. However, for the following reasons, your chances of success are not great. One reason is that if the IP address on the email transmission was dynamic rather than static, you will need both the date and time the email transmission was received in order to conduct a trace. Yet, the majority of financial institutions do not log the date and time of email transmissions.

Another reason that e-mail transmissions are often difficult to trace is that financial institutions estimate that over 97% of fraudulent accounts are opened from free email addresses such as Excite, Hotmail, Juno, Usa.Net and Yahoo. Not surprisingly, because the services are free, the information collected from users is often false. As Excite's form response letter to a subpoena states, "I confirm that Excite-mail Services is a free service and while Excite requests that its users complete registration information prior to receiving an Excitemail account, Excite does not validate the completeness or accuracy of the user data supply." The user data supplied in that case stated that the user was O.J. Simpson of 2828 Crazy Ass Street with no city or state of residence.

There is at least one benefit to having a case involving computer transmissions. If a search of the suspect's computer occurs, it may reveal cookies, e.g. special text files created by a Website service and written onto the hard drive of a Web site visitor. These cookies will provide a road map of the Web sites visited by the computer user on the Internet.

Finally, perhaps the most valuable technique for investigating identity theft cases is the familiar advice to "follow the money." In cases involving cash, the victim financial institution will have records of where cash transfers were sent. In cases involving the purchases of goods, ship-to addresses can be identified and controlled deliveries made.

### III. Congress' response to the identity theft problem

#### A. The Identity Theft and Assumption Deterrence Act of 1998

In an effort to address the growing problem of identity theft, on October 30, 1998, the Identity Theft Act [Pub. L. 105-318] went into effect. The Act was needed since Section 1028 ["Fraud and related activity in connection with identification documents"] previously addressed only the fraudulent creation, use, or transfer of identification documents, and not theft or criminal use of the underlying personal information. The Act criminalizes fraud in connection with unlawful theft and misuse of personal identifying information itself, regardless of whether it appears or is used in documents.

Subsection 1028(c)(3), as amended, provides that the circumstances under which an offense will be established now include instances in which the production, transfer or use prohibited by this section is in or affects interstate or foreign commerce; or the means of identification, identification document, false identification document or document-making implement is transported in the mail in the course of the production, transfer, possession or use prohibited by the section. In December 2000, this subsection was further amended to include transfers by electronic means and Subsection 1028(d) was amended by defining "transfer" to include selection or placement of such documents or implements on an online location.

Section 3 of the Act amends 18 U.S.C. §1028 by, among other things, adding new Subsection (a)(7). That subsection establishes an offense by anyone who "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

The Act amends the penalty provision of Subsection 1028(b) by extending its coverage to offenses under new Subsection 1028(a)(7). Violations of Section 1028 are generally subject to a fine and imprisonment of up to fifteen years, or both, with several exceptions. When an individual commits an offense "that involves the transfer or use of one or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any one year period," 18 U.S.C. 1028(b)(1)(D) provides for a penalty of imprisonment of not more than fifteen years, a fine or both. Subsection 1028(b)(2)(B) provides for imprisonment of not more than three years and/or a fine for other offenses under the new Subsection 1028(a)(7). Thus, the Act applies more stringent penalties for identity thefts whose purpose is to obtain property.

Subsection 1028(b)(3), as amended, provides that if the offense is committed to facilitate a drug trafficking crime, or in connection with a crime of violence, or is committed by a person whose prior conviction under this section has become final, the individual can be subject to a fine or imprisonment of up to twenty years, or both. The Act also adds a forfeiture provision under new Subsection 1028(b)(5) which allows proceedings to forfeit "any personal property used or intended to be used to commit the offense." Subsection 1028(g) provides that forfeiture procedures are governed by the provisions of Section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. §853).

Subsection 1028(d)(4), as amended, defines "means of identification" broadly to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." It gives several specific examples, such as name, social security number, date of birth, and government issued driver's license, as well as unique biometric data, such as fingerprints, voice print, retina or iris image, or other physical representation. It also covers unique electronic identification numbers, and telecommunication identifying information or access devices.

Subsection 1028(d)(1), as amended, modifies the definition of "document-making implement" to include computers and software specifically configured or primarily used for making identity documents. The Act is intended to cover a variety of individual identification information that may be developed in the future and utilized to commit identity theft crimes. This subsection was further amended in December 2000 to expressly include in the definition the terms "template, computer file and computer disc."

The Act amends Section 1028 by adding Subsection 1028(f), which makes attempts and conspiracies to violate Section 1028 subject to the same penalties as those prescribed for substantive offenses under Section 1028.

**B. Fraudulent access to financial information [Gramm-Leach-Bliley Act of 1999]**

In yet another effort to address the problem of identity theft, in 1999, Congress passed The Fraudulent Access to Financial Information subchapter of the "Gramm-Leach-Bliley Act of 1999" (GLBA), 15 U.S.C. §§ 6821-27 which contains, among other things, specific prohibitions against obtaining financial institution customer information by means of false pretenses (pretext calling or pretexting) and directs federal banking regulatory agencies to ensure that financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information.

The GLBA prohibits the making of false, fictitious or fraudulent statements to an officer, employee or agent of a financial institution, or to a customer of a financial institution, in an effort to obtain, or attempt to obtain "customer information of a financial institution relating to another person". 15 U.S.C. § 6821(a). Financial institutions are defined as "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution." Certain financial institutions, such as brokerage firms, insurance companies, credit card issuers, etc. are specifically included in the definition. 15 U.S.C. §6827 (4). "Customer information of a financial institution" is defined as "any information maintained by or for a financial institution which is derived from the relationship between the financial institution and a customer of the financial institution and is identified with the customer". 15 U.S.C. § 6827(2). In addition, the GLBA prohibits any person from obtaining such customer information by "providing any document to an officer, employee or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation." 15 U.S.C. § 6821(a)

The GLBA also prohibits anyone from requesting a person "to obtain customer information of a financial institution, knowing that

the person will obtain, or attempt to obtain, the information from the institution in any manner described in subsection (a)." 15 U.S.C. §6821(b).

These provisions are directed at "pretext calling", where callers use bits of personal information they have obtained from other sources to impersonate a bank customer, in order to gain access to that individual's account information. The caller may use this personal information, such as the individual's name, address, social security number, or mother's maiden name, to convince a bank's employee to provide confidential account information. This confidential account information may then be used in an identity theft scheme, or be sold to debt collection agencies, attorneys, and private investigators.

The GLBA specifies that it does not apply to actions by law enforcement agencies, financial institution use in certain circumstances, insurance institutions for investigation of insurance fraud, and collection actions for child support. 15 U.S.C. § 6821(c)-(f).

The GLBA provides for a criminal penalty of imprisonment of not more than five years and a fine for "[w]hoever knowingly and intentionally violates, or knowingly and intentionally attempts to violate section 6821...." 15 U.S.C. § 6823(a). If a person violates Section 6821 while violating another United States law, or as a part of a pattern of criminal activity involving more than $100,000 in a twelve month period, he is subject to an enhanced fine of twice the amount provided in Section 6823(a) and imprisonment for not more than ten years or both. 15 U.S.C. §6823(b).

The GLBA also requires Federal banking agencies, the Securities and Exchange Commission, and self regulatory organizations to review regulations and guidelines applicable to financial institutions under their jurisdiction and prescribe such revisions as may be necessary to ensure that these institutions have in place requisite policies, procedures, and controls to prevent the unauthorized disclosure of customer financial information and deter and detect activities prohibited by Section 6821. 15 U.S.C.§ 6825. Administrative enforcement by the Federal Trade Commission and other regulatory agencies is also provided by the Act. 15 U.S.C. § 6822.

**C. The Sentencing guidelines**

Section 4 of the Identity Theft Assumption and Deterrence Act of 1998 directs the United States Sentencing Commission to review and amend the Sentencing Guidelines to provide appropriate penalties for each offense under Section 1028. The Commission completed its review and issued Sentencing Guidelines amendments that became effective November 1, 2000. The Department of Justice and the Identity Theft Subcommittee assisted the staff of the Sentencing Commission in this review.

One such amendment provides for a two level increase in the offense level in cases involving, *inter alia*, "the unauthorized transfer or use of any means of identification unlawfully to produce any other means of identification" or "the possession of five or more means of identification that unlawfully were produced from another means of identification or obtained by the use of another means of identification." U.S. Sentencing Guidelines Manual §2F1.1(b)(5) (2000). This new subsection sets a minimum offense level of twelve. *Id*.

Another such amendment is the addition of Application Note 16 to USSG §2F1.1 which states that an upward departure may be warranted "in a case involving unlawfully produced or unlawfully obtained means of identification . . . if the offense level does not adequately address the seriousness of the offense." Examples given are where:

> (A) The offense caused substantial harm to the victim's reputation or credit record, or the victim suffered a substantial inconvenience related to repairing the victim's reputation or a damaged credit record.
>
> (B) An individual whose means of identification the defendant used to obtain unlawful means of identification is erroneously arrested or denied a job because an arrest record has been made in the individual's name.

(C) The defendant produced or obtained numerous means of identification with respect to one individual and essentially assumed that individual's identity.

U.S. Sentencing Guidelines Manual §2F1.1 (2000), comment. (n.16).

**IV. Victim notification**

Perhaps one of the most enormous tasks in prosecuting identity theft cases is the notification of victims. "Victims" include both the financial institutions that suffer monetary losses and the persons whose identities were stolen. There may be hundreds of such individual victims and, to make matters worse, many of them will not know that their identities have been stolen until they are notified by your office. Thus, if you have an identity theft case, bring your Victim/Witness Coordinator on board immediately.

Section 5 of the Identity Theft and Assumption Deterrence Act directs the FTC to establish a procedure to log in and acknowledge receipt of complaints from individuals who believe one or more of their means of identification have been assumed, stolen, or otherwise unlawfully acquired in violation of the Act, to provide educational materials to these individuals, and refer the complaints to appropriate entities, including the three major national credit reporting bureaus and appropriate law enforcement agencies.

Victims of identity theft should be encouraged to report their complaints to the FTC for filing in its secure victim database. These victims may need assistance in determining additional steps they should take to ameliorate the damage to their credit, reputation, or for other personal considerations. Victims should be referred to the FTC for assistance in addressing their problems and for filing complaints by telephone on the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338) or online at www.consumer.gov/idtheft. The FTC also has developed a consumer guide for the public on identity theft, ID Theft, When Bad Things Happen to Your Good Name, explaining steps that identity theft victims can take to inform credit reporting agencies, credit issuers, law enforcement authorities, and other agencies of the improper use of their identification information. The guide provides the public with educational information, including preventive measures that can be taken to minimize the risk of becoming victims of identity theft.

