March 2002
Volume 50
Number 2

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

Kenneth L. Wainstein
Director

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

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

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

Managing Editor
Jim Donovan

Assistant Editor
Nancy Bowman

Law Clerk
Ginny Nissen

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

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

Fraud in the Corporate Context

In This Issue

The FBI Criminal Undercover Operations Review Committee

Joshua R. Hochberg
Chief, Fraud Section,
Criminal Division

The FBI Criminal Undercover Operations Review Committee (CUORC) is a formal committee whose approval is required for all FBI undercover operations involving "sensitive circumstances", so-called "Group I" Undercover Operations. The Committee, which is chaired by the FBI, meets every other week. Its members include Section Chiefs from FBI headquarters, FBI representatives from the office of General Counsel and senior Department of Justice Criminal Division members.

Representatives from the Fraud, Asset Forfeiture and Money Laundering, Public Integrity, Narcotic and Dangerous Drug, and Organized Crime and Racketeering Sections usually attend CUORCs. In addition, the Office of International Affairs, the Computer Crime and Intellectual Property Section and the Terrorism and Violent Crime Section send representatives as needed.

The Attorney General's Guidelines on FBI Undercover Operations, which were revised in 1992 and are available on the Department of Justice Intranet, govern the CUORC. These guidelines currently are being reworked to clarify procedures relating to potential terrorism investigations. SAC's can authorize undercover operations that do not involve "sensitive" circumstances or that need authorization on an emergency basis. This article gives a brief overview of the operations of the CUORC and highlights a few of the issues that may arise. It does not discuss many of the specific rules and considerations applicable to undercover operations. Other federal law enforcement agencies have analogous review procedures and committees for their own undercover operations. AUSAs should consult with their case agents to ensure that appropriate rules are being followed.

The CUORC reviews written submissions from the sponsoring FBI field office and the FBI headquarters Section, which describe the nature of the undercover operation, analyze any "sensitive" circumstances, and provide a legal opinion on the propriety of the investigative technique. In all undercover operations, reviewing officials must consider the suitability of government activity and evaluate and weigh the risks of injury, liability, interference with privileged activity, and involvement in criminal activity. All proposed Group 1 undercover operations require the personal, written approval of the United States Attorney for the District sponsoring the investigation. The FBI also requires various levels of approval including the approval of the SAC, the headquarters section, and an Assistant Director, or higher level official.

The Guidelines provide specific definitions of the sensitive circumstances that require CUORC review. In general terms, AUSAs should be aware that the following types of activities are likely to be considered sensitive circumstances:

- Most investigations of criminal conduct by government officials, including systemic corruption in government, or activities which will intrude on the governmental function.
- Undercover operations which require the creation or use of a proprietary business.
- Participation in most felonious activities.
- Relationships which impinge on privileged areas.
- Operations which create a significant risk of violence.
- Operations which may subject the government to significant damage claims.
- Operations in which the government provides goods or services that are essential to the commission of a crime and are otherwise not reasonably available.

The approvals required for participation in felonious and other serious crimes, are detailed and specific. The Guidelines require CUORC approval, except for a limited number of felonies, including, the receipt of stolen property, and the controlled delivery of drugs that will not enter commerce. SACs must authorize participation in all undercover operations involving illegal activities, and higher level FBI approvals are needed for specific types of activities, including those which create a risk of violence.

In addition to sensitive circumstances, the CUORC evaluates complex issues, including those related to investigations which impact other countries and the Government's proper role in computer-related investigations. The CUORC will always consider whether the targets of the proposed undercover operation have been appropriately predicated. In determining the adequacy of predication, the Committee will generally engage in an analysis of potential entrapment issues. Next, even if the subjects are clearly predisposed to engage in the targeted criminal activity, Committee members will consider whether these targets are sufficiently significant targets, whether other investigative techniques have been tried, and whether the investigation merits the use of undercover techniques that involve a major investment of time and resources, as well as potential liability issues.

In practice, the CUORC approves undercover operations only after reaching a consensus of its members. Typically, through the use of stipulations pursuant to the Undercover Guidelines, the Committee attempts to "minimize the incidence of sensitive circumstances and reduce the risks of harm and intrusion that are created by such circumstances." Stipulations set forth written restrictions and policies for the operation. In addition to the CUORC review, the FBI will often perform an onsite review of the ongoing operation to identify problems and to ensure that stipulations are being followed.

As a practical matter, AUSAs and Special Agents are encouraged to raise and discuss any issues posed by the undercover operation. The supervising AUSA should evaluate types of issues considered in the CUORC before support is given for a proposal. Furthermore, the CUORC approves undercover operations for specified time periods, generally six months. The undercover operations have to be re-presented to the CUORC for renewal beyond six months, for additional funding, or if there has been a change in their focus. At all times during the undercover operation, and specifically at the time of renewal, AUSAs should be consulting with the case agents and monitoring and reevaluating the progress of the undercover operation. AUSAs are encouraged to discuss any issues informally with members of the CUORC before they actually present an undercover proposal. AUSAs should pose their questions to the Criminal Division Section Chief with responsibility for the type of activity involved in the undercover proposal or to the FBI Section that is reviewing the application. On occasion, AUSAs attend CUORC meetings to answer questions and explain the significance of the investigations. The CUORC committee members have seen numerous proposals over the years and can often suggest ways to minimize risks and to ensure that, once the undercover operations are completed, there will be well-founded, prosecutable cases.❖

ABOUT THE AUTHOR

❑**Joshua R. Hochberg** has been the Chief of the Criminal Division's Fraud Section since 1998. Mr. Hochberg was the Deputy Chief for Litigation in the Public Integrity Section from 1995 to 1998, and a Trial Attorney and Senior Litigation Counsel in the Fraud Section from 1986 to 1995. He has been a regular member of the CUORC for several years.✠

Investigating Accounting Frauds

David L. Anderson
Assistant United States Attorney
Northern District of California

Joseph W. St. Denis
Assistant Chief Accountant
Division of Enforcement
United States Securities and Exchange Commission

"How can this be a criminal matter?"

This question seems to come up in every accounting-fraud investigation. The person asking the question is typically a target and likely speaking through his attorney.

The target's question has no basis in law. A criminal prosecution is authorized by statute whenever a willful violation of the Securities Exchange Act of 1934 or any rule or regulation adopted under that Act occurs. *See* 15 U.S.C. § 78ff(a). Rule 10b-5 prohibits fraud, including accounting fraud, in connection with the purchase or sale of any security. *See* 17 CFR 240.10b-5. When a publicly traded company willfully engages in accounting fraud, it commits a federal crime.

The target's question may be rooted in the false hope that accounting frauds are too technical or arcane for a prosecutor to explain to a lay jury. This hope has no basis in fact.

In the Northern District of California, the United States Attorney has established a Securities Fraud Unit with a team of prosecutors dedicated to securities-fraud matters, principally accounting frauds and insider trading. The experience in our District is that prosecutors can make accounting frauds understandable to lay people.

The Northern District of California is home to San Francisco and Silicon Valley. The District is also home to companies such as Cal Micro, Media Vision, Critical Path, Indus, and Scorpion Technologies, all of which have seen their officers, directors, or employees prosecuted for securities fraud. These cases have been brought on investigations conducted by the Federal Bureau of Investigation, usually in cooperation with the United States Securities and Exchange Commission ("SEC").

This article draws on recent experiences in the Northern District of California and on the even broader, nationwide experience of the SEC in accounting-fraud cases. This article discusses how to recognize common accounting frauds, use documentary evidence to obtain witness statements in an accounting-fraud case, and cooperate effectively with the SEC.

I. Common accounting frauds

In his book, *Financial Shenanigans* (1993), Howard M. Schilit identifies the seven basic patterns of accounting fraud. They are:

- Recording bogus revenues;
- Recording revenues too soon (for example, by backdating or channel stuffing);
- Boosting income with one-time gains;
- Shifting current expenses to future periods (manipulating accruals or reserves);
- Failing to record or disclose all liabilities (understating expenses or hiding debt);
- Shifting current income to a later period; and
- Shifting future expenses to the current period.

Id.

The impropriety of some of these accounting frauds is readily apparent. For example, a company that finds itself just short of quarterly revenue goals might "keep its books open" for a few days into the succeeding quarter, thereby improperly accelerating the recognition of revenues from a later quarter to an earlier one. To avoid detection, someone at the company may backdate sales contracts and shipping documents. If a sales contract was backdated to meet quarterly numbers, arguing that the backdating was the result of "accounting judgment" or "immaterial inadvertence" is going to be difficult.

The significance of other accounting frauds may not be so transparent. A company that shifts

current income to a later period or that shifts future expenses to the current period is understating its current financial performance. The motive for this type of accounting fraud may be to "smooth" or "manage" earnings. If the company has already exceeded its quarterly financial goals, it might create a safety net for future quarters by delaying the recognition of revenue or accelerating the recognition of expenses.

Having at least some awareness of all seven of Schilit's financial shenanigans is advantageous because they seldom appear in isolation. An accounting misstatement, which appears defensible in isolation, may become completely unjustifiable when viewed in the context of other, contemporaneous misstatements. For example, a company may improperly record revenue from a bogus sales contract but still find itself short of quarterly financial goals, and so drain off its reserves to make up the difference. Viewed in isolation, the company's decision to adjust its reserves might look like a perfectly permissible accounting judgment that takes into consideration some recent changes in circumstances. However, if you find a bogus sales contract, you may be well on your way to unraveling the more obscure aspects of the overall fraud.