The Criminal Division's Fraud Section has prepared a form indictment and model jury instructions for Section 1028(a)(7) offenses, which will be available on USA Book.❖

**ABOUT THE AUTHOR**

❑**Beth Moskow-Schnoll** is an Assistant United States Attorney for the District of Delaware. She is a member of the Financial Crimes and Identity Theft Working Group in the District of Delaware, a group comprised of federal, state, and local law enforcement. Ms. Moskow-Schnoll also is a member of a national working group sponsored by the United States Postal Inspection Service and comprised of federal law enforcement and financial institution fraud investigators whose goal it is to develop a best practices guide for financial institutions doing business over the Internet.✠

# Prosecuting Offenses Under the Access Device Statute (18 U.S.C. § 1029)

*Jonathan J. Rusch*
*Special Counsel for Fraud Prevention*
*Fraud Section*

"Symbols," the theologian Paul Tillich once wrote, "have one characteristic in common with signs; they point beyond themselves to something else." Paul Tillich, Dynamics of Faith (1958). One characteristic of modern life is its substantial dependence on symbolic data combinations of numbers and letters, as devices that point to and control access to funds, credit, and other valuable personal data. Particularly with the growth of mail-order, telephone-order, and Internet-related sales, many symbolic data (e.g., bank account numbers, credit card numbers, personal identification numbers or "PINs", and computer passwords) can be easily used in lieu of physical mechanisms, such as door keys or plastic cards, to obtain such access.

These same features, ease of use and lack of dependence on physical mechanisms, can also make it easier for criminals to acquire, transfer, and use credit card and other symbolic data for a wide range of illegal activities that often span state or international boundaries. As a result, crimes such as telemarketing fraud, Internet fraud, identity theft, and use of "cloned" cell telephones have increasingly become concerns for law enforcement authorities in many countries.

A statute that can be particularly useful in prosecuting criminal ventures of this type is 18 U.S.C. § 1029, popularly known as the "access device statute." First enacted in 1984, and amended six times since then, section 1029 contains ten separate subsections that define specific criminal offenses. As this article will show, section 1029 can be a highly versatile means of investigating and prosecuting different aspects of criminal activity that involve fraud. If the mail fraud statute is, as a former Assistant United States Attorney (now a federal judge) put it, "the Colt 45" of white-collar crime prosecutors, Jed S. Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 DUQ. L. REV. 771(1980), the access device statute may be their Swiss Army knife.

This article will first review some of the key terms and concepts in section 1029. It will then address each of the substantive offenses in that section and examine various sentencing issues that can arise in section 1029 prosecutions.

**I. Key terms and concepts**

Before turning to specific offenses within section 1029, it is important to understand some of the key terms and concepts that appear in many of those sections. The most important of these is the term "access device." Subsection 1029(e)(1) defines "access device" broadly as

> any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument) . . . .

As the terms within this definition make clear, the general ambit of section 1029 extends not only to physical cards or plates bearing account numbers, such as credit cards and bank cards, but to any numbers or nonnumeric identifiers (e.g., passwords) that can be used to obtain money or things of value or to initiate nonpaper transfers of funds.

Appellate courts have ruled that the term "access device" includes things as diverse as validated airline tickets (*United States v. Abozid*, 257 F.3d 191, 195-97 (2d Cir. 2001)); a blank credit card, where the defendant also possessed card embossing equipment and card numbers (*United States v. Nguyen*, 81 F.3d 912, 914-15

(9th Cir. 1996)); long-distance telephone service access codes (*United States v. Brewer*, 835 F.2d 550, 553 (5th Cir. 1987)); the number of a merchant account at a bank that was used to process credit card transactions (*United States v. Dabbs*, 134 F.3d 1071, 1079 (11th Cir. 1998)); and restaurant checks with credit card numbers imprinted on them (*United States v. Caputo*, 808 F.2d 963, 966 (2d Cir. 1987)).

Two other terms that are directly dependent on the meaning of "access device" are "counterfeit access device" and "unauthorized access device." "Counterfeit access device" is defined as "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device." 18 U.S.C. § 1029(e)(2). The Fifth and Ninth Circuit Courts of Appeals have ruled that the term "counterfeit access device" as used in section 1029 encompasses otherwise legitimate credit cards that are acquired through the submission of false information. *United States v. Soape*, 169 F.3d 257, 262-64 (5th Cir. 1999); *United States v. Brannan*, 898 F.2d 107, 109 (9th Cir. 1990). The Fifth Circuit also held that long distance telephone service access codes fabricated by the defendant can be "counterfeit" even though those codes matched valid code numbers in the telephone company's computer. *Brewer*, 835 F.2d at 553-54. Similarly, the United States Court of Appeals for the Eighth Circuit held that American Express account numbers that the defendant obtained by surreptitiously accessing the American Express computer system may be considered "unauthorized access devices." *United States v. Taylor*, 945 F.2d 1050, 1051 (8th Cir. 1991).

"Unauthorized access device" is defined as "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud." 18 U.S.C. § 1029(e)(3). The United States Court of Appeals for the Eleventh Circuit held that merchant account numbers which a defendant uses in furtherance of a fraud scheme can be considered "unauthorized access devices," where the merchant bank prohibited the practice of "factoring" (i.e., a business's use of another's merchant account to process credit card transactions) and the defendant knew of, and intentionally violated, the bank's policy. *Dabbs*, 134 F.3d at 1080-81. The United States Court of Appeals for the First Circuit held that the term "unauthorized access device" includes credit cards that the defendant had obtained on her late father's account and proceeded to use after she was told that the company required a power of attorney authorizing her to use those accounts. *United States v. Goodchild*, 25 F.3d 55, 60 (1st Cir. 1994).

It is important to note that section 1029 generally addresses each of the major phases in the stream of criminal activity that exploits access devices, including unlawful acquisition, production, trafficking in, use, and possession of access devices. The term "produce," for example, "includes design, alter, authenticate, duplicate, or assemble." 18 U.S.C. § 1029(e)(4). The term "traffic" is defined to mean "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. § 1029(e)(5).

One of the essential elements in proving any section 1029 offense is that the offense in question "affects interstate or foreign commerce." 18 U.S.C. § 1029(a). To date, courts have construed this requirement expansively to affirm the broad ambit of section 1029. The United States Court of Appeals for the Ninth Circuit held that a defendant's illicit possession of out-of-state credit card account numbers is an offense "affecting interstate or foreign commerce" within the meaning of section 1029. *United States v. Rushdan*, 870 F.2d 1509, 1514 (9th Cir. 1989). In a similar vein, the United States Court of Appeals for the Sixth Circuit held that a fraudulent credit card transaction affects interstate commerce, for purposes of section 1029, inasmuch as banking channels were used for gaining authorization approval of the charges. *United States v. Scartz*, 838 F.2d 876, 879 (6th Cir. 1988). The United States Court of Appeals for the Fourth Circuit held that even an interstate telephone call by a bank manager to a credit card authorization center concerning the defendant's attempt to secure a cash advance on a credit card, was sufficient, in and of itself, to establish the effect on interstate commerce under section 1029. *United States v. Lee*, 818 F.2d 302, 305-06 (4th Cir. 1987). On the other hand, the United States

Court of Appeals for the Third Circuit held that failure to allege the interstate commerce element of a section 1029 violation created a jurisdictional defect requiring reversal of the defendant's conviction. *United States v. Spinner*, 180 F.3d 514, 516 (3d Cir. 1999).

**II. Substantive offenses**

The ten subsections of section 1029 that define criminal offenses fall into three broad categories: (1) offenses generally concerning fraud and access devices; (2) offenses more specifically concerning fraudulent use of telecommunications instruments and service; and (3) attempts and conspiracies to commit any of those offenses. This section of this article will first examine the seven subsections under the first category, then turn to the three subsections under the second category and then the two provisions under the third category.

*Offenses Concerning Fraud and Access Devices*

a. *Subsection 1029(a)(1)*. This subsection states that whoever "knowingly and with intent to defraud produces, uses, or traffics in one or more unauthorized access devices" commits a federal offense if the offense affects interstate or foreign commerce. This offense does not require proof of direct contact between the issuer and the defrauder. *United States v. Jacobowitz*, 877 F.2d 162, 165-66 (2d Cir. 1989).

b. *Subsection 1029(a)(2)*. This subsection states that whoever "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period" commits a federal offense if the offense affects interstate or foreign commerce. The term "one-year period" in this subsection is not limited to a single calendar year, but includes any continuous one-year period within which the defendant has obtained anything of value aggregating $1,000 or more.

This offense may apply in a wide range of circumstances relating to fraud schemes. Examples would be a criminal who takes a credit card receipt from a trash basket at a restaurant, or uses email to Internet users to persuade them to disclose their credit card numbers, and then uses those numbers to purchase merchandise such as computers or other electronic equipment. Another example would be a criminal in a large scale telemarketing or investment scheme who needs a merchant account at a bank to process credit card charges, but cannot get one if he were to describe his activity truthfully. He instead uses another business's merchant account to process charges but does not disclose to the bank that he is using the account without the bank's authorization or approval. *See Dabbs*, 134 F.3d at 1079-81.

One court of appeals held that this offense establishes a separate criminal violation for the use of each unauthorized access device for which $1,000 of value was obtained during the one-year period. In its view, the "one or more" language of this subsection was meant to cover situations in which "multiple unauthorized access devices were required in conjunction with each other to complete a fraudulent transaction." *United States v. Iredia*, 866 F.2d 114, 120 (5th Cir. 1989) (per curiam).

c. *Subsection 1029(a)(3)*. This subsection states that whoever "knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices" commits a federal offense if the offense affects interstate or foreign commerce. This offense may apply, for example, to a person participating in a credit card fraud scheme who has in his possession fifteen or more lost or stolen credit cards, or credit card numbers obtained from e-commerce websites or emails from consumers. It may also apply to a criminal who obtains 100 credit card numbers by "hacking" into a computer, and then offers to sell others a list of those numbers.

The United States Court of Appeals for the Ninth Circuit held that under this offense, the United States needs to prove only that the aggregate possession of fifteen or more unauthorized access devices affected interstate commerce, and not that each of the access devices had an interstate nexus. *United States v. Clayton*, 108 F.3d 1114, 1118 (9th Cir. 1997). In addition, the Fifth Circuit held that a defendant could be convicted of possessing fifteen or more unauthorized long-distance telephone service

access codes, even though only five of the codes were working. The Court of Appeals reasoned that requiring each code number that the defendant possessed to be active as a prerequisite for conviction "would serve as a disincentive to credit card or long-distance telephone companies immediately to invalidate stolen or lost numbers to protect themselves." *Brewer*, 835 F.2d at 554. Two decisions by the United States Court of Appeals for the Eighth Circuit indicate that the government may not aggregate separate possessions of fewer than fifteen stolen credit cards under this offense, but may aggregate fifteen or more unauthorized credit cards, even if those cards were not used at the same moment in time, so long as the defendant did not dispose of any card numbers after his unauthorized use. *Compare United States v. Russell*, 908 F.2d 405, 406-07 (8th Cir. 1990) *with United States v. Farkas*, 935 F.2d 962, 967 (8th Cir. 1991).

d. *Subsection 1029(a)(4)*. This subsection states that whoever "knowingly and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment" commits a federal offense if the offense affects interstate or foreign commerce. Section 1029 further defines the term "device-making equipment" as "any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device." 18 U.S.C. § 1029(e)(6). One court of appeals held that a tumbling cellular telephone, which permits the user to access telecommunications services without paying for them, was not "device-making equipment" within the meaning of this offense, as the telephone was designed and primarily used to make calls rather than to make access devices. *United States v. Morris*, 81 F.3d 131, 134 (11th Cir. 1996). Cloned cell phones and similar or related devices are now clearly covered, *inter alia*, under subsections 1029(a)(7)-(9), as discussed below.

e. *Subsection 1029(a)(5)*. This subsection states that whoever "knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000" commits a federal offense if the offense affects interstate or foreign commerce. As in subsection 1029(a)(2), the term "one-year period" in this subsection is not limited to a single calendar year, but includes any continuous one-year period within which the defendant has obtained anything of value aggregating $1,000 or more.

This offense may apply, for example, when a criminal involved in any kind of fraud scheme (such as telemarketing fraud, investment fraud, or credit protection fraud) persuades a person with a valid credit card number to give the criminal that credit card number because the person believes that he or she will receive something of substantial value in return. It may also apply when a criminal involved in a credit card scheme over the Internet fraudulently obtains individuals' valid credit card numbers and uses them to make purchases of high value consumer goods from e-commerce Web sites.

f. *Subsection 1029(a)(6)*. This subsection states that whoever

> without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of –
>
> (A) offering an access device; or
>
> (B) selling information regarding or an application to obtain an access device

commits a federal offense if the offense affects interstate or foreign commerce. This offense may apply, for example, to persons in a telemarketing or Internet-based fraud scheme who contact consumers to offer them credit cards, but then obtain advance fee payments and either fail to provide the promised credit cards at all or send the consumers generic information about applying for credit cards. In this type of case, it may be important to present testimony from the relevant credit card issuer that the persons soliciting consumers were not authorized to do so or to use the name of the issuer or association to which that issuer belongs (e.g., Visa) in their solicitations.

g. *Subsection 1029(a)(10)*. This subsection states that whoever "without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the

member or its agent, for payment, 1 or more evidences or records of transactions made by an access device" commits a federal offense if the offense affects interstate or foreign commerce. Within this definition, the term "credit card system member" means "a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system." 18 U.S.C. § 1029(e)(7).

This offense may apply, for example, when a criminal operating a large scale fraud scheme has used false information about his business to obtain a merchant account from a bank, or uses an existing account of a legitimate business, so that he can process credit card charges through that account. The criminal then obtains credit card numbers from the victims of his scheme and submits those numbers for payment to the bank where the merchant account is located. If the financial institution that established the merchant account did not authorize that account to be used by telemarketing operations, all transactions that the criminal conducts through that merchant account may be considered "unauthorized" by that financial institution.

*Offenses Relating to Fraud and Telecommunications Instruments and Service*

During the early 1990s, several courts ruled that "cloned" cell phones or satellite television descramblers did not come within the meaning of "access device" in section 1029. Consequently, in 1994 and 1998, Congress added three new subsections to section 1029 to address modified or altered telecommunications instruments, scanning receivers, and hardware and software to modify or alter telecommunications instruments.

a. *Subsection 1029(a)(7)*. This subsection states that whoever "knowingly and with intent to defraud uses, produces, traffics in, has custody or control of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications service" commits a federal offense if the offense affects interstate or foreign commerce. While section 1029 does not specifically define the term "telecommunications instrument," that term clearly extends to both hardwire and cellular telephones, and to any other category of electronic device by which someone may obtain "telecommunications service."

Section 1029 elsewhere defines "telecommunications service" to have the meaning given that term in Section 3 of Title I of the Communications Act of 1934, 47 U.S.C. § 153. 18 U.S.C. § 1029(e)(9). Section 3 of the 1934 Communications Act defines "telecommunications service" to mean "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(46). Section 3 further defines "telecommunications" as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." 47 U.S.C. § 153(43). This offense may apply, for example, to persons who make, distribute, or use "cloned" cell phones in the course of a scheme to defraud, such as a telemarketing fraud scheme, or in connection with another criminal enterprise.

b. *Subsection 1029(a)(8)*. This subsection states that whoever "knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver" commits a federal offense if the offense affects interstate or foreign commerce. As used in that subsection, the term "scanning receiver" is elsewhere defined in section 1029 as "a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 (of Title 18 – i.e., Title III of the Omnibus Crime Control and Safe Streets Act of 1968) or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument." 18 U.S.C. § 1029(e)(8).

c. *Subsection 1029(a)(9)*. This subsection states that whoever "knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunications identifying information associated with or contained in a

telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization" commits a federal offense if the offense affects interstate or foreign commerce. As used within that subsection, the term "telecommunications identifying information" is elsewhere defined in section 1029 as "electronic serial number or other number that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument." 18 U.S.C. § 1029(e)(11).

Two other provisions of section 1029 specifically limit the ambit of subsection 1029(a)(9). First, subsection 1029(g)(1) states that "[i]t is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person engaged in business with, a facilities-based carrier, to engage in conduct (other than trafficking) otherwise prohibited by that subsection for the purpose of protecting the property or legal rights of that carrier, unless such conduct is for the purpose of obtaining telecommunications service provided by another facilities-based carrier without the authorization of such carrier." 18 U.S.C. § 1029(g)(1). The term "facilities-based carrier" is elsewhere defined in section 1029 as "an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934." 18 U.S.C. § 1029(e)(10).

Second, subsection 1029(g)(2) states that "[i]n a prosecution for a violation of subsection (a)(9), it is an affirmative defense (which the defendant must establish by a preponderance of evidence) that the conduct charged was engaged in for research or development in connection with a lawful purpose."

*Attempts and Conspiracies Under Section 1029*

Subsection 1029(b)(1) makes an attempt to commit an offense under section 1029 subject to the same penalties as those which section 1029 prescribes for the offense that the defendant attempted. Subsection 1029(b)(2) does not create a new offense of conspiracy to commit an offense under section 1029. The general conspiracy offense, 18 U.S.C. § 371, should therefore be used to charge a conspiracy to violate section 1029. As explained below, however, subsection 1029(b)(2) defines the maximum penalties for anyone who "is a party to a conspiracy of two or more persons" to commit an offense under section 1029. 18 U.S.C. § 1029(b)(2).

Nothing in section 1029 prohibits "any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of [title 18 – i.e., protection of witnesses]." 18 U.S.C. § 1029(f). This subsection further defines the term "State" to include "a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States." *Id.*

**III. Sentencing for Section 1029 offenses**

Subsection 1029(c) establishes a two-tier system of penalties for convictions under section 1029 for first and repeat offenders. Subsection 1029(c)(1)(A) states that "in the case of an offense that does not occur after a conviction for another offense under this section," the maximum punishment for offenses under subsections 1029(a)(1), (2), (3), (6), (7), or (10) is ten years imprisonment, a fine under Title 18, or both, and the maximum punishment for offenses under subsections 1029(a)(4), (5), (8), or (9) is fifteen years imprisonment, a fine or both. Subsection 1029(c)(1)(B) states that "in the case of an offense that occurs after a conviction for another offense under this section," the maximum punishment for all section 1029 offenses is twenty years imprisonment, a fine under Title 18, or both.

Whether the section 1029 offense is a first or subsequent offense, section 1029 also provides for criminal forfeiture to the United States "of any personal property used or intended to be used to commit the offense." 18 U.S.C. § 1029(c)(1)(C). Forfeiture of property under section 1029, including any seizure and disposition of the property and any related administrative and

judicial proceeding, is governed by section 413 of the Controlled Substance Act, except for subsection (c) of that Act. 18 U.S.C. § 1029(c)(2).

Finally, with respect to a conspiracy to commit a section 1029 offense, subsection 1029(b)(2) states that

> [w]hoever is a party to a conspiracy of two or more persons to commit an offense under [section 1029], if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection [1029(c)] or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection [1029(c)], or both.

This provision will apply in lieu of the general punishment provisions in section 371, if the object of the conspiracy is to violate section 1029.

Under the current version of the United States Sentencing Guidelines (USSG), the relevant Guideline for all section 1029 offenses is section 2F1.1. Under the substantially revised Guidelines scheduled to take effect November 1, 2001, the relevant Guideline for all section 1029 offenses will be a new section 2B1.1, which essentially consolidates the current theft and fraud Guidelines under sections 2B1.1 and 2F1.1, respectively. (Unless otherwise specified, references to the Guidelines in this section of the article will pertain to the Guidelines scheduled to take effect on November 1. A copy of the Guidelines revisions is available online at http://www.ussc.gov/2001guid/congress2001.PDF.

USSG subsection 2B1.1(b)(1), like the current section 2F1.1, generally requires a calculation of loss with reference to a loss table. While prosecutors should note that the section 2B1.1 table contains some differences from the current section 2F1.1 table, they also will need to take into account special rules that apply in section 1029 cases. Application Note 7(F) for USSG section 2B1.1 sets forth the following special rules for stolen and counterfeit credit cards and access devices and purloined numbers and codes:

> In a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than $500 per access device. However, if the unauthorized access device is a means of telecommunications access that identifies a specific telecommunications instrument or telecommunications account (including an electronic serial number/mobile identification number (ESN/MIN pair), and that means was only possessed, and not used, during the commission of the offense, loss shall be not less than $100 per unused means. For purposes of this subdivision, 'counterfeit access device' and 'unauthorized access device' have the meaning given those terms in Application Note 7(A).