Here is a sadly common fact pattern: A company engages in a low-risk, low-transparency accounting fraud. To meet its second-quarter goals, the company draws down its accounting reserves in a way that is somewhat defensible. The company reports pleasing quarterly results and makes third-quarter predictions that appear aggressive, but not overly so, in light of its reported second-quarter performance. The problem is that even its second-quarter numbers were a stretch. To compound the problem, the company has eliminated whatever cushion it had by drawing down its reserves. At the end of the third quarter, it is far short of its quarterly goals. Now there is pressure to engage in some bigger accounting fraud — executing a bogus sales contract, or characterizing a one-time gain as income from operations. If that accounting fraud succeeds, it sets the stage for even higher expectations for the fourth quarter. Sooner or later, the company engages in some truly brazen accounting misstatement. Investigating the most egregious violation, you uncover a larger pattern of fraud.

An egregious accounting fraud may provide the initial impetus for your investigation. However, its significance does not end there. The worst frauds are typically the most difficult for targets or defendants to defend, either before or during trial. During a proffer session, a target who is perfectly comfortable defending his company's fraudulent reserve practices, may find himself with no choice but to tell the truth about a side agreement or backdating scheme. A defendant at trial may lose credibility with the jury as he attempts to explain his most outlandish accounting frauds.

Here are four brazen accounting frauds around which you can build a good criminal case:

A. Side agreements

It is the end of the quarter. Top management desperately wants to meet its publicly stated revenue goals for the quarter. A valued customer is ready to execute a transaction that will push the company beyond its goals. However, the customer wants one last concession to close the deal – an extended payment term, or an evaluation period, or something else that will disrupt revenue recognition during the quarter.

To close the deal and meet the company's goals, a sales manager prepares the deal paperwork in the usual form, omitting the last-minute concession. Separately, he assures the customer that the special concession will be delivered as promised. The phrase "side agreement" refers to the common practice of placing that last-minute concession into a separate document. Whatever form the side agreement may take, the problem arises when its substance is hidden from the company's accounting department and external auditors. What looks like a standard deal has additional baggage that would, if fully disclosed, prevent revenue recognition, at least until some later period.

In the Northern District of California, we have seen side agreements that promise customers unlimited rights of return, extended or unusual payment terms, or even the right to void sales contracts at will. A company that gives these types of special concessions typically cannot recognize revenue until after the concessions expire because, in the face of such concessions,

collectibility is not reasonably assured. *See* AICPA Statement of Position 97-2, *Software Revenue Recognition* ("SOP 97-2"), ¶ 8 (1997) (describing four primary criteria, including reasonable assurances of collectibility, for the recognition of software-licensing revenue); SEC Staff Accounting Bulletin No. 101, *Revenue Recognition in Financial Statements* ("SAB 101") (1999) (applying the criteria set forth in SOP 97-2 to all types of business transactions).

If you discover the existence of a side agreement, look for high-level management involvement. Customers often will demand that their special concessions be approved by top management. Even if the side agreement is not signed by a top manager, the customer may have received comfort from management, in the form of a telephone call, or verbal approval through the salesperson. What customer wants a side agreement that is later repudiated by top management?

Salespeople may also have an incentive to involve top management in the approval of side agreements. Rarely do individual salespeople have actual legal authority to change standard contract terms. Except in cases involving the "rogue salesperson," expect to find top-level managers involved in some way with the issuance of the side agreement.

B. Nonmonetary transactions

When a customer pays cash for a product in an arm's-length transaction, the transaction is generally valued in the amount of money paid. For example, if a house buyer and house seller agree on a cash price for a house, that cash price is generally considered good evidence of the true value of the house at the moment the transaction is closed.

The situation is different if two parties agree to exchange houses. In this situation, their agreement may establish that the houses are approximately equal in value, but the agreement does little to show how much each house is worth. The parties might agree that each house is worth $1 or $1 million, but because cash is not changing hands, the parties' agreement is not persuasive evidence of value.

Transactions, in which something other than money changes hands, are sometimes described as "swap transactions" or "barter deals." Accountants call them "nonmonetary transactions." In a nonmonetary transaction, the accounting issue is typically not *whether* revenue should be recognized, but *how much* revenue should be recognized. *See* Accounting Principles Board Opinion No. 29, *Accounting for Nonmonetary Transactions* ("APB Opinion No. 29"), ¶ 2 (1973).

The valuation rules for nonmonetary transactions are complex in some ways. *See*, *e.g.*, APB Opinion No. 29; FASB Emerging Issues Task Force, Issue No. 99-17, *Accounting for Advertising Barter Transactions* ("*Barter Transactions*") (November 17, 1999); AICPA Technical Practice Aid 5100.46, *Nonmonetary Exchanges of Software (Part I)* (December 29, 2000).

You need not become bogged down in these valuation rules to recognize a problem transaction. Nonmonetary transactions must generally be separately disclosed to investors. APB Opinion No. 29 at ¶ 28. A company engaging in a fraudulent nonmonetary transaction will almost invariably fail to disclose it. Even if the company's valuation of the transaction conforms with generally accepted accounting principles (GAAP), the failure to disclose will still likely constitute fraud.

To avoid the special scrutiny to which nonmonetary transactions are subjected under GAAP, a company may structure the transaction to make it look like two separate cash sales. A company may go so far as to prepare two separate sales contracts and to exchange checks in equal (or, better yet, not quite equal) amounts. But swapping checks does not evidence fair value. *Barter Transactions* at ¶ 4 ("An exchange between the parties to a barter transaction of offsetting monetary consideration, such as a swap of checks for equal amounts, does not evidence the fair value of the transaction.").

If you find evidence of a fraudulent nonmonetary transaction, look for the involvement of the company's internal accounting and finance personnel. Their expertise will likely have been called upon in structuring the transaction and perhaps in disguising it. Also look for the involvement of top company management.

C. Backdating

The accounting rules do not allow "wiggle room" for transactions that close one week, one day, or even one hour after the end of the accounting period. If the company has a calendar fiscal year, and its fourth quarter ends on December 31, it cannot count fourth-quarter revenue for a transaction closed on January 1, or 5, or 15.

What happens if a company discovers on January 2 that it is a mere few million dollars short of public expectations for its quarterly revenues? Or if a customer delays signing an agreement that the company had been counting on to meet its numbers? Company management may be tempted to backdate the agreement to create the false appearance that the transaction was closed during the previous quarter.

Revenue generally cannot be recognized until there is evidence of a sales arrangement and delivery of the product. SOP 97-2 at ¶ 8; SAB 101. If a company customarily executes written contracts with its customers, a written contract will normally be required before revenue may be recognized. SOP 97-2 at ¶¶ 15-17.

If you find backdating, look for other evidence of wrongdoing because a criminal case focused on backdating alone may be difficult to prosecute. An individual salesperson may backdate an agreement without the overt or obvious involvement of sales management. Also, if the customer eventually pays under the agreement, your prosecution will be susceptible to the argument that the backdating was a mere technical violation.

Backdating may provide important evidence in the context of a larger pattern of fraud. Backdating is both inexcusable and readily comprehensible. Periodic reporting systems obligate a company to report its revenues in the appropriate accounting period. Accelerating those revenues by backdating sales contracts or shipping documents cannot be justified with reference to generally accepted accounting principles.

D. Concealing debt or expenses

The fraudulent schemes just discussed — issuing side agreements, executing nonmonetary transactions, or backdating sales agreements — all involve the improper recognition of revenues. Overstating revenues is the most common type of accounting fraud. *See* Lynn E. Turner, *Revenue Recognition* ("*Revenue Recognition*") (May 31, 2001),<http://www.sec.gov/news/speech/spch495.htm>. Revenue fraud also has the greatest impact in terms of damages to shareholders. *Id.* (stating that "[b]ased on research performed by my office, restatements for revenue recognition also result in larger drops in market capitalization than any other type of restatements.").

Frauds involving debt or expenses should not be overlooked, however. These, too, may result in substantial losses to shareholders. For example, from 1992 to 1996, Arthur Andersen LLP issued audit reports for financial statements of Waste Management, Inc. that improperly deferred current expenses to future periods and failed to disclose one-time gains, which were used to offset current expenses. *See In re Arthur Andersen LLP*, SEC Accounting and Auditing Enforcement Release No. 1405 (June 19, 2001). The cumulative effect of these and other misstatements was to overstate Waste Management's earnings by $1.43 billion. *Id.* Losses to shareholders were as high as $6.5 billion.

One common way for companies to conceal expenses is to defer the recognition of expenses to some future period. Waste Management improperly reduced depreciation expenses on its vehicles, equipment, and containers, so as to defer those depreciation expenses to later accounting periods. *Id.*

Another way to conceal debt or expenses is to attribute them to unconsolidated subsidiaries or special-purpose entities. In such instances, the attribution may be permitted by GAAP, but the company's failure to disclose the true nature of the entity or transaction results in an unfair presentation of the company's financial performance or position.

Yet another way for companies to conceal expenses is to accelerate their recognition. This fraudulent scheme is sometimes referred to as the "big bath." In conjunction with a bad-news announcement or nonrecurring event, the company records expenses in an amount greater

than actually incurred. The excess of recorded over actual expenses is "stored" in a reserve account, sometimes referred to as a "cookie-jar" reserve. In a later period, the company uses the cookie-jar reserve to reduce then-current expenses.

Here is a well-known example of a company taking a big bath: In 1996, after "Chainsaw" Al Dunlap took control of Sunbeam Corporation, the Company inflated its reported annual loss by creating cookie-jar reserves. *See In re Sunbeam Corporation*, SEC Accounting and Auditing Enforcement Release No. 1393 (May 15, 2001). Then, in 1997, the company released these reserves to reduce expenses and inflate income, thus creating the false impression of a rapid turnaround. *Id.* When the fraud was revealed, shareholders lost $3.5 billion.

II. Turning paper into witnesses

The government doesn't often win criminal trials with documents alone. Strong witnesses make strong cases. Accounting-fraud cases may be paper intensive, but they are witness intensive too. In an accounting-fraud case, just as in other types of cases, you need powerful testimony, not just incriminating documents.

One common mistake in the prosecution of accounting-fraud cases is to focus on the paper to the exclusion of key witnesses. Another common mistake is to spend so much time obtaining or analyzing the relevant documents that, in the meantime, key witnesses forget or misremember relevant facts. Don't let your witnesses go stale! Obtain and organize your paper quickly, and then use it while interviewing witnesses.

A. "Flip" lower-level participants like narcotics prosecutors would

Narcotics prosecutors are familiar with the concept of "flipping" a witness. A lower-level participant in the narcotics-distribution scheme agrees to testify against a higher-level participant. Typically, the lower-level participant does not agree to become a government witness solely because of strong feelings of patriotism or good citizenship. He has an eye on his own criminal liability.

Company salespeople, lower-level managers, and rank-and-file accounting personnel are all potential government witnesses. Many of them will have a keen appreciation of their own potential criminal exposure. In the Northern District of California, lower-level employees who fully cooperate with an accounting-fraud investigation may not be prosecuted for their involvement in the accounting fraud. To secure nonprosecution, they must, among other things, provide statements and testimony that are truthful and complete.

Some lower-level employees demonstrate an unfortunate tendency to minimize the misconduct of themselves, their supervisors, or the company. If a lower-level employee has difficulty providing truthful cooperation, he will not be an effective government witness. In the Northern District of California, a lower-level employee who has difficulty telling the truth may quickly find himself a defendant, not merely a witness, in an accounting-fraud case.

B. Use emails to obtain witness statements

As narcotics prosecutors know, the most successful narcotics distributors do not often talk about drugs on the telephone. Instead, they use their telephones to arrange personal meetings or make calls over payphones. Some narcotics distributors speak in coded language. They realize what they say may be recorded and used against them.

Incredibly, white-collar criminals often use their email accounts with much less sophistication than street-level criminals handle their telephones. White-collar criminals may communicate openly in email about their criminal plans.

A company that cooperates fully with an accounting-fraud investigation may not be prosecuted for the criminal acts of its officers or employees. To secure nonprosecution, the company must, among other things, promptly produce all relevant emails in its possession or control. Typically, this includes all emails that were sent or received on company computers.

Contemporaneous emails between participants in an accounting-fraud conspiracy may provide an abundance of evidentiary and investigative information. Contemporaneous emails may help

establish plans, intentions, dates, or participants relevant to the criminal scheme. They may be useful at trial or, just as importantly, they may help obtain early, truthful statements from company witnesses.

C. Focus on the defendant's acts of deception

In some instances, GAAP is highly discretionary or even quite malleable. In theory, this discretion allows the accounting professional to choose the most appropriate accounting treatment for any given transaction. Regrettably, in practice, this discretion may allow a company to manage its revenues or earnings in a way that is advantageous to management but does not result in a fair presentation.

At trial, an accounting-fraud defendant may proffer expert testimony that his accounting judgments were within GAAP, or that any departure from GAAP was immaterial. This expert testimony may present unique challenges. Although the government may present its own expert testimony, this may leave a lay jury with the wrong impression that the case is about a debate within the accounting profession, not criminal wrongdoing.

Look for the contemporaneous acts and statements of the defendant that reveal *the defendant himself believed he was engaged in wrongdoing*. A defendant's expert testimony will ring hollow at trial if the defendant has acted or spoken in a way that shows awareness of his wrongdoing.

For example, a defendant in a side-agreement case may argue at trial that the amendments contained in the side agreement are immaterial. If they are immaterial, then why did the defendant hide them in a side agreement? By pointing to the defendant's own actions, you may avoid becoming embroiled in a debate over materiality. Your closing argument is that the defendant knew the amendments were material, which is why he hid them in a side agreement.

Here is another example: A defendant in a barter-transaction case argues at trial that his valuation of the transaction was fair and appropriate under the circumstances. If that is true, then why didn't the defendant disclose the barter nature of the transaction? Again, by pointing to the defendant's own actions, you may neutralize a technical defense based on accounting principles that may be challenging to even the most intelligent lay juror. Your closing argument is that the defendant knew the company could not properly recognize revenue for the barter transaction without further evidence of value and that's why he hid the true nature of the transaction.

Acts of deception may prove useful during an investigation as well as at trial. A witness who is perfectly comfortable defending his accounting judgments may have greater difficulty explaining why he failed to disclose significant aspects of a suspect transaction.

III. Conducting parallel investigations

United States Attorney's Offices handle a wide range of federal criminal and civil matters. A good, experienced prosecutor may have a deep understanding of the rules of evidence and a nose for wrongdoing, but nothing in the job description says he or she has to be an accounting expert also.

The United States Securities and Exchange Commission has more than sixty years of investigatory and regulatory experience with the United States securities markets. Among other considerable resources, the Commission has a staff of accounting professionals deployed in field offices around the country and in Washington, D.C.

Public policy and good practice dictate that federal prosecutors work cooperatively with the SEC whenever possible. As a matter of policy, "prosecutors should consult with the government attorneys on the civil side and appropriate agency officials regarding the investigative strategies to be used in their cases." Office of the Attorney General, *Coordination of Parallel Criminal, Civil, and Administrative Proceedings* ("*Coordination of Proceedings*"), 2 (July 28, 1997). As a matter of practice, you will almost invariably benefit from effective cooperation with the SEC. SEC attorneys and accountants may assist you in finding, organizing, and understanding relevant documents. They may also educate you on the specific accounting principles most relevant to

your investigation.

To cooperate effectively with the SEC, you must be sensitive to the requirement of grand jury secrecy. You generally may not disclose to the SEC matters occurring before the grand jury. *See* Fed. R. Crim. P. 6(e)(2); *cf.* Fed. R. Crim. P. 6(e)(3)(A)(ii) (permitting disclosure only as necessary to enforce the federal criminal law). If you subpoena a witness before the grand jury, you generally may not disclose even the identity of the witness or the existence of the subpoena. Although documents subpoenaed before the grand jury may, in some circumstances, be disclosed to the SEC, this outcome is generally achieved only by motion before the District Court. *See United States v. Dynovac*, 6 F.3d 1407, 1411-12 (9th Cir. 1993) (finding that "if a document is sought for its own sake rather than to learn what took place before the grand jury, and if its disclosure will not compromise the integrity of the grand jury process, Rule 6(e) does not prohibit its release").

In many cases, not launching an extensive early grand jury investigation is best. Witness statements may often be obtained informally through FBI interviews, rather than through grand jury subpoenas. The SEC may be invited to participate in these witness interviews or may be provided with the FBI 302s memorializing the witnesses' statements. If you take witness testimony before the grand jury, or withhold the results of your witness interviews from the SEC, the SEC will likely issue administrative subpoenas for the same witness testimony. Taking testimony from the same witnesses in separate proceedings may be desirable if the witnesses are evasive or motivated to lie, but for witnesses who are cooperative and truthful, rarely much is to gain from having them testify before both the grand jury and the SEC.

Oftentimes, documentary evidence may also be obtained in a manner that readily facilitates its use by your office and the SEC. "With proper safeguards, evidence can be obtained without the grand jury by administrative subpoenas, search warrants and other means. Evidence can then be shared among various personnel responsible for the matter." *Coordination of Proceedings* at 2.

IV. Conclusion

Here is a final case example: In the third and fourth quarters of 2000, a high-tech company known as Critical Path, Inc. engaged in the sorts of accounting frauds discussed in this article — backdating sales contracts, issuing undisclosed side agreements, executing improper nonmonetary transactions, and concealing expenses. *See Securities And Exchange Commission v. David A. Thatcher and Timothy J. Ganley*, SEC Accounting and Auditing Release No. 1504 (February 5, 2002). On April 5, 2000, the Company restated its financial results for those quarters and for the fiscal year 2000. Net losses for the third and fourth quarters of 2000 were restated upward by more than 50%. Revenues for those quarters were restated downward by more than 20%. *Id.*

Both the FBI and SEC opened investigations into Critical Path's accounting practices, with the U.S. Attorney's Office for the Northern District of California vigorously participating in the FBI's investigation. On February 12, 2002, less than a year from the date of the Company's restatement, Critical Path's former president pled guilty to conspiring to commit securities fraud.

In today's legal and market environment, the investing public needs and demands the criminal enforcement of the federal securities laws. As the SEC's former Chief Accountant recently stated, "at some point in time, investors are going to lose more than their money, they are going to lose their trust in the numbers and the system and people who produce and audit them. We cannot, and shall not let that happen." *See* Lynn E. Turner, *Revenue Recognition* ("*Revenue Recognition*") (May 31, 2001),<http://www.sec.gov/news/speech/spch495.htm>. What are you doing in your District to protect investors and prosecute accounting fraud?❖

ABOUT THE AUTHORS

❑**David L. Anderson** is an Assistant United States Attorney in the Northern District of California. Mr. Anderson has a degree in accounting from San Jose State University. Mr. Anderson graduated from Stanford Law School in 1990 and clerked for Associate Justice Anthony M. Kennedy. In 1998, Mr. Anderson testified

before Congress on securities litigation reform.✠

Joseph W. St. Denis is an Assistant Chief Accountant in the United States Securities and Exchange Commission's Division of Enforcement in Washington, D.C. Mr. St. Denis has a degree in accounting and an M.B.A. from the University of Colorado at Boulder. Mr. St. Denis is a licensed CPA in Colorado. Before joining the SEC's Division of Enforcement, Mr. St. Denis was an auditor with Coopers & Lybrand and a CFO, controller and vice president-finance in the high-tech industry.✠

The Securities and Exchange Commission, as a matter of policy, disclaims any responsibility for any private publication or speech by its members or staff. The views expressed herein are those of the authors and do not necessarily reflect the views of the Commission or the authors' colleagues on the staff of the Commission.