USSG § 2B1.1, Application Note 7(F)(i).

Under Application Note 7(A), the term "unauthorized access device" is defined to have the meaning given that term in subsection 1029(e)(3). The Application Note's definition of "counterfeit access device," however, is significantly broader than section 1029's definition of that term. Under Application Note 7(A), "counterfeit access device" has the meaning given in subsection 1029(e)(2), but also "includes a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications service." The Note defines "telecommunications service" to have the meaning given that term in subsection 1029(e)(9). This broader definition brings offenses under subsection 1029(a)(7) within the scope of USSG section 2B1.1.

In addition to calculating loss under USSG section 2B1.1(b)(1), prosecutors should consider the number of access devices involved in the defendant's conduct. USSG subsection 2B1.1(b)(2) requires application of the greater of: (a) a two level enhancement if the offense involved more than ten but fewer than fifty victims, or was committed through mass marketing (e.g., telemarketing or the Internet), or (b) a four level enhancement if the offense involved fifty or more victims. USSG § 2B1.1(b)(2)(A), (B).

USSG subsection 2B1.1(b)(9) pertains specifically to section 1029 offenses. This subsection provides an additional two level enhancement

> [i]f the offense involved (A) the possession or use of any device-making equipment; (B) the production or trafficking of any unauthorized access device or counterfeit access device; or (C)(i) the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification; or (ii) the possession of 5 or more means of identification that unlawfully were produced from, or obtained by the use of, another means of identification . . . . If the resulting offense level is less than 12, increase to 12.

USSG § 2B1.1(b)(9)

Application Note 7 has several provisions that help to define the ambit of USSG subsection 2B1.1(b)(9):

a. *Subsection 2B1.1(b)(9)(A).* Application Note 7(A) defines the term "device-making equipment" not only to have the meaning given that term in section 1029(e)(6), but also to include "(I) any hardware or software that has been configured as described in [subsection] 1029(a)(9); and (II) a scanning receiver referred to in [subsection] 1029(a)(8)." USSG § 2B1.1, Application Note 7(A). The Note also provides that the term "scanning receiver" has the meaning given that term in subsection 1029(e)(8). *Id.* This broader definition brings offenses under subsection 1029(a)(8) and (a)(9) within the scope of USSG section 2B1.1.

b. *Subsection 2B1.1(b)(9)(B).* Application Note 7(A) defines the terms "produce" and "production" to include "manufacture, design, alteration, authentication, duplication, or assembly." This definition adds the word "manufacture" to the list of terms used to define "produce" in subsection 1029(e)(4). The terms "counterfeit access device" and "unauthorized access device" are defined as specified above.

c. *Subsection 2B1.1(b)(9)(C).* Although the term "means of identification" is statutorily defined in the identity theft offense (18 U.S.C. § 1028(a)(7)) rather than the access device statute, section 1028 defines "means of identification" to include the term "access device" as defined in subsection 1029(e). This means that each of the bases for enhancement under USSG subsection 2B1.1(b)(9) may be applicable in sentencing for section 1029 offenses. However, Application Note 7(A) states that "means of identification" has the meaning given that term in subsection 1029(e)(6), with the proviso that "such means of identification shall be of an actual (*i.e.*,, not fictitious) individual, other than the defendant or a person for whose conduct the defendant is accountable under § 1B1.3 (Relevant Conduct)." USSG § 2B1.1, Application Note 7(A).

Application Note 7 contains four provisions that further define the ambit of USSG subsection 2B1.1(b)(9)(C)(i). First, Application Note 7(C) states that subsection 2B1.1(b)(9)(C)(i)

> applies in a case in which a means of identification of an individual other than the defendant (or a person for whose conduct the defendant is accountable under § 1B1.3 (Relevant Conduct)) is used without that individual's authorization unlawfully to produce or obtain another means of identification.

USSG § 2B1.1, Application Note 7(c)(i)

Second, Note 7(C) gives two examples of conduct to which subsection (b)(9)(C)(i) applies:

> (I) A defendant obtains an individual's name and social security number from a source (e.g, from a piece of mail taken from the individual's mailbox) and obtains a bank loan in that individual's name. In this example, the account number of the bank loan is the other means of identification that has been obtained unlawfully.
>
> (II) A defendant obtains an individual's name and address from a source (e.g., from a driver's license in a stolen wallet) and applies for, obtains, and subsequently uses a credit card in that individual's name. In this example, the credit card is the other means of identification that has been obtained unlawfully.

USSG § 2B1.1, Application Note 7(C)(ii).

Third, Note 7(C) gives two examples of conduct to which subsection 2B1.1(b)(9)(C)(i) does not apply:

(I) A defendant uses a credit card from a stolen wallet only to make a purchase. In such a case, the defendant has not used the stolen credit card to obtain another means of identification.

(II) A defendant forges another individual's signature to cash a stolen check. Forging another individual's signature is not producing another means of identification.

USSG § 2B1.1, Application Note 7(C)(iii).

Application Note 7(D) states that subsection 2B1.1(b)(9)(C)(ii) "applies in any case in which the offense involved the possession of 5 or more means of identification that unlawfully were produced or obtained, regardless of the number of individuals in whose name (or other identifying information) the means of identification were so produced or so obtained." USSG § 2B1.1, Application Note 7 (D).

Finally, Application Note 15 lists three factors that a sentencing court may consider in determining whether an upward departure is warranted in a case involving access devices or unlawfully produced or unlawfully obtained means of identification:

(I) The offense caused substantial harm to the victim's reputation or credit record, or the victim suffered a substantial inconvenience related to repairing the victim's reputation or damaged credit record.

(II) An individual whose means of identification the defendant used to obtain unlawful means of identification is erroneously arrested or denied a job because an arrest record has been made in that individual's name.

(III) The defendant produced or obtained numerous means of identification with respect to one individual and essentially assumed that individual's identity.

USSG § 2B1.1, Application Note 15(A)(vii).

**IV. Conclusion**

Section 1029 has far more than symbolic value in prosecuting a wide variety of criminal conduct, whether or not fraud is the principal object of that conduct. The broad scope and variety of the offenses in that section make it one of the more versatile statutes for use in white-collar crime and other prosecutions.❖

**ABOUT THE AUTHOR**

❑**Jonathan J. Rusch** is Special Counsel for Fraud Prevention in the Fraud Section of the Criminal Division. His responsibilities include coordination of the Internet Fraud Initiative, a Department-wide initiative established in 1999 to improve the Department's abilities to combat all forms of Internet fraud. He also serves as Chair of the Interagency Telemarketing and Internet Fraud Working Group. Mr. Rusch is an Adjunct Professor of Law at Georgetown University Law Center, where he teaches courses on Global Cybercrime Law and International and Comparative Law of Cyberspace, and has written several law review articles on various aspects of cyberspace law. He received the Attorney General's Award for Distinguished Service in 1995.✠

# Investigating and Prosecuting Nigerian Fraud

*Jim Buchanan*
*Assistant United States Attorney*
*Southern District of Texas*

*Alex J. Grant*
*Trial Attorney*
*Criminal Division, Fraud Section*

**Introduction**

During the last twenty years, organized crime elements with ties to Nigeria have come to dominate crime emanating from West Africa. These criminal groups, also known as Nigerian Crime Enterprises (NCE's), have become adept at executing transnational criminal activities, including fraud schemes directed to the United States. See *Combating International African Crime: Hearing Before Subcomm. on Africa of House Comm. on Int'l Rel.* (July 15, 1998) (statement of Thomas Kneir, FBI) *available in 1998 WL 400598* [hereinafter *Kneir Statement*]; *Impact of Data-Sharing on National Security: Hearing Before Subcomm. on Nat'l Sec., Vet. Affairs & Int'l Rel. of House Comm. on Govt. Reform* (July 24, 2001) (statement of Bruce Townsend, United States Secret Service), *available in* 2001 WL 870378 [hereinafter *Townsend Statement*].

Nigeria is the largest country in Africa and boasts a population of 100 million people, a rich diversity of languages, customs, and ethnic groups, as well as large oil and gas reserves. However, since gaining full independence from Great Britain in 1960, Nigeria has been plagued by long periods of military rule, and consequently, weak democratic institutions, including an often ineffective and corrupt court system. *See* U.S. Dept. of State, Bureau of African Affairs, *Background Note: Nigeria* (August 2000) (visited Sept. 12, 2001) http://www.state.gov/r/pa/bgn/index.cfm?docid=2836> [hereinafter *Background Note*]; *International Crime in Africa: Hearing Before the Africa Subcomm. on African Organized Crime of House Com. on Int'l Rel.* (July 15, 1998) (statement of Jack A. Blum), *available in* 1998 WL 403633 [hereinafter *Blum Statement*] (noting "non existent criminal justice systems"); *Situation in Africa: Hearing Before Subcomm. on African Affairs of Senate Comm. on For. Rel.* (May 15, 1996) (statement of Jean Herskovits, Prof. of History), *available in* 1996 WL 387276 [hereinafter *Herskovits Statement*]. While most Nigerians are law-abiding people, a yearly per capita income of $300, combined with governmental institutions lacking legitimacy, have helped to spawn organized crime of all types. *See Background Note*; *Blum Statement*; *Herskovits Statement.*

The United States is Nigeria's largest trading partner, and not surprisingly, is the frequent target of drug smuggling and fraudulent schemes by NCE's. NCE's perpetrating fraudulent schemes have proven to be sophisticated and elusive foes. There is no true organized crime structure as is found in more traditional organized crime investigations, although Nigerians do associate along tribal lines. *See Combating International African Crime: Hearing Before Subcomm. on Africa of House Comm. on Int'l Rel.* (July 15, 1998) (statement of Phil Williams, Director, Ctr. for Int'l Sec. Studies, Univ. of Pittsburgh) *available in 1998 WL 400575* [hereinafter *Williams Statement*]. This association is often one of convenience, and many times, the lines between the groups are blurred. There are no clear lines of authority or communication, and tribal lines are crossed with regularity when it is

convenient and profitable. Taken together, these factors make for an investigator's nightmare. The usual organized crime investigative techniques are difficult, if not impossible, to implement in Nigerian cases.