Prime Bank/High Yield Investment Schemes

Joel E. Leising
Senior Trial Attorney
Fraud Section, Criminal Division

Michael McGarry
Trial Attorney
Fraud Section, Criminal Division

I. Introduction

Ever since Breton Woods and the formation of the International Monetary Fund and World Bank in the late 1940's, the major banks in the world have engaged in trading programs among themselves, yielding returns ranging from 10% to 100% per month, at little or no risk. Only these banks, and a few select traders authorized by the Federal Reserve, are allowed to participate in these trading programs, which are principally designed to generate funds for humanitarian and other worthwhile projects. On occasion, particular traders allow individual investors to participate in these secret trading programs by pooling the individual's funds with funds from other investors until a certain amount, usually a minimum of $100 million, is accumulated for a trade. However, these individuals must enter non-disclosure agreements with the traders and agree to contribute half of their profits to a designated charitable cause.

Interested? Your investment advisor never told you about this? Maybe that's because all of what you have just read is false. Nevertheless, thousands of people during the past decade have fallen prey to scams based on similar claims and lost billions of dollars believing they were investing in such mythical trading programs. Despite repeated warnings over the years from various regulatory agencies and international organizations that such trading programs do not exist, these prime bank or high-yield investment schemes have continued to proliferate and are now nearing epidemic levels.

Various agencies or organizations, such as the Federal Reserve Board, Office of Comptroller of Currency, Department of Treasury, Securities and Exchange Commission (SEC), International Chamber of Commerce, North American Securities Administrators Association, International Monetary Fund, and World Bank have all issued explicit warnings to the public about prime bank fraud. Occasionally, you will find copies of these among the items seized during execution of a search warrant at a fraudster's

office. A number of good reference materials are publicly-available relating to these schemes, including PRIME BANK AND RELATED FINANCIAL INSTRUMENTS FRAUD issued by the SEC in 1998. Two others are PRIME BANK INSTRUMENT FRAUDS II (THE FRAUD OF THE CENTURY), prepared in 1996 by the ICC Commercial Crime Bureau, and THE MYTH OF PRIME BANK INVESTMENT SCAMS, by Professor James Byrne of the Institute of International Banking Law & Practice, George Mason University Law School.

Prime bank fraud first appeared in the early 1990's, waned somewhat in the mid 1990's in response to aggressive enforcement actions and media coverage, then reemerged as a significant problem in the late 1990's. At present, over one hundred pending federal criminal investigations involve prime bank fraud. In addition, the Securities and Exchange Commission and various state law enforcement agencies have a number of active investigations. Moreover, as the problem has become worldwide, more foreign law enforcement agencies, particularly in English-speaking countries, have actively investigated and prosecuted this type of fraud.

The purpose of this article is primarily two-fold: first, to alert readers to the existence of this particular type of fraudulent scheme, and second, to offer some suggestions for investigating a prime bank scheme.

II. Common characteristics of the scheme

"Prime bank" schemes — "prime bank instrument" schemes, "high yield trading programs" or "roll programs"— are essentially Ponzi schemes, in which the perpetrators claim exists a secret trading market among the world's top banks or "prime banks." Perpetrators claim to have unique access to this secret market. The "top" or "prime" banks purportedly trade some form of bank security such as bank guarantees, notes, or debentures. These instruments can supposedly be bought at a discount and sold at a premium, yielding greater than market returns with no risk. In reality, no such market exists. Furthermore, high-yield "prime bank notes," as described by these perpetrators, do not exist.

They often claim that there are only a few "traders" or "master commitment holders" who are authorized to trade in these securities and that the securities must be traded in large blocks, typically millions of dollars or more. Promoters tell potential investors that they have special access to a trading program, and that by pooling their money with that of other investors, they can participate in the program. Promoters also tell investors that the programs participate in some humanitarian cause and that they are giving the investors a special opportunity to participate in the program, but only if they agree to give a share of the profits to the cause. They also typically require investors to execute a "non-disclosure" and "non-circumvention agreement" because , as they are told, banks and regulatory agencies will deny the existence of these trading programs.

III. Case law involving prime bank schemes

Over the past few years, a number of reported decisions affirmed convictions of prime bank schemers. For example, this past summer the Fourth Circuit affirmed defendants' convictions in *United States v. Bollin,* 264 F.3d 391 (4th Cir. 2001), for conspiracy, wire fraud and money laundering. As described by the Court of Appeals:

> This case arose out of a wide-ranging investment fraud scheme, carried out by a network of conspirators, who bilked millions of dollars from investors across the country. The investments were programs that promised enormous profits, supposedly derived from secret trading in debentures issued by European "prime" banks.
>
> The programs involved supposed trading of European "prime bank" debentures and promised very high rates of return with little or no risk to investors. According to the ... literature that they distributed, the programs were available on a limited basis to groups of investors whose money would be pooled and delivered to a "prime" bank. The investment principal was supposedly secured by a bank guarantee and, therefore, was never at risk. Millions of dollars in profits were to be generated within a few months from the trading of debentures. For example, one program ... offered a profit of $73,000,000 in ten months, based on an investment of $400,000.

Id. at 399-400.

In *United States v. Polichemi*, 201 F.3d 858, *aff'd on rehearing*, 219 F.3d 698 (7th Cir. 2000), defendants defrauded nearly thirty investors out of more than $15 million by marketing "prime bank instruments," which they described as multi-million-dollar letters of credit issued by the top fifty or one-hundred banks in the world. As the Seventh Circuit explained, defendants

> told their victims that they could purchase these instruments at a discount and then resell them to other institutions at face value; the difference in price represented the profits that would go to the defendants and their "investors." This was nothing more than a song and dance: the trades were fictional; there was no market for the trading of letters of credit; and nothing capable of generating profits ever occurred. Somehow, notwithstanding the implausibility of "prime bank instruments" to one familiar with normal business practice for letters of credit, they managed to persuade their victims to give them money to finance the purchase of phantom discounted instruments. While this did not earn a cent for any of the investors, it definitely changed the defendants' own lifestyles.

Id. at 859-860. Among those convicted in *Polichemi* were attorneys, salespeople, an individual who acted as a reference, and *Polechemi*, who claimed to be one of the few people in the world with a license to trade prime bank securities.

In a related case, *United States v. Lauer*, 148 F.3d 766 (7th Cir. 1998), Lauer, the administrator of an employee pension fund, plead guilty to diverting millions of dollars to the prime bank scheme prosecuted in the *Polichemi* case. In rejecting Lauer's appeal on the loss calculation for sentencing purposes, the Seventh Circuit upheld the trial court's use of an intended loss figure, rather than a lower actual loss amount.

In another recent case, *S.E.C. v. Lauer*, 52 F.3d 667, 670 (7th Cir. 1995), Chief Judge Posner declared

> Prime Bank Instruments do not exist. So even if [a co-schemer] had succeeded in raising money from additional investors, it would not have pooled their money to buy Prime Bank Instruments. It would either have pocketed all of the money, or, if what its masterminds had in mind was a Ponzi scheme, have pocketed most of the money and paid the rest to the investors to fool them into thinking they were making money and should therefore invest more (or tell their friends to invest).

In *United States v. Richards*, 204 F.3d 177 (5th Cir. 2000), the Fifth Circuit upheld defendants' convictions for conspiracy, wire fraud, mail fraud and interstate transportation of stolen property. At trial, the government presented the following evidence describing how defendants induced participants to invest in a "roll program":

> Potential investors were told that their money would be pooled with that of other investors and used to buy letters of credit. The letters of credit would be "rolled"-- sold, repurchased, and resold -- to European banks frequently and repeatedly. Each "roll" would generate a large profit to be distributed among the investors, in proportion to their investment. The investors were told that their funds would be safe at all times, held either in an account at a nationally-known brokerage firm or invested with a "prime" or "top 50" international bank. Investors were also told that they would receive at least the return of their initial investment, with interest, and would likely make substantial profit. In fact, the defendants took the invested funds for their own use, bought no letters of credit, and, except for a small payment to one participant, returned no money to the investors.

Id. at 185.

In *United States v. Rude,* 88 F.3d 1538, 1548 (9th Cir. 1996), defendants were charged with engaging in a prime bank scheme. In affirming their convictions, the Court of Appeals found, among other things, that the government had proved beyond a reasonable doubt "that the very

notion of a 'prime bank note' was fictitious," and cited other evidence that the term "prime bank" was not used in the financial industry "and was commonly associated with fraud schemes." *Id.* at 1545.

In *Stokes v. United States*, No. 97-1627, 2001 WL 29997, at *1 (S.D.N.Y. Jan. 9, 2001), defendant was convicted of conspiracy, wire fraud, money laundering and interstate transportation of fraudulently obtained money. Defendant claimed that "through various personal connections in the banking industry, he could purchase and sell 'prime bank guarantees' or letters of credit and make a substantial profit in a short period of time, with no risk to the investor." As is typical in these kinds of cases, the defendant attempted, unsuccessfully, to portray himself as a victim, as someone unwittingly conned by co-conspirators to carry out the fraud.

A number of other criminal cases involving prime bank schemes have also been reported. *See e.g., United States v. Wonderly,* 70 F.3d 1020 (8th Cir. 1995); *United States v. Hand*, No. 95-8007, 1995 WL 743841 (10th Cir. Dec. 15, 1995); *United States v. Aggarwal*, 17 F.3d 737 (5th Cir. 1994); *United States v. Gravatt*, No. 90-6572, 1991 WL 278979 (6th Cir. Dec. 27, 1991); *United States v. Lewis,* 786 F.2d 1278 (5th Cir. 1986). There are also a number of reported civil cases brought by the S.E.C. *See*, e.g. *S.E.C. v. Milan Capital Group, Inc.,* No. 00 Civ. 108 (DLC), 2000 WL 1682761 (S.D.N.Y. Nov. 9, 2000); *S.E.C. v. Kenton Capital, Ltd.,* 69 F. Supp.2d 1 (D.D.C. 1998); S.E.C. v. Infinity Group., 993 F. Supp. 324 (E.D. Pa. 1998), *aff'd,* 212 F.3d 180 (3d Cir. 2000); *S.E.C. v. Deyon*, 977 F. Supp. 510 (D. Me 1997); *S.E.C. v. Bremont*, 954 F. Supp. 726 (S.D.N.Y. 1997).

Assistant U.S. Attorney Michael Schwartz in Houston prepared an excellent memorandum titled "United States' Memorandum of Law Concerning Fraudulent High-Yield or International 'Prime Bank' Financial Instrument Schemes," a copy of which can be obtained from either him or the Fraud Section. Appropriately modified versions of this memorandum can not only be used to educate your trial judge on the legality of such schemes, but also excerpted for use in search warrant affidavits.

IV. First steps

While the particular facts presented in each case will obviously dictate which steps you should first take in investigating a prime bank or high yield investment program (HYIP) scheme, we have found the following to be generally very useful:

- **Check subject's background:** Check to see if the subject has a criminal record, or if his name appears anywhere in FBI indices. Check with other agencies as well, since these types of investigations are handled not only by the FBI, but also by Customs, Secret Service, IRS-CID, or the Postal Inspection Service. Many prime bank scammers are career cons who have been previously convicted of fraud. Prime bank scammers also seem to operate within an extensive network, using each other to broker or solicit investments in particular HYIP schemes, to backstop some fraudulent claim, or to help create a "plausible deniability" defense. Therefore, your subject may have been interviewed in the past by an agent in another matter and made statements that could prove useful in your case. If you are fortunate, you will find that an agent expressly put your subject on notice in the past as to the fraudulent nature of prime bank trading programs. Such notice would substantially aid your efforts in establishing probable cause for a search warrant and generally in proving the subject's fraudulent intent.
- **Contact the Securities and Exchange Commission:** The SEC actively investigates and prosecutes prime bank fraud as securities fraud. Your subject may be, or has been, involved in a SEC investigation. If so, this would also help build probable cause for an eventual search warrant, and prove intent at trial. If the SEC has not investigated your subject, you should consider asking them to do so. Contact either your regional SEC office or Brian Ochs, Assistant Director, Division of Enforcement, SEC at (202) 942-4740 in Washington, D.C. (*See* Tips below).

- **Contact Jim Kramer-Wilt and Bill Kerr:** Jim Kramer-Wilt is an attorney in the Treasury Department's Bureau of Public Debt and has taken a very active role in attempting to expose and combat prime bank fraud. He has compiled an extensive database on known and suspected prime bank scammers and will readily share with you the database, as well as other useful materials. In all likelihood he will have, or can get, some background information about your subject. He may be reached at (304) 480-8690. Bill Kerr, with the Enforcement and Compliance Division, Office of the Comptroller of Currency, may also provide some valuable information about your subject, particularly if a bank has filed a Suspicious Activity Report (SAR) with the OCC, or has otherwise made an informal inquiry to the OCC or Federal Reserve about a particular financial transaction or investment. His number is (202) 874-4450.
- **Locate subject's bank accounts and/or assets:** These cases typically involve millions of dollars of victims' funds, and are often directed at wealthy individuals or institutions, with minimum investment levels (e.g., $25,000) and representations that "trades" can not be entered until $100 million has been pooled. Although offshore accounts are frequently used in these schemes, surprisingly enough, you will often find that the subject still has large sums on deposit in accounts at United States banks under his control. This may be because he has not yet transferred the funds offshore, or perhaps because, as part of his scheme, the funds are being maintained in an alleged trust account so he can assume the persona of a well financed investment manager with the bank employees. At any rate, to locate the accounts is important, in order to determine the scope and nature of the fraud, as well as prepare for ultimate seizure of the funds. A subject's account can usually be identified by asking a victim for the wiring instructions that he received from the subject. Accounts can also be located through other means, including mail drops, trash runs, the clearing process of a victim's check, and grand jury subpoenas. Of course, the likelihood that the subject has used more than one account is high. In determining whether to seize the account, informally contact the financial institution's security officer to get a rough idea of how much is in the account.
- **Consider initiating a proactive approach:** The most difficult element to prove in a prime bank case, as with most investment frauds, is fraudulent intent. The most common defense is, "I didn't know those trading programs didn't exist. I believed Mr. X when he told me they did." Therefore, it is important at the start of an investigation to plan how to overcome this defense. The FBI has developed a number of different proactive approaches that have proven successful in establishing the requisite intent that will substantially assist you in prosecuting your case. Indeed, in most instances, the defendant will enter a plea after being confronted with such evidence. For one successful prosecution resulting from a sting operation, see *United States v. Klisser*, 190 F.3d 34 (2d Cir. 1999).
- **Execute search and seizure warrants:** As soon as you have been able to determine the nature and scope of the fraud, you should consider applying for search and seizure warrants.
- **Victim questionnaires:** Many of these cases involve hundreds, if not thousands, of potential victims. Questionnaires sent out to victims have proven to be an excellent way to quickly collect evidence, including witness statements and documents, which you can then review for possible in-depth interviews later. Obviously, this should be done only once the existence of the investigation becomes public. Questionnaires are also a good way to gauge the degree of cooperation you can expect to receive from victims,

who oftentimes in these Ponzi type schemes do not feel "victimized". (See Section VII below).

V. Pssst... here are a few good "tips"

Identifying the existence of a prime bank investment scheme is clearly easier than determining the scope of the scheme, or trying to explain to a jury precisely what is meant by (or supposedly meant by) such terms as "prime bank discounted negotiable debenture" or "World Bank high-yield humanitarian trading program." The following tips will hopefully help you build and prove a case.

- **Keep it simple**: Once you determine the target or targets, focus your investigative efforts on building the strongest case against them without trying to uncover every transaction or proving every illegal act they may have committed. First, as a practical matter, you simply can not include every transaction. These schemes are often quite broad in scope and can often meld into other investment schemes. Stay focused on the heart of the case you are developing. Attempting to be all-inclusive can be a waste of time and resources. By focusing on the key transactions, you can present a case that the average juror will understand. Second, you need not include each and every victim. More than likely, the majority of the scheme can be proven through a handful of victims. Use your best witnesses. Often these are people who retained investment contracts they executed with the targets or who remember specific misrepresentations. The details regarding the other victims can be saved for the sentencing phase. Third, you need not endeavor to disprove the myriad of misrepresentations made to the victims. Prime bank schemes are often based on a series of misrepresentations that seem, at least to the investors at the time, to have some basis in reality. You are better off focusing on the material misrepresentations that establish the nature of the scheme than disproving each of the various ancillary misrepresentations. Proving that the subject did not invest investor funds, but instead spent for his personal benefit, is easier than disproving a tale about the World Bank, the IMF, or the yield on prime bank notes from an emerging nation. In short, do not argue on the defendant's terms. Just show that the defendant did not invest the money as promised.
- **Get a financial analyst assigned to the matter**: Reaching out and utilizing the full range of tools available to a prosecutor can go a long way towards turning an investigation into a prosecutable case. Having an FBI Financial Analyst (FA) assigned early in the investigation can help in a number of ways. First, an FA can review the pages and pages of bank records and determine how the subject transferred, concealed and eventually spent the victim's invested funds. Second, in many of these cases, checks and wire transfers go back and forth between the accounts of targets, investor-victims, and brokers who bring victims into the scheme. A thorough review by an FA can help determine who's who. Further, an early review will most likely unearth additional victims, either because they sent funds into a target's account or because they received lulling payments from the target's accounts. Interviews of these witnesses may yield additional counts of fraud and money laundering pursuant to 18 U.S.C. §§ 1956 (lulling payments) and 1957 (spending of proceeds from a "specified unlawful activity"). Third, the FA will generally be able to identify additional bank accounts into which the subject is secreting proceeds. Such information will provide additional accounts to subpoena, including foreign accounts of which you may not have known. Identifying the foreign accounts as early as possible is important because of the time involved in attempting to obtain that information.
- **Get MLATs out early**: If you anticipate

needing evidence from abroad, you should contact the Office of International Affairs (OIA) in Washington, D.C. at (202) 514-0000 to initiate the steps necessary to obtain such information. The United States has Mutual Legal Assistance Treaties (MLAT) with many nations, establishing a framework for obtaining evidence from another country. For those countries with which we have no MLAT in force, OIA can advise you on the appropriate means by which to obtain the requested information. OIA will provide you with a format-request for your particular country, which you will need to complete and return to OIA. MLATs can be used to obtain authenticated foreign documents and testimony abroad, execute search warrants, and seize funds.

- **Get started soon:**

  Once OIA has forwarded your request on to the foreign country, the requested evidence can take months to arrive. As discussed above, bank security officers can often tell you if an account is active and if there are funds in the account. Obtaining this information through informal channels can help determine if you need to wait for a response to an MLAT request. In the meantime, you may receive the collateral benefit of encouraging the foreign authorities to open their own investigation, which may later provide you with an invaluable level of cooperation.

- **Don't go it alone**: Coordinating with other agencies can save time and effort. While you must be mindful of the non-disclosure obligations of Rule 6(e), working with the SEC, IRS, NASD, and other federal and state regulatory agencies can save a great deal of time. These agencies and regulators may have investigations underway and may have collected useful information about your targets as well as potential victims. Often victims complain to the SEC or their particular state regulator, and, as a result, civil enforcement actions may already be underway. Working with the regulators and other arms of law enforcement is always preferable to working at cross purposes. Additionally, civil cases may already be in the works. Not knowing the full scope of the scam, victims often retain lawyers to pursue civil claims for breach of contact. These civil attorneys can also be a useful source of information. Finally, requesting information from FinCEN and the IRS may also prove to be useful.