In light of these challenges, federal law enforcement agencies and the Department of Justice have developed specific policy initiatives and have devoted significant resources during the past few years to combating Nigerian fraud schemes and other types of Nigerian organized crime. Part I of this article outlines the most prevalent kinds of Nigerian fraud schemes. Part II describes the multi-agency Nigerian Crime Initiative (NCI), which attempts to provide the infrastructure necessary for investigators and prosecutors to pursue individual cases. Finally, Part III reports on recent cases from the United States Attorney's Office for the Southern District of Texas and the Houston Area Fraud Task Force. The cases suggest how these success stories might be replicated elsewhere.

**I. Types of Nigerian fraud schemes**

According to the Secret Service, one quarter of the major fraud scams it investigates now involve Nigerians. Described as brazen and brilliant, these scams result in the loss of hundreds of millions of dollars each year worldwide. The favorite target of these scam artists is the United States. In the past few years, a significant percentage of the total loss from Nigerian fraud has occurred in the United States, and the amount of loss is expected to continue to grow. *See Townsend Statement.* The frauds take on many forms including dubious business deals with advance fees, insurance scams, health care fraud, credit card fraud, bank fraud, and identity theft.

**A. Advance fee/"419" fraud**

The most notorious of Nigerian scams is the advanced fee fraud scheme known as the "419" scheme, named after a statute in the Nigerian criminal code. This fraud typically begins with an unsolicited letter or e-mail. The communication purports to be from a Nigerian official or ex-official, a doctor or a tribal chief. The letters are addressed personally to a potential victim explaining that a "mutual business associate" has suggested that the writer contact the addressee confidentially. The letter requests the recipient's assistance in transferring large sums of money in exchange for a percentage. The letter almost always represents that: 1) there is a large sum of money, known only to the writer, waiting to be paid out of the government coffers as a result of accounting shenanigans or over invoicing; 2) the writer is a member of the Nigerian government or the Nigerian military trying to move the money out of Nigeria but needs help from abroad; 3) the writer is willing to share the money with the recipient who provides assistance; and 4) secrecy is an absolute must because other corrupt officials would seize the money for themselves if they knew of its existence. The amounts represented are usually in the area of $35 million but may be as much as $75 million. In return for the help of the addressee, the writer promises anywhere from 20% to 30% of the total. In other words, the addressee is offered $7 -10 million for very little effort and virtually no risk.

The vast majority of these letters and e-mails arriving in the United States are promptly deposited into actual or virtual wastebaskets. Hundreds more are forwarded to the United States Postal Service, the F.B.I., or the Secret Service. Sometimes, however, the crooks get lucky. A victim responds with a tiny nibble and the hook is set. The Nigerians are masters of this game and go to great lengths to convince the victim of the legitimacy of the plan. Many times a "disinterested" third party, usually from a European nation, is introduced to lend an air of legitimacy. Sometimes, an important sounding institution becomes a part of the plan.

After a number of communications and an appropriate amount of time, the Nigerian will report that the money is finally available for transfer. Unfortunately, some unforeseen problem arises, and the advance payment of fees is necessary to clear the final hurdle. This is the essence of the fraud. Sometimes, another government official "finds out about the plan" and hush money is needed to bribe him. Other times, it is a transfer fee, or shipping insurance, or "points" for the financial institution or middle man. If the victim sends the money, similar roadblocks will continue to pop up until the victim is out of money or realizes he has been duped.

**B. "Black Money" scheme**

A recent variation on the Advance Fee scheme is known as the "black money" scheme. In this variation, the millions of dollars in the possession of the writer have been defaced by government officials with a chemical which has turned the bills black (a precaution to keep the money safe from thieves or corrupt officials), or by some sort of industrial accident. The writer can have the money shipped to the victim if the victim agrees to front the cash necessary to purchase the chemical to cleanse the money. The writer agrees to send a representative to meet the victim and demonstrate the cleansing process. At the meeting, the representative demonstrates the process by "cleaning" several one hundred dollar bills with what he claims is the last of the chemical. He then pressures the victim to pay money for storage fees, shipping fees, and more of the chemicals to clean the remaining millions of dollars.

Unfortunately, the victims of these 419 schemes typically do not report the crime because they are embarrassed by their naivete and feel personally humiliated. Some even feel they may be criminally liable as a result of their involvement in the scheme.

**C. Access device fraud**

Another Nigerian scheme involves access device fraud, usually in connection with several other federal criminal violations. The fraud typically begins with the leasing of a commercial mail box (usually in a false name). By searching dumpsters or rifling through mailboxes at an apartment complex, the Nigerian thief can obtain fifteen to twenty credit card offers in a matter of minutes. Using the name of the true addressee, but changing the address to his newly acquired commercial postal box, the crook applies for hundreds of credit cards each day. Once the cards begin to arrive, the fraud grows exponentially. Cash advances are obtained. Credit card convenience checks are used to open bank accounts and investment accounts. Checks drawn on the fraudulently opened bank accounts are used to pay down the credit card bills. Even though the checks are fraudulent, the credit card companies are required to give immediate credit on the account. This allows the thief to obtain even more cash advances and open more bank accounts. If investment accounts are used, the accounts are opened with fraudulent items. Once funded, the Nigerian or his recruit forwards a wire transfer order directing the investment company to forward the funds to a bank account under his control.

**D. Identity fraud and credit card fraud**

One credit card is never enough, nor is one identity. The typical Nigerian fraud scheme involves multiple identities, several postal boxes, many bank accounts, and, recently, more than one city. To further decrease his visibility, the Nigerian recruits young Americans to participate in the scams. The lure of fat wallets and expensive automobiles is more than enough to encourage the minimum wage earner to take a chance. With a little coaching, the recruit becomes adept at opening bank accounts and moving the money. If caught, the recruit feigns ignorance or has a canned story about his wallet being stolen.

The Internet has increased the opportunities for the Nigerian criminal while decreasing his exposure. Using computer programs, groups of Nigerians have routinely been able to obtain lists of credit card numbers issued by credit card companies operating in international commerce. The card numbers are issued through foreign banks to customers who are residents of Great Britain, Germany, or other European countries. By fax or phone, the Nigerians use the stolen credit card numbers to order expensive computers or computer parts from small dealers in the United States. The buyer provides the stolen credit card number in payment of the purchase. Most purchases are successful because neither the cardholder nor the credit card company realizes that the card number has been compromised. The purchases are shipped to coconspirators in the United States who repackage the products and ship them to various cities in Europe or to Lagos, Nigeria.

It is not unusual for the Nigerian to open a small retail business such as a clothing resale shop or import/export business. Naturally, to become competitive in our capitalist society, a small businessman must agree to accept credit cards for

payment. In the case of some Nigerian small businessmen, the credit card merchant account becomes merely another tool of fraud. Stolen and counterfeit credit cards are routinely "swiped" through the point of sale terminal, each transaction representing what would appear to the credit card company to be a large purchase. The funds are forwarded from the credit card company to the Nigerian's merchant account to complete the transaction. In reality, no transaction or sale of merchandise took place because there was never any inventory of goods to be sold. Investigation usually shows that the Nigerian businessman, his friends, and relatives acquired by theft and other means, a number of credit card numbers and re-encoded the information onto magnetic strips on the back of plastic blanks. The blank cards are swiped through the terminal during business hours in order to avoid scrutiny.

**E. Bank fraud**

Bank fraud scams orchestrated with stolen and counterfeit checks also comprise a large part of the Nigerian fraud repertoire. Armed with a computer, scanner, desk top publishing program, color printer, and basic computer know how, the Nigerian fraudster can print corporate checks in any dollar amount with an authorizing signature that is virtually identical to the original. By recruiting coconspirators and opening multiple accounts, including some in assumed business names, an enterprising Nigerian fraudster can operate without fear of getting caught.

It is not unusual for a Nigerian fraud perpetrator to recruit a bank insider to provide account information. Employees in a bank's customer service department usually have access to all customer accounts via computer in order to assist customers who have questions or complaints about their accounts. Once the employee finds an account with a large balance, the account information is compromised and forwarded to the Nigerian. Armed with the essential account information, the Nigerian prints checks or issues wire transfer orders directing the bank to transfer large sums into accounts under the control of the Nigerian. Sometimes two or three wire transfers are used to insulate the Nigerian from the transaction.

**II. Resources and policy initiatives**

**A. Nigerian Crime Initiative (NCI)**

The Nigerian Crime Initiative was launched in compliance with the 1995 Presidential Decision Directive 42 (PDD-42), which was aimed at combating international organized crime and which directed agencies to collaborate with each other and foreign governments in order to fight international organized crime more effectively. *See Townsend Statement.* In keeping with this mission, the NCI has helped to develop: (1) an interagency working group in order to share information and help make policy, (2) the Anti-Drug Network (ADNET) computer system for collecting and tracking data relating to Nigerian crime, and (3) Interagency Nigerian Organized Crime Task Forces (INOCTF), which are located in cities where Nigerian crime is more prevalent and investigate local Nigerian Crime Enterprises. *See id.*; *Impact of Data-Sharing on National Security: Hearing Before Subcomm. on Nat'l Sec., Vet. Affairs & Int'l Rel. of House Comm. on Govt. Reform* (July 24, 2001) (statement of Bruce C. Swartz, Deputy Asst. Attorney General), *available in* 2001 WL 846011 [hereinafter *Swartz Statement*].

*1. NCI Working Group*

The NCI working group brings together representatives of every important federal law enforcement agency as well as the Department of Justice and the Department of State. The NCI includes the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Immigration and Naturalization Service (INS), National Drug Intelligence Center (NDIC), U.S. Customs Service (USCS), U.S. Secret Service, Financial Crimes Enforcement Network (FINCEN), IRS - Criminal Investigation Division (IRS-CID), U.S. Marshals Service (USMS), U.S. Postal Inspection Service (USPIS), Department of Defense/Defense Information Systems Agency (DISA). Because Nigerian organized crime is sophisticated and multifaceted, the response to it must draw upon all of the resources of the Federal Government, working in concert. The working group helps to pool information among the law enforcement agencies by discussing the latest issues and ensuring that ADNET is a useful tool

for investigators and prosecutors. The working group tracks the timeliness of data entry, and it educates users on how to use ADNET effectively.

The working group develops policies and plans to combat international Nigerian crime by supporting the task forces. It helps to select task force cities and assures that the task force cities carry out the mission of the NCI. The working group also addresses policy issues, such as privacy and discovery in criminal cases.