- **Helpful websites**: A number of websites can be consulted in investigating a prime bank scheme. Two of the most useful are the Treasury Department's www.treasuryscams.gov and the SEC's www.sec.gov/divisions/enforce/primebank.shtml, both of which list numerous other very helpful links.

- **Don't reinvent anything**: More than likely, the target is operating in a similar, if not identical, manner to that of a number of other prime bank scammers. Consulting with other prosecutors who have handled these types of cases may save you time and effort. Furthermore, these prosecutors can provide you with materials such as sample indictments and search warrant affidavits. The Fraud Section, Criminal Division, in Washington D.C., (202) 514-7045, also has some guidance materials.

VI. Countering defenses - "It wasn't me"

Echoing the lyrics of a recent reggae-pop hit, when caught red-handed, even on camera, defendants will often claim simply "It wasn't me." The participants and funds of a particular prime bank schemes are often intertwined with other schemes. For the target or targets to send funds back and forth to other brokers or "traders" who are running similar schemes either in this country or offshore is not uncommon. Those brokers or traders often return the favor. The precise reason for these intermingled transactions is not entirely clear, but it does make tracing funds more difficult and sometimes gives defendants a built-in defense.

Defendants may claim that they sent an investor's money to Mr. X on the Isle of Man, and thus, like everyone else, were fooled by Mr. X, *i.e.*, "it wasn't me."

On March 15, 2001, in a case prosecuted by AUSA Linda M. Betzer of the Northern District of Ohio and Fraud Section Trial Attorney Glen G. McGorty of the U.S. Department of Justice, defendants Geoffrey P. Benson, Susan L. Benson and Geoffrey J. O'Connor were found guilty of twenty-one counts including conspiracy, mail and wire fraud, and tax evasion. The defendants were the former operators of The Infinity Group Company ("TIGC"), which collected over $26.6 million from over 4,400 victim investors across the country over a one and one-half year period. Through their *Financial Resources* newsletter, the defendants promised investors up to 181% return on their money, depending on the principal invested. The defendants claimed successful investment experience and business associations with individuals providing access to prime bank programs "ordinarily unavailable to the individual investor." The defendants promised the victims that their money would be pooled to purchase "prime bank instruments" in the European market with high guaranteed rates of return.

In reality, the defendants sold no product and offered no service. They had no investment experience, nor did they have any success with "prime bank investment" programs in Europe. In typical Ponzi/pyramid scheme fashion, they paid some investors in TIGC's "Asset Enhancement Program" with money collected from new investors, but the great majority of victims never received any money back from TIGC. In 1997 the State of Ohio, Department of Commerce, Division of Securities, and the federal Securities and Exchange Commission halted the TIGC operations, resulting in a court-ordered injunction of TIGC's sales activities. Of the $26 million collected by the defendants, a court-appointed trustee and forensic accountant collected almost $12 million in assets, which was subsequently returned to the victims. The alleged investments yielded no profits for the investors for over a year and a half, though TIGC allegedly sent approximately $11 million out of the $26 million to "investment programs" run by Geoffrey Benson's associates located around the world.

Though the defendants did not testify at trial, their attorneys argued through government witnesses and exhibits that the $11 million sent to these programs was evidence that the defendants believed the money they solicited from the investors was being invested in the prime bank programs they promoted in the newsletters. This defense attempted to convince the jury that the defendants were themselves victimized by Benson's associates and that they were acting in good faith in operating TIGC's Asset Enhancement Program. To refute this argument, the government demonstrated that the only assets the defendants enhanced were their own. As part of its case, the government called several expert witnesses, including an expert on international banking, who testified that the prime bank instruments and programs promoted by the defendants do not exist. The government highlighted the fact that only part of the received funds were invested, while the balance was placed in off-shore bank accounts or used by defendants to purchase an eighty-six acre plot of lakefront property, build a multi-million dollar home, and pay for many personal expenses. The government's fraud case focused on the misrepresentations contained in the *Financial Resources* newsletters. In these monthly mailings, the defendants not only lured investors with guarantees of high returns, but also lulled them by claiming successful investments and even starting a grant program using the "profits" of the trust's investments abroad. Over the period of the Asset Enhancement Program, TIGC's alleged $11 million investments yielded no profits — a clear inconsistency with what TIGC told its investors. The government succeeded in convincing the jury to focus on these lies and to understand that TIGC never intended any monies sent to its business associates to return a profit, but rather only to be hidden from any future investigating authority.

The jury found that the defendants were not victims as they claimed, but were guilty on all charged counts. Geoffrey Benson was ultimately sentenced to 360 months' incarceration, while Susan Benson and Geoffrey O'Connor each were

sentenced to 121 months' incarceration. All were ordered, jointly and severally, to pay $12,975,341 in restitution. All of the sentences reflected guideline enhancements for a fraud loss of over $20 million, more than minimal planning, mass marketing, violation of a judicial order, use of sophisticated means, and obstruction. Geoffrey Benson's sentence also reflected enhancements for his leadership role, an offense affecting a financial institution, and abuse of a position of trust.

Defeating this defense and proving intent can be accomplished in a number of ways. First, one of the proactive approaches discussed above can be used. After a target is put on notice by the government that prime bank trading programs do not exist and that claims to the contrary would be false, subsequent involvement by the target would not survive the "I too was duped defense." Second, circumstantial evidence can be used to establish intent. In most cases, an analysis by the FA will be able to show that a majority of investors' money did not go directly to the so-called "bigger fish," but instead went to accounts controlled by the target(s). Moreover, the amount of money sent to these other traders/brokers, the so-called "bigger fish," rarely coincides with the amounts invested. The lulling payments sent to other investors as interest also demonstrate intent since the fraudster misrepresents the true source of funds, *i.e.*, fellow investors. Intent can also be circumstantially proven through evidence of the defendant's conscious avoidance of various indicia of fraud or red flags associated with prime bank schemes. Third, experts can help show that the representations made to investor/victims were false on their face and that the lingo used to induce investors was made from whole cloth. *United States v. Robinson*, No. 98 CR 167 OLC, 2000 WL 65239 (S.D.N.Y. Jan. 26, 2000), contains a discussion of the use of an expert in a prime bank case.

Among government officials who have testified as experts in such cases are James Kramer-Wilt (Department of Treasury, Bureau of Public Debt (304) 480-8690); Bill Kerr (Office of the Comptroller of Currency (202) 874-4450); Herb Biern and Richard Small (Federal Reserve Board (202) 452-5235). There are also a number of private persons who provide expert testimony in these cases, *e.g.*, John Shockey (retired OCC official (703) 532-0943); Professor James Byrne (George Mason University Law School (301) 977-4035); and Arthur Lloyd (retired Citibank senior counsel (802) 253-4788). In addition, Jennifer Lester of the International Monetary Fund (202) 623-7130 and Andrew Kircher of the World Bank (202) 473-6313 may be able to provide assistance.

VII. Dealing with uncooperative victims

Unlike victims of some other crimes, victims of prime bank schemes often do not know or want to believe that they have been scammed. Often fraudsters have told them up front not to believe the government. Some prime bank victim/investors may, at least initially, refuse to cooperate with agents or prosecutors.

Many victim/investors are "true believers," who have received "interest payments" in a timely fashion and are often talked into "rolling over" or "reinvesting" their principal. While much of the principal has been secreted away by the fraudster, true believers remain convinced (or want to remained convinced) that the "high yield prime bank market" does exist and that their proverbial ship has come in. This belief, coupled with the non-disclosure, secret nature of the investment, prevents them from cooperating with the investigation, their reasoning being: "why risk breaching the non-disclosure provision of the contract by talking to the government when I'm getting paid?"

Most investors have been told that the government will deny the existence of the "programs," and that speaking to an FBI agent or other government agent will jeopardize the success of the secret programs, as well as bar them from any future opportunity to invest in these trading programs.

However, some investors may recognize the Ponzi scheme but want it to continue for just a few more payment periods so they can get their money back. These investors have little interest in seeing a speedy investigation and would rather be left alone so that they can get their money out before the roof caves in.

Dealing with each of these types of investors

can be difficult. However, being forewarned that you may encounter some of them will allow you to plan ahead. In our experience, a few low key meetings or phone calls from the agent will allow at least the first two categories of witnesses time to come to grips with reality. If they remain uncooperative, simply move on and concentrate on counts centered around more helpful witnesses.

VIII. Conclusion

Over the past decade, prime bank schemes have proven to be an incredibly durable form of Ponzi scheme by being able to adapt to changing conditions and obstacles. We can expect the scheme to continue to morph into whatever form necessary in an attempt to lure victims and evade detection. A vigorous and coordinated effort on the part of federal and state law enforcement and regulatory agencies is clearly needed. ❖

ABOUT THE AUTHORS

❑**Joel E. Leising** is a Senior Trial Attorney in the Fraud Section of the Criminal Division. He has investigated and prosecuted a number of prime bank cases in the past. He is a member of the Steering Committee of the Combating Prime Bank and Hi-Yield Investment Fraud Seminar of George Mason University Law School, and has been a speaker at the Seminar's annual meetings.✠

❑**Michael McGarry** has been a trial attorney in the Fraud Section of the Criminal Division since 2000. His casework includes matters involving "Prime Bank" or "High Yield Instrument" investment schemes. Prior to joining the Department, Mr. McGarry worked in private practice in the New York office of Fried Frank Harris Shriver & Jacobson for five years where he worked on large white collar criminal and regulator matters. Mr. McGarry has written articles published in newspapers and journals on money laundering regulation and procurement fraud.✠

Prosecuting Corporations: The Federal Principles and Corporate Compliance Programs

Philip Urofsky
Senior Trial Attorney
Fraud Section

Increasingly prosecutors must decide whether, in specific cases, a corporation should be prosecuted for crimes committed by one of its officers, employees, or agents. Since 1999, the Department's *Principles of Federal Prosecution of Corporations* have provided a framework for making this decision and have identified factors relevant to the determination. In the end, however, as in every criminal case, the essential question remains: should *this* corporation be prosecuted for *this* conduct?