*2. ADNET*

ADNET is a computer network with powerful capabilities for the storage and retrieval of data concerning Nigerian crime. ADNET is a secure system and can be accessed through dedicated ADNET terminals in the task force cities. *See Townsend Statement.* In conjunction with the working group, an outside private contractor trains and provides support to investigators working Nigerian crime cases. ADNET terminals are also located in Lagos, Nigeria and Accra, Ghana, so that data can be accessed close to sources of much of the Nigerian crime activities.

Several federal law enforcement agencies contribute and access ADNET data. In the last two years the number of records in the NCI database has increased dramatically, making the network a potentially valuable resource to law enforcement. Some of this data consists of information collected from prior criminal investigations, including aliases used by persons involved in Nigerian criminal activities.

*3. Interagency Nigerian Organized Crime Task Forces*

The Interagency Nigerian Organized Crime Task Forces (INOCTF) consist of several law enforcement agencies in a number of United States cities where NCE activity has been particularly troublesome. INOCTF target NCE's and investigate Nigerian crime, including Nigerian fraud schemes, in a coordinated manner. As noted above, task force cities have access to ADNET terminals, so that data from other cities can be used in investigations. The coordinated NCI approach expects that through information sharing, investigators can spot connections between different types of Nigerian criminal activity. Indeed, experience has shown that NCE's rarely engage in one type of criminal activity to the exclusion of all others. *See Swartz Statement.*

The predecessors to the INOCTF were the Secret Service task forces already in place to counter Nigerian crime. Under the NCI, the Secret Service task forces were transformed into multiagency task forces, but the Secret Service continues to host the task forces. This has allowed the NCI to tap into expertise that has been developed by the Secret Service since the 1980's in areas such as access device fraud.

**B. United States Secret Service website and Financial Crimes Division**

The United States Secret Service was designated in 1998 by the Attorney General as the lead investigative agency for Nigerian crime. Through the Secret Service Internet website, and its Financial Crimes Division in its Washington headquarters, the Secret Service acts as a central repository for complaints about Nigerian fraud. The internet address is http://www.treas.gov/usss [hereinafter *Secret Service Web Site*]. The most commonly reported scheme is the Advance Fee scam, described in Part I. The Secret Service receives hundreds of reports of solicitations on a daily basis concerning Nigerian fraud. *See Electronic Fraud & Identity Theft: Hearing Before Subcomm. on Fin. Serv. & Tech. of Senate Comm. on Banking, Housing & Urban Affairs*, (Sept. 16, 1997) (statement of Dana Brown, U.S. Secret Service) *available in 1997 WL 572487* [hereinafter *Brown Statement*]. Victims of Nigerian fraud can make a report to the Secret Service through the website, through the mail, or by telephone. The Secret Service web site serves as an example for another component of the NCI, namely public education. It informs potential victims of the warning signs of an advance fee scheme and advises them to avoid these "too good to be true" offers.

The Secret Service compiles all of the complaints it receives relating to Nigerian fraud in an investigative database. Where the victim has suffered financial loss, the Secret Service initiates an investigation. For simple solicitations, *i.e.*, where the recipient has not fallen for the scam and has not sustained financial loss, the Secret Service

will save the information for future cases. The database helps to link victims of the same perpetrator, since the fraudster always sends out numerous solicitations and attempts to hook as many victims as possible with the same offer. Proof of these multiple victims is powerful evidence in demonstrating a defendant's fraudulent intent.

**III. Recent cases and analysis**

A number of Nigerian cases have been successfully prosecuted in the Southern District of Texas as a result of aggressive investigation by the Houston Area Fraud Task Force. The task force is comprised of representatives from a number of federal and local law enforcement agencies including the Secret Service, the FBI, the Immigration and Naturalization Service, the Postal Inspection Service, the Houston Police Department, the Harris County Sheriff's Office, the Texas Rangers, the State Department, and the Drug Enforcement Administration. The combination of expertise and assets provided by the representatives of these agencies allows for rapid response to ongoing fraud schemes as well as the ability to work through complicated, long-term fraud investigations.

**A. *United States v. Okonkwo***

After several attempts to arrest Nigerians perpetrating 419 schemes, the Houston task force attained its first success in June 2000 with the arrest of John Okonkwo, Jerome Okwudi, and Kingsley Ireke. This case combined elements of both the advance fee and the black money schemes. The case began in March 2000 when Russell Burris, a New Mexico real estate salesman, responded to an email from "Joy Anan" who purported to live in Cotonou, Republic of Benin. Anan advised that she had been left a large sum of money by her late husband who had been killed in West Africa. Between April 1, 2000 and June 14, 2000, Burris, Anan, and an associate of Anan, exchanged emails over the Internet regarding Anan's desire to have Burris act as a manager/investor for the $15,500,000 left by Anan's late husband. If Burris agreed to be the manager and travel to Cotonou to receive the appointment, he would receive a 5% fee.

Burris received a fax from "Koffi Biyah" of Trans-World Security Company in Cotonou confirming the information provided by Anan and requesting that Burris pay $2,500 to open a "special domiciliary account" and $24,500 for a "Telegraphic Transfer Clearance Certificate." The fax stated that the funds were necessary to effect the transfer of the money to an account of Burris' specification. When Burris requested further explanation, he was advised by fax that the money was needed to expedite the transfer process and to buy the proper "banking permit."

Burris began to receive email communications from "Kite Anan" who purported to be the son of Joy Anan. Kite Anan told Burris that he would need to send $24,000 to Biyah as soon as possible to expedite the transaction and that he would need to bring $2,500 with him to Benin to open the account. Burris also received a fax from Biyah confirming the need for Burris to send the money so that the funds could be released from the vault of Trans-World Security. When Burris refused to travel to Africa, Kite Anan stated that the $15,500,000 could be placed with a Trans-World Security agent in Chicago so that the deal could be consummated in the United States. Burris would pay all transfer and handling charges in Chicago.

On June 14, 2000, Burris received a fax from the "Debt Reconciliation Committee" in Houston, Texas referencing the $15,500,000 and requesting that Burris come to Houston to sign the final release documents for the transfer of the money. The fax stated that Burris would have to pay an $18,000 processing fee and $5,000 for insurance before the funds could be released.

On June 19, 2000, Burris, with Secret Service Agent Tonya Cook posing as his wife, "arrived" in Houston and were met by a limousine driver. They were taken to the Marriott Hotel where a room had been prepared with audio and video equipment to record any subsequent meetings. One hour later, three individuals arrived and two men, dressed in full tribal regalia, went up to the room while the third stayed near the vehicle.

The two men who went to the room stated that they were in possession of $15,500,000 that was being kept at a different location. They stated that

the money had been defaced with some sort of chemical and needed to be cleaned before it could be taken to a bank. They requested the $23,000 be paid immediately. Burris gave the two Nigerians $5,000 in cash and a check in the amount of $18,000. HAFTF agents burst into the room and arrested them.

The third Nigerian was arrested downstairs and his car was impounded and inventoried. Inside a briefcase, agents found an envelope with the name Russell Burris written on it. There was also a piece of paper with five other names and associated telephone numbers along with various dollar amounts written on it. By contacting the individuals, agents found that each of them had paid between $15,000 and $25,000 to the defendants.

All three Nigerians were charged and convicted of conspiracy and inducing another to travel in interstate commerce in furtherance of a scheme to defraud. Crm. No. H-00-4777 (S.D. Tex. 2000.) The videotape proved to be compelling evidence and helped to induce all three defendants to plead guilty. Okonkwo and his two codefendants received sentences ranging from eight to twenty-one months. When they complete their stay at the Bureau of Prisons, they will be released to the INS for deportation proceedings.

**B. *United States v. Okiti***

A second successful investigation of a 419 scheme began in February 2001. The task force was contacted by Lawrence Siler, a businessman in Portland, Oregon. Siler told the task force that he had been contacted by a group of Nigerians requesting that Siler invest a large sum of money on their behalf.

In September 2000, Mr. Siler received a letter via facsimile entitled "Abacha Family Estate." The letter outlined a business proposal in which Dr. Maryam Abacha requested that Siler receive $25.6 million from her to invest in the United States. The letter indicated that the funds were the result of some deal between her late husband and a Russian firm. After the Nigerian government revoked her license to own a financial or oil company, Abacha had removed the funds and packaged it into two trunks. Because of the oppression of the Nigerian government, she supposedly was looking for a way to sneak the money out of Nigeria quickly.

Mr. Siler responded to the letter via email, requesting that the trunks of money be sent to him in Portland. A series of faxes and emails followed with Abacha insisting that Siler travel to Europe to receive the money and pay shipping and insurance costs. Siler refused.

In December 2000, Abacha advised that the money would be in Houston with a family representative named Mohammed and that Siler should contact Mohammed to make arrangements to obtain the trunks containing the money. From December 2000 through March 2001, several telephone calls were placed and recorded between Siler and Mohammed.

On March 11, 2001, Siler arrived in Houston and met with task force members. Agents wired a room at the Marriott Hotel and waited for Mohammed to arrive. Secret Service Agent Alicia Broussard posed as Siler's secretary. "Mohammed" arrived at the hotel bringing two large bags with him. In the room, he opened the bags and told Siler that they contained $6 million each. Inside the bags were numerous individually wrapped stacks of money. The money was stamped with the initials "U.N." According to Mohammed, the "U.N." stamp meant that the money was from the United Nations and could only be used overseas. A special chemical was necessary, according to Mohammed, to clean the money. Mohammed then removed two hundred dollar bills from one of the stacks and cleaned the initials with a small amount of liquid. He stated that he needed $23,000 to purchase additional chemicals to clean the rest of the money. After receiving the money, agents arrested Mohammed and identified him as Victor Okiti. The suitcases were found to contain numerous stacks of cut paper which had counterfeit hundred dollar bills on top and bottom of each stack. The only legitimate currency in the bags were the hundred dollar bills Mohammed had washed during his demonstration.

A search warrant executed at Okiti's residence revealed more suitcases and more counterfeit money. Okiti was charged with wire fraud and possessing counterfeit currency. In the face of videotaped evidence of his crimes, he pled guilty to the charges. Despite the fact that this was a "no loss" case, Okiti received a sentence of thirty-three months in prison, after which he will be deported. Crm. No. H-01-261 (S.D. Tex. 2001).