I. Corporate criminal liability

Every law student learns early on of the concept known as the "legal person," *i.e.*, corporations. In law school, we are taught that to have a legal personality means that a corporation can be served with process and sued for tort damages and in contract disputes, and that the corporate form protects individual shareholders, including other legal persons, from liability except in those limited circumstances in which the "corporate veil" can be pierced. However, there was little discussion as to what the consequences

of having a legal personality might mean in the criminal law context.

The black letter law in this area is fairly simple. A corporation, having been granted legal personality, may be prosecuted to the same extent as a natural person. For the most part, federal criminal statutes make no special provision for corporations and simply assume that the same prohibitions applicable to natural persons are applicable to corporations. To the extent that this approach is vague, the first section of the *United States Code*, the "Dictionary Act," which provides "the words 'person' and 'whoever' include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals," resolves any ambiguity. 1 U.S.C. § 1. Particular statutes that find it necessary to be more explicit define the legal person extremely broadly or comprehensively. For instance, for all offenses in Title 18, a statutory definition provides: "As used in this title, the term 'organization' means a person other than an individual." Alternatively, in the Foreign Corrupt Practices Act, a person is defined as a natural person or "any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship." *See* 15 U.S.C. §§ 78dd-1(g)(2). On the other hand, Congress has provided a narrower definition when necessary to implement the specific goals of a particular statute. *See, e.g.*, 15 U.S.C. 78c(8) (defining "issuer" for purposes of the Securities Exchange Act of 1934 as only those "persons" who had issued or proposed to issue securities).

Obviously, a corporation, despite its legal personality, acts only through natural persons — its officers, directors, employees, agents, and, in certain circumstances, its shareholders — or through its subsidiaries, as well as the natural persons affiliated with them. In the former case, the law imposes what is essentially strict liability: a corporation is liable for the acts of a natural person acting within the scope of his or her duties and, at least in part, for the benefit of the corporation. *See United States v. Automated Medical Laboratories*, 770 F.2d 399 (4th Cir. 1985); *United States v. Cincotta*, 689 F.2d 238 (1st Cir. 1982). In the latter case, the parent corporation can only be held liable for the acts of its subsidiary or affiliate if it directed, ordered, or controlled the subsidiary's violation of the law. *See United States v. Bestfoods*, 524 U.S. 51, 52 (1998) (stating that "the corporate veil may be pierced and the shareholder liable for the corporation's conduct when, *inter alia*, the corporate form would otherwise be misused to accomplish certain wrongful purposes, most notably fraud, on the shareholder's behalf."); *Chicago, M. & St. P.R. Co. v. Minneapolis Civic and Commerce Assn.*, 247 U.S. 490, 501 (1918) (finding that the corporate veil may be pierced when subsidiary company is used as a "a mere agency or instrumentality of the owning company"). These rules apply whether or not a particular statute refers to parent corporation liability. *See United States v. Sutton*, 795 F.2d 1040, 1059 (Temp. Emer. Ct. App. 1986).

In most cases, the liability of the corporation for the acts of a corporate agent is not a matter of law but of prosecutorial discretion. As discussed below, charging a corporation is often justified and appropriate. On the other hand, the fact that a corporation is technically subject to strict *respondeat superior* for the acts of its employees, even if contrary to the corporation's policies and interests, requires a prosecutor to examine carefully the equities of charging a corporation under the specific circumstances presented by a particular case.

II. The principles of federal prosecution of corporations

The "Holder memo" of June 16, 1999 set forth the Department of Justice's policy in this area through the *Principles of Federal Prosecution of Corporations. See Bringing Criminal Charges Against Corporations* (last modified March 9, 2000) < http://www.usdoj.gov/criminal/fraud/policy/Chargingcorps.html>. These *Principles*, which were modeled on the familiar *Principles of Federal Prosecution* in the *United States Attorney's Manual*, § 9-27.000, are non-binding and are intended to guide a prosecutor in the exercise of his or her discretion, not to mandate a specific outcome in a particular case. They do, however, list factors that will help a prosecutor evaluate the appropriateness of

criminal charges and weigh the merits of the inevitable arguments by corporate defense counsel that his client was merely the victim of the acts of a "rogue employee" or, having already reformed itself, has no need of the corrective whip of a criminal prosecution.

The single over-arching principle governing charging corporations, as set forth in the *Principles*, is worth quoting in full:

> Corporations should not be treated leniently because of their artificial nature, nor should they be subject to harsher treatment. Vigorous enforcement of the criminal laws against corporate wrongdoers, where appropriate, results in great benefits for law enforcement and the public, particularly in the area of white collar crime. Indicting corporations for wrongdoing enables the government to address and be a force for positive change of corporate culture, alter corporate behavior, and prevent, discover, and punish white collar crime.

Corporate Prosecutions Principles at § I.A. However, "charging a corporation . . . does not mean that individual directors, officers, employees, or shareholders should not also be charged. Prosecution of a corporation is not a substitute for prosecution of criminally culpable individuals within or without a corporation." *Id*. at § 1.B.

Initially, prosecutors, in determining whether to charge a corporation, should apply the factors set out in the *Principles of Federal Prosecution*, such as sufficiency of the evidence, likelihood of success, and probable deterrent effect. *Id*. at § II.A (citing USAM § 9-27.220-27.260). When a corporation is the putative defendant, additional factors become relevant because of the artificial nature of the "legal person." As set forth in the *Corporate Prosecution Principles*, these factors are:

- The nature and seriousness of the offense, including the risk of harm to the public, and applicable policies and priorities, if any, governing the prosecution of corporations for particular categories of crime;
- The pervasiveness of wrongdoing within the corporation, including the complicity in, or condonation of, the wrongdoing by corporate management;
- The corporation's history of similar conduct, including prior criminal, civil, and regulatory enforcement actions against it;
- The corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents, including, if necessary, the waiver of the corporate attorney-client and work product privileges;
- The existence and adequacy of the corporation's compliance program;
- The corporation's remedial actions, including any efforts to implement an effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, to pay restitution, and to cooperate with the relevant government agencies;
- Collateral consequences, including disproportionate harm to shareholders and employees not proven personally culpable; and
- The adequacy of non-criminal remedies, such as civil or regulatory enforcement actions.

Id. at II.A (citations omitted).

Although some of these factors appear self-explanatory, the *Principles* provide additional guidance and discussion in subsequent sections, and the reader is encouraged to review these.

III. Attorney-client privilege waivers

A corporation's willingness to waive its attorney-client and work product privileges may be taken into account in evaluating a corporation's cooperation. *See id*. at II.A(4) and VI(A & B). Perhaps no aspect of the *Corporate Prosecution Principles* has caused more consternation in the defense bar than this simple statement. This

section has resulted in denunciations of the *Principles* as demonstrating the Department's full-bore attack upon the attorney-client privilege, its denigration of the important role played by corporate counsel, its attempt to override the Sentencing Guidelines, and its disregard for our nation's firmly embedded rights and liberties. *See, e.g., Conference Rep. on 15th Ann. Natl. Inst. on White Collar Crime: DOJ Guidelines on Corporate Waivers of Attorney Client Privilege Draws Criticism*, 68 Crim. L. Rep. 563 (Mar. 28, 2001); Loomis, *Privilege Waivers: Prosecutors Step Up Use of Bargaining Chips*, N.Y.L.J (Sept. 9, 2000) at 5; American Corporate Counsel Assn., *Letter to Hon. Eric Holder, Deputy Attorney General* (dated May 12, 2000) <www.acca.com/gcadvocate/advocacy/holder.html>; Breckinridge Willcox, *Attorney Client Privilege Waivers: Wrongheaded Practice?*, 6 No. 12 BUS. CRIMES BULL., Jan. 2000 at 1. These groups predict a parade of horribles arising from the suggestion that a waiver may sometimes be appropriate, including that corporations will no longer seek advice of counsel and will exclude counsel from corporate deliberations, and that counsel will not memorialize their advice or will destroy notes of meetings and interviews to avoid having to produce them at some later date to comply with a corporate cooperation agreement.

The reaction to *Corporate Prosecution Principles'* statement on waiver of the privilege has been overblown. The *Principles* do no more than acknowledge an existing practice that has long been used by the defense bar and prosecutors across the country. A prosecutor may request a waiver when necessary to enable him or her: (1) to determine the completeness of the corporation's disclosure; (2) to evaluate the accuracy of that disclosure; (3) to identify potential targets and witnesses; and (4) to obtain evidence to use in its investigation and any resulting prosecution. The Principles do not require, or even encourage, a prosecutor to seek a waiver in all circumstances, and they make it absolutely clear that such waivers are not absolute requirements for cooperation. *Corporate Prosecution Principles* at VI.B.

However, such waivers are sometimes critical, and the *Principles* acknowledge the importance of such waivers in evaluating a corporation's cooperation. The reasons why such waivers are sometimes necessary are not hard to discern, and, indeed, some are even tacitly acknowledged by members of the defense bar. For instance, as noted by, Breckinridge Willcox, former United States Attorney for the District of Maryland, "Corporations on occasion have made carefully considered *strategic decisions* to produce *some of this material* to the prosecutors, often preceded by a plan *to minimize* or *to shape* the work product that may later be disclosed." *Supra* (emphasis added). This is precisely the evil that the *Principles* seek to avoid. A corporation that seeks leniency must be fully forthright. It cannot pick and choose which crimes it will admit or against which employees it will provide evidence. Either it cooperates or it does not; no middle-ground exists.