**C. *United States v. Nwachukwu***

Combining his bank fraud scheme with religion, "Pastor" Christian Nwachukwu engaged in fraud for several years. The investigation began when a local bank contacted members of the task force concerning the deposit of counterfeit checks drawn against accounts at foreign banks. Worthless checks totaling thousands of dollars drawn against a closed account at a London bank had been deposited to the Bank United account of Ty Scearce. Because bank personnel handled the deposited checks as normal items instead of sending them for collection, Scearce's account was immediately credited and the funds represented by the checks were withdrawn before the checks were returned from Great Britain.

The account holder, Ty Scearce, stated that she had been introduced to "Pastor" Christian Nwachukwu by a friend. Nwachukwu had explained to her that depositing checks in her account would help his ministry. She agreed and was supposed to receive $4,000 from the deposits. Her cooperation allowed agents to record her conversations with Nwachukwu and led to his arrest. As he was being arrested, Nwachukwu told an agent that the banks were at fault for not verifying the checks before releasing the money to him. The defendant later moved to suppress this incriminating statement, claiming that he never made it and that law enforcement agents had beaten him. Nwachukwu testified on his own behalf at trial and repeated these allegations, which were refuted by a large number of government witnesses who were in a position to observe the injuries caused by the alleged beating and who saw none of the injuries claimed by the defendant.

Subsequent investigation revealed that Nwachukwu had convinced several other young females to open accounts in their names for his use. All of them had been duped into believing they were somehow assisting his ministry, and the defendant took advantage of this trust by using the accounts to execute his fraudulent scheme, as he did with Ty Searce's bank account. In addition, INS records revealed that Nwachukwu had entered the United States on a student visa to enroll at a ministry school in Tennessee. He was refused enrollment when his application was found to contain several false statements.

Nwachukwu was convicted of bank fraud and money laundering by a jury which rejected his claim of mistreatment by law enforcement agents. He is currently awaiting sentencing with the Sentencing Guidelines placing his sentence in the range of 87-108 months. Crm. No. H-00-781 (S.D. Tex. 2000).

***D. Challenges in Prosecuting Nigerian Fraud Cases***

The successes achieved in Houston can be attributed to the commitment of the various agencies in the task force, the cooperation of the banks and credit card industry, and the United States Attorney's office dedicating a prosecutor to coordinate the prosecution of these cases. Much remains to be done, however, and significant hurdles must be overcome before lasting success against Nigerian fraud can be achieved.

The transnational quality of these cases presents the most fundamental difficulty. Perpetrators meet with their victims, if at all possible, in Nigeria. If a victim travels to Nigeria to obtain the pot of gold promised by the fraudster, not only does the victim face physical danger or death, but finding and arresting the perpetrator is extremely difficult, if not impossible. *See Combating International African Crime: Hearing Before Subcomm. on Africa of House Comm. on Int'l Rel.* (July 15, 1998) (statement of Edward Markey, U.S. Representative) *available in 1998 WL 400600* [hereinafter *Markey Statement*] (reporting that 15 foreign businessmen and two United States

citizens have been murdered in Nigeria in connection with 419 schemes).

Obtaining evidence from Nigeria is an uncertain enterprise because it has been rarely tried, and a Mutual Legal Assistance Treaty (MLAT) is not yet in force. Extradition of fugitives from Nigeria has been difficult, in part because the country is just emerging from military rule and lacks a well established judicial process for the return of fugitives. *See Nigerian White Collar Crime: Hearing Before Subcomm. on Africa of House Comm. on Int'l Rel.* (Sept. 16, 1998) (statement of Mark Richard, Deputy Asst. Attorney General) *available in 1996 WL 517475* [hereinafter *Richard Statement*] ("Nigeria's response to U.S. extradition requests has been very uneven and unreliable"). However, the Department of Justice's Office of International Affairs (OIA) is currently engaged in a dialogue with Nigerian officials about improving the extradition process, and OIA encourages prosecutors to submit fresh extradition requests in order to move this dialogue forward. The Fraud Section has produced a monograph entitled "Prosecuting Nigerian Advance Fee Fraud" which discusses the issues of collecting foreign evidence and extradition in more depth.

Fortunately, when members of NCE's decide to come to the United States, the prospects for success change dramatically, as demonstrated by the recent Houston cases. In *Okonkwo*, investigators with the Houston task force were able to set up a sting operation where the fraudster could be videotaped making his false promises. The agents in *Okonkwo* also obtained valuable documentary evidence from a search of one of the coconspirators namely, a piece of paper with the names of other victims. This type of evidence is powerful proof of a defendant's scheme and intent to defraud. It also impacts the defendant's sentence under the Sentencing Guidelines as relevant conduct.

Even when Nigerian fraudsters travel to the United States and "smoking gun" evidence is obtained, it is difficult to do lasting damage to the NCE itself. Leaders of the NCE tend not to travel to the United States and meet victims. This task often is left to low-level members of the organization, and the prosecution of the crime bosses is frustrated by the problems involved in obtaining evidence and extradition from Nigeria. Moreover, because NCE's tend to organize around tribal relationships, it is difficult to infiltrate an NCE with an undercover agent who does not belong to the requisite tribe. These difficulties present investigators and prosecutors with a substantial and continuing challenge in the fight against Nigerian fraud. Toppling NCE's will require greater assistance from foreign governments and the use of innovative investigative techniques by law enforcement.

## IV. Conclusion

While Nigerian fraud schemes are pervasive and have been aided by the growth of the Internet, they remain for the most part, brazen and almost transparently fraudulent. These repetitious and seemingly outlandish scams continue to lure United States citizens looking to strike it rich. Investigating and prosecuting Nigerian fraud in a coordinated fashion, as demonstrated by the recent cases in Houston, can be done successfully with cooperative victim-witnesses and sting operations. Once victims come forward and the full scope of the defendant's criminal behavior is revealed, the fraudulent nature of the transactions engineered by the defendant is readily grasped by a jury. Achieving greater success against Nigerian fraud will require continued interagency collaboration, public education, and greater international cooperation.❖

## ABOUT THE AUTHORS

❑**Jim Buchanan** A career prosecutor, Jim Buchanan was an Assistant District Attorney for Harris County, (Houston) Texas for eleven years and has been an Assistant United States Attorney since 1993. As an AUSA, he has served as a white collar crimes prosecutor and is currently assigned to the Organized Crime Strike Force. He received the Director's Award in 1998 for superior performance by an AUSA for his prosecution of insurance/health care fraud in South Texas. In 1999, Mr. Buchanan was named as the coordinator for the Attorney General's Nigerian Organized Crime Strategy in the Southern District of Texas. He served as the chairman of the Government Lawyer's Section of

the State Bar of Texas in 1999 - 2000. He has taught local law enforcement and private investigators, and has lectured on prosecuting organized criminal activity in Romania. An experienced trial attorney, Mr. Buchanan has been lead prosecutor in over 100 jury trials.

**Alex J. Grant** has been a trial attorney with the Criminal Division's Fraud Section since 1999 and served as a Special Assistant U.S. Attorney at the District of Columbia U.S. Attorney's office in 2000. He is the Fraud Section's representative on the Nigerian Crime Initiative's Working Group. Prior to joining the government, Mr. Grant worked in private practice for nearly three years where he concentrated on complex civil and appellate litigation. Mr. Grant has published articles on a variety of topics in newspapers and law reviews.✠

# Civil and Criminal Remedies for Immigration Related Document Fraud

*Jack Perkins*
*Chief Administrative Hearing Officer*
*Executive Office for Immigration Review*

Federal prosecutors should be reminded that an alternative to criminal prosecution of immigration related document fraud exists. That alternative, enacted as § 274C of the Immigration and Nationality Act (INA) by the Immigration Act of 1990, was expanded in scope by amendments made by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA). (P.L. 104-208, Sept. 30, 1996, 110 Stat. 3009). These provisions were codified at 8 U.S.C. § 1324c.

Criminal provisions dealing with immigration-related document fraud include 18 U.S.C. §§1426, 1542, 1543, 1544 and 1546; as well as statutes of more general application, such as 18 U.S.C. §§ 1001 and 1028. The INS General Counsel's Office has also taken the position that §274C(a) can also be used *in addition to* criminal prosecution, i.e., that the double jeopardy clause would not be violated by such a course of action. In a 1998 memorandum to all Regional and District INS Counsels, the General Counsel for INS interpreted *Hudson v. United States*, 522 U.S. 93 (1997) as rendering the Double Jeopardy Clause not applicable to § 274C civil cases.

A class action lawsuit entitled *Walters v. Reno*, 145 F.3d. 1032 (9th Cir. 1998), *cert. denied*, 526 U.S. 1003 (1999), effectively suspended enforcement of § 274C before the expanded 1996 version of the statute went into effect. However, the *Walters* case has been settled, so the Immigration and Naturalization Service is free to resume enforcement of § 274C.

The specific provisions of § 274C are as follows:

(a) Activities Prohibited

It is unlawful for any person or entity knowingly–

(1) to forge, counterfeit, alter, or falsely make any document for the purpose of satisfying a requirement of this Act or obtain a benefit under this Act,

(2) to use, attempt to use, possess, obtain, accept, or receive or to provide any forged, counterfeit, altered, or falsely made document in order to satisfy any requirement of this Act or to obtain a benefit under this Act,

(3) to use or attempt to use or to provide or attempt to provide any document lawfully issued to or with respect to a person other than the possessor (including a deceased individual) for the purpose of satisfying a

requirement of this Act or obtaining a benefit under this Act,

(4) to accept or receive or to provide any document lawfully issued to or with respect to a person other than the possessor (including a deceased individual) for the purpose of complying with section 274A(b) or obtaining a benefit under this Act, or

(5) to prepare, file, or assist another in preparing or filing, any application for benefits under this Act, or any document required under this Act, or any document submitted in connection with such application or document, with knowledge or in reckless disregard of the fact that such application or document was falsely made or, in whole or in part, does not relate to the person on whose behalf it was or is being submitted, or

(6)(A) to present before boarding a common carrier for the purpose of coming to the United States a document which relates to the alien's eligibility to enter the United States, and

(6)(B) to fail to present such document to an immigration officer upon arrival at a United States port of entry.

Subsections § 274C(a)(5) and (6) were added by the IIRIRA amendments.

The term "falsely make," as used in § 274C(a), is defined at § 274C(f). That subsection, also added to the statute by the IIRIRA amendments, states:

(f) Falsely Make

For purposes of this section, the term "falsely make" means to prepare or provide an application or document with knowledge or in reckless disregard of the fact that the application or document contains a false, fictitious, or fraudulent statement or material representation, or has no basis in law or fact, or otherwise fails to state a fact which is material to the purpose for which it was submitted.

Other IIRIRA amendments to § 274C include the following criminal penalties:

(e) Criminal Penalties for Failure to Disclose Role as Document Preparer

(1) Whoever, in any matter within the jurisdiction of the Service, knowingly and willfully fails to disclose, conceals, or covers up the fact that they have, on behalf of any person and for a fee or other remuneration, prepared or assisted in preparing an application which was falsely made (as defined in subsection (f)) for immigration benefits, shall be fined in accordance with title 18, United States Code, imprisoned for not more than 5 years, or both, and prohibited from preparing or assisting in preparing, whether or not for a fee or other remuneration, any other such application.

(2) Whoever, having been convicted of a violation of paragraph (1), knowingly and willfully prepares or assists in preparing an application for immigration benefits pursuant to this Act, or the regulations promulgated thereunder, whether or not for a fee or other remuneration and regardless of whether in any matter within the jurisdiction of the Service, shall be fined in accordance with title 18, United States Code, imprisoned for not more than 15 years, or both, and prohibited from preparing or assisting in preparing any other such application.

Because § 274C(e) requires proof of two additional elements to establish a false making, that is willfully concealing the false making and performing the act for a fee or other remuneration, its utility to prosecutors seems debatable. However, there is the advantage of having the term "falsely make" clearly defined in the statute itself at § 274C(f). Whether the term "falsely make" includes providing false information on a form has been the subject of controversy in the case law. *See e.g., Moskal v. United States*, 498 U.S. 103 (1990) and *United States v. Merklinger*, 16 F.3d. 670 (6th Cir. 1994). ❖

**ABOUT THE AUTHOR**

❑**Jack E. Perkins** was appointed Chief Administrative Hearing Officer in January 1990.

He served as Acting Deputy Director of the Executive Office for Immigration Review from March to August 2001 while continuing to serve as Chief Administrative Hearing Officer. Much of Mr. Perkins's professional career has been spent serving in various positions within the Department of Justice including Deputy Assistant Attorney General, Office of Legislative Affairs, 1986 to 1990; legislative counsel and staff attorney, Office of Legislative Affairs, 1976 to 1985; staff attorney, Criminal Division, 1974 to 1976 and 1972 to 1973; and assistant U.S. attorney, Northern District of California, 1973 to 1974. ✠

# Know the Professional Responsibility Issues that You May Confront

*Claudia J. Flynn*
*Director, PRAO*

*Joan L. Goldfrank*
*Senior Legal Advisor, PRAO*

**I. Introduction**

In conducting investigations and prosecutions involving allegations of fraudulent conduct, there are numerous professional responsibility issues that a Department attorney may confront. Many of these issues become more difficult to resolve when the investigation involves corporations and their employees. A corporate attorney may assert that he represents the corporation and all of its employees. Employees may be represented by individual counsel in addition to the corporate attorney. Typically, there are parallel civil and criminal government investigations, and parallel private civil law suits or qui tam actions.

Because advice from the Professional Responsibility Advisory Office is provided only to Department attorneys and is otherwise confidential, the following discussion simply identifies issues but does not analyze them. Each issue must be analyzed under the relevant attorney conduct rules. Although some professional responsibility issues are easy to resolve, others are more difficult, requiring more analysis and consultation. There is case law and ethics opinions that provide guidance in analyzing these issues. In that regard, you are advised to contact your office's or component's Professional Responsibility Officer (PRO) when there is an issue and, if appropriate, to contact the PRAO at 202-514-0458 or on e-mail at PRAO, DOJ. In most circumstances, you should contact your PRO in the first instance. There is a PRAO website on the Department's intranet: http://10.173.2.12/prao/index.html.

**II. Which rules of professional responsibility govern**

The first step is to determine which rules of professional responsibility govern your conduct. Each state, including your state(s) of licensure, has adopted its own rules of professional responsibility. Each federal district court has adopted, by local court rule, the rules applicable to practice in that jurisdiction. Some federal district courts simply incorporate the rules adopted by the state in which the court sits; others adopt a version of the state rules; others adopt the ABA Model Rules or Code; and still others have adopted their own rules. The substance of the various rules of professional responsibility may conflict. In that case, a choice of law analysis is required. *See* ABA Model Rule 8.5; 28 C.F.R. Part 77.

**III. Contact with represented persons**

Every set of attorney conduct rules includes a provision governing the issue of a lawyer's communicating with a represented individual. The rules vary in text and interpretation from jurisdiction to jurisdiction. It is important that the relevant rule be analyzed in a given circumstance to determine whether a contact is proper.

The American Bar Association Model Rule 4.2 provides:

> In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized by law to do so.

In addition, ABA Model Rule 8.4(a) prohibits an attorney from violating the rules through the acts of another. Therefore, nonattorneys, including agents, working on the case with a Department attorney may not engage in a contact with a represented person when the attorney could not.

Each word or phrase of the contact rule raises different issues. We suggest you read three ABA formal opinions for background: ABA Formal Opinion 95-396; ABA Formal Opinion 95-390; and ABA Formal Opinion 91-359. The following sets forth recurring issues.

- How does a Department attorney know when an individual or an entity is represented by a lawyer? If you know that an entity is generally represented does that representation amount to knowledge that the entity is represented on the subject matter about which you want to communicate with it? Does the Department attorney have an affirmative obligation to ask if he or the entity is represented by a lawyer? When is the attorney/client relationship over?
- Does the rule apply only after a formal proceeding has been commenced? Does the rule apply to represented witnesses?
- What is considered a "communication"? A communication involves oral and written contact.
- The rule prohibits a lawyer from communicating with a represented person about the subject of the representation. It does not govern communications with a represented person concerning matters outside the representation. What constitutes the subject of the representation?
- Where there are parallel criminal and civil investigations regarding the same fraudulent activities but only one investigation is known by the represented individual or organization, is the represented person considered represented in both investigations for purposes of the contact rule?
- Where the represented person is an organization such as a corporation, which employees are considered represented by the organization's attorney? Comment [4] to Model Rule 4.2 states that there are three categories of persons considered to be represented by the organization's attorney: 1) persons having managerial responsibility on behalf of the organization; 2) persons whose act or omission in connection with the matter in representation may be imputed to the organization for purposes of civil or criminal liability; and 3) persons whose statement may constitute an admission on the part of the organization.
- Does an organization's attorney represent percipient witnesses?
- Are former employees represented by the organization's attorney? Are an organization's consultants or independent contractors represented by the organization's attorney?
- If a parent corporation is represented in the subject matter, is a subsidiary company deemed also to be represented for purposes of the contact rule?
- Is there a conflict of interest for the organization's attorney to represent both the organization and a given employee? If so, the Department attorney should consider raising this issue with the organization's attorney, and perhaps with a court, seeking that attorney's withdrawal of representation of the individual employee. PRAO can assist you in drafting a letter or a motion.
- What should you do when a client contacts you without his or her lawyer's

consent? It is the attorney's consent to the communication that is required. This rule is different from that governing who can waive the attorney/client privilege. The attorney/client privilege belongs to the client, and thus only the client can waive it. Pursuant to the contact rule, only the lawyer can consent to a direct contact of a represented person.

- If an employee has individual counsel, is consent by the individual counsel sufficient for purposes of obtaining lawyer consent under the contact rule? Or is consent of the organization's counsel also required?
- What does the phrase "authorized by law" mean? It may include: 1) a specific statute; 2) a court order; or 3) case law. A communication with a represented person made pursuant to formal discovery procedures or judicial or administrative process in accordance with the orders of the rules of the tribunal is "authorized by law."
- When can an investigator or cooperating witness communicate with a represented person? What do you do with information an investigator obtained through contact with a represented person when such contact may have been improper?
- Can you direct an agent, a cooperating witness or an informant to engage in an undercover contact, including consensual monitoring, with a represented person or an employee of a represented organization?

**IV. Obligation not to use a method to obtain evidence in violation of a third party's legal rights**

ABA Model Rule 4.4 provides that a lawyer shall not use a method of obtaining evidence that violates the legal rights of another. For example, when communicating with a witness (including a former employee), you cannot ask the witness to disclose information that is protected by a legal privilege or a contractual agreement.

- Can you use materials provided to you by an employee of a represented organization that belong to the organization and not the employee?
- What do you do with materials provided to you by the employee that are clearly marked "attorney/client privileged"?

**V. Conclusion**

The rules of professional responsibility govern every phase of an investigation and litigation or prosecution. The rules address how you should deal with the opposing party, the opposing counsel, witnesses and potential witnesses, and the court. You should be mindful that some of the rules of professional responsibility go beyond the requirements of the Constitution.❖

**ABOUT THE AUTHORS**

❑**Claudia J. Flynn** became an Assistant United States Attorney for the District of New Jersey in 1984 and, in 1989, Deputy Chief of that Office's Criminal Division. Ms. Flynn left the United States Attorney's Office in 1992 to become an Associate Independent Counsel at the Office of Independent Counsel (Adams), which conducted the investigation and prosecutions relating the HUD scandal of the 1980s. She returned to the United States Attorney's Office in New Jersey in 1994 as Chief of the Criminal Division. In 1996, she left New Jersey for the Department of Justice in Washington, D.C., where she acted as Chief of Staff to the Assistant Attorney General, Criminal Division (February 1996 to September 1997); as Senior Counsel to the Director, Executive Office for United States Attorneys (September 1997 to January 2000); and as Director of the Professional Responsibility Advisory Office (January 2000 to the present).

**Joan L. Goldfrank** presently is a Senior Legal Advisor in the United States Department of Justice's Professional Responsibility Advisory Office, which provides advice to Department attorneys regarding professional responsibility issues. She has been with the Department since 1994, when she joined the Office of Professional Responsibility to investigate allegations of

misconduct against Department attorneys. She became Senior Attorney for Professional Responsibility in the Environment and Natural Resources Division in 1997. For nine years prior to joining the Department, Ms. Goldfrank was the Executive Attorney for the D.C. Board on Professional Responsibility, an arm of the District of Columbia Court of Appeals responsible for the administration of the attorney discipline system in the District of Columbia.

She frequently conducts training sessions on professional responsibility issues for the Department, other government agencies, and bar associations. She teaches legal ethics as an adjunct professor for Vermont Law School.✠

# NOTES

## UPCOMING PUBLICATIONS

January, 2002 - Project Safe Neighborhoods

# Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' **BULLETIN** to all who wish to receive, 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.