The corporate bar's reliance on the absence of a waiver requirement from the Sentencing Guideline's definition of a corporation's cooperation, *see* U.S.S.G. § 8C2.5, demonstrates a fundamental misunderstanding of the purpose of the *Corporate Prosecution Principles*. Although the Sentencing Guidelines clearly encourage self-reporting and cooperation, they apply only when a corporation has already been charged and convicted. Thus, they have no relevance to determining whether that corporation should be charged in the first place. Section 8C2.5 permits a court to mitigate a convicted corporation's punishment in recognition of its cooperation. The Guidelines, however, do not attempt to limit the scope of a cooperation a corporation may or should provide to the government.

The *Principles*, on the other hand, are explicitly intended to guide a prosecutor's discretion in determining whether or not to bring charges against a corporation. The critical distinction at work here is between leniency at the charging stage and mitigation at the punishment stage. A corporation, in approaching the government and offering to cooperate, is asking that the government refrain from charging it for the crimes it admits to committing. This is not something which a corporation can automatically earn simply by coming to the government in the first place. To echo John Houseman in that old

Smith Barney ad, a corporation that has committed a crime is not *entitled* to leniency; it must *earn* it.

One way that a corporation may earn leniency is by fully cooperating with the government by not holding back any relevant information in its possession. Contrary to the corporate defense bar's assertions, the *Principles* do not authorize or encourage a prosecutor to trespass in the defense camp. Indeed, the *Principles* clearly state that, when a prosecutor requests a waiver, "[t]his waiver should ordinarily be limited to the factual internal investigation and any *contemporaneous* advice given to the corporation concerning the conduct at issue. Except in unusual circumstances, prosecutors should not seek a waiver with respect to communications and work product related to advice concerning the government's criminal investigation." *Corporate Prosecution Principles* at VI.B. n.2 (emphasis added).

It is highly unlikely that the possibility of a future waiver will result in the host of problems predicted by the corporate bar, even if waivers were routinely requested. Corporations are unlikely to avoid seeking legal advice for fear of having to disclose it down the road. Only a foolish corporate board would choose to proceed blindly down complex regulatory and legal paths in the hope that its employees would manage either not to violate the law or not to get caught doing it. Further, discerning what advantage a corporation would obtain by excluding lawyers from meetings concerning compliance issues is difficult. Assuming that the corporation wishes to obey the law, someone will presumably have to advise it on how to do so. The advice received, if it came from a non-lawyer, would be discoverable in both criminal and civil proceedings and would not even provide the cloak of an advice of counsel defense. Finally, as former Assistant Attorney General for the Criminal Division, James Robinson noted, "[H]aving been a corporate attorney myself, I doubt that any competent and ethical attorney would destroy records or attempt to give advice in a complex area based solely upon his recollection of interviews and meetings simply to avoid discovery." *Reader Offers Some Clarifications of Prnciples of Federal Prosecution of Corporations,* 7 No. 4 BUS. CRIMES BULL., May 2000 at 3.

IV. Compliance programs

In talking with an attorney representing a corporation in a criminal investigation, a prosecutor will inevitably hear the talismanic phrase, "rogue employee." Corporate counsel will argue that, although, in the words of former President Reagan, "mistakes were made," charging the corporation, even if it is technically liable, for the acts of one or more rogue employees who were acting against corporate policy and without the approval of sufficiently senior management is not appropriate. In making this argument, corporate counsel will point to the existence of a corporate compliance program as evidence of the corporation's efforts to be a law-abiding corporate citizen.

Such arguments should not be dismissed out of hand. The rogue employee is truly a rare animal, but, as the *Corporate Prosecution Principles* recognize, the existence or the remedial implementation of a corporate compliance program are only relevant factors in determining whether to charge a corporation. *Corporate Prosecution Principles* at II.A(5 & 6). A corporation should be permitted, in most cases, to attempt to demonstrate to the prosecutor's satisfaction that the wrongdoer was truly on a "frolic," such that the corporation should not be held liable for his or her conduct.

What, then, is a corporate compliance program? For the most part, each program is tailored to the lines of business and organizational structure of its corporation. Generally, however, a compliance program is a corporate policy, together with implementing mechanisms, that is intended to detect and deter, and if possible, prevent altogether, wrongful conduct by a corporation's employees and agents. Although particular programs may vary depending upon the size and complexity of the corporation, compliance programs will include, at a minimum, the following components: (1) a designated compliance officer or department, which may or may not be within the general counsel's office, that is charged with monitoring compliance issues, conducting or reviewing due diligence on business opportunities, and investigating alleged wrongdoing; (2) a training program to educate employees and agents concerning corporate

policies and applicable laws, rules, and regulations; and (3) a mechanism for reporting wrongdoing to management or the Board of Directors for appropriate action. The program should be designed to detect "red flags," which would indicate the potential for running afoul of the law and provide appropriate mechanisms for investigation.

Whether a corporation has a compliance program and whether it is effective is relevant at three stages of a prosecution: charging, plea negotiations, and sentencing. As noted, the *Corporate Prosecution Principles* specifically refer to compliance programs as a factor in determining whether to charge a corporation. In addition, a prosecutor who has already decided to charge or has obtained an indictment of a corporation, may wish to impose compliance requirements in a corporate plea agreement. Finally, the Sentencing Guidelines specifically refer to the existence of a compliance program as one factor in determining whether to reduce a corporation's sentence. *See* U.S.S.G. § 8C2.5(f).

At the charging stage, which is the focus of this article, several factors are worth remembering. First, the Department, as a whole, encourages self-policing. *Corporate Prosecution Principles* at VI.A. Of course, committing no crime is better than seeking forgiveness for one later. Second, the existence of a compliance program, whether adequate or not, is not, in and of itself, sufficient to prevent a corporation from being charged for criminal conduct by its officers, directors, employees, or agents, nor is it a legal defense. *Id*. Indeed, the fact that a crime was committed, notwithstanding the existence of a compliance program, may call into question the adequacy of the program or the corporation's commitment to compliance. Third, although the existence of compliance programs is a *factor* in the charging decision, no uniform Department policy on the weight that must be accorded this element exists. For instance, although the Antitrust Division, as a matter of policy, will not consider compliance programs in determining whether to bring charges, it nevertheless encourages corporations to implement such programs to detect wrongdoing early enough for the corporation to take advantage of the Antitrust Division's amnesty program. *Id*.

In evaluating a corporation's plea for leniency based on the existence of its compliance program, *i.e*., that it had a stated policy against the wrongful conduct and a program to detect, deter, and prevent such conduct, the prosecutor should approach the issue in three stages: threshold, substantive, and retrospective.

First, at the threshold level, the prosecutor should ask: *Is the nature of the crime, or the corporate conduct that led to it, such that little or no weight should be given to the existence of a corporation's compliance program?* Some crimes, for whatever reason, simply require prosecution, and the prosecutor need not engage in a pointless exercise. *See Corporate Prosecution Principles* at II.A(1) and III. For other crimes, the prosecutor should first attempt to determine the pervasiveness of wrongdoing within the corporation and the involvement of management. *See id.* at II.A(2) and IV. Obviously, if the conduct was a tacitly accepted common practice within the corporation as a whole, or within the relevant business unit, the corporation was not committed to compliance and should get no credit for a paper compliance program. Similarly, if the corporation's management, which is ultimately responsible for the corporation's conduct, not to mention implementing and monitoring any compliance program, participated in the conduct, the compliance program cannot be deemed to be true expression of corporate policy. Indeed, where corporate management is involved, further inquiry is usually unnecessary.

Other factors that are relevant at this threshold level include the corporation's prior history of similar conduct and whether it was prosecuted, or otherwise sanctioned, for such conduct. *See id*. at II.A(3) and V. For some crimes, a corporation's remedial actions may be relevant. *See id*. at II.A(6) and VIII. For instance, in the context of environmental crimes, the Environmental and Natural Resources Division places a premium on a corporation's willingness promptly to implement voluntary remedial clean-up and decontamination efforts. Finally, the corporation's self-reporting of the wrongful conduct and its willingness to

cooperate in the government's investigation are relevant factors. *See id.* at II.A(4) and VI.

If the corporation surmounts this threshold evaluation, the next step is to conduct a substantive review of the corporation's compliance program and to ask: *Does a true corporate commitment to compliance exist?* In practice, this means giving the corporation and its attorneys an opportunity to persuade you that the program is not merely a paper program — that the corporation really means what it says and is, and has been, willing to back it up with resources and commitment. In evaluating this claim, the prosecutor should evaluate whether: (1) the program is an off-the-shelf program or is specifically tailored to detect and deter conduct within this corporation; (2) the corporation has devoted sufficient resources, including audit and investigative staff; (3) it has conducted adequate and periodic training; (4) it provides for reporting to the highest levels of management; and (5) it has imposed discipline upon officers, employees, and agents found to have violated its compliance policies.

Finally, having reviewed the specific compliance program, the prosecutor should conduct a retrospective review and ask: *If the program was properly designed, supported by corporate management, and properly implemented, what went wrong?* The corporation's easy answer at this stage, of course, will be that this was a rogue employee who ignored the corporation rules and procedures. Fair enough, if true. The prosecutor, however, should demand that the corporation demonstrate some evidence that the so-called rogue employee deliberately evaded the safeguards imposed by the compliance program and that the corporation was not put on notice of this conduct in time to prevent the wrongdoing. For instance, the prosecutor should inquire whether any calls were made to the compliance program's "hot line" or whether any audit uncovered unexplained or unauthorized transactions. Did the corporation conduct adequate due diligence and did it follow up on red flags? Did the program provide for ongoing due diligence and monitoring, such as by periodic audits, and did the corporation conduct such continuing due diligence in this instance? Finally, as a result of discovering this conduct, albeit perhaps too late, has the corporation identified gaps in its compliance program, and has it taken steps to close those gaps?

The bottom line comes back to the very first question in the threshold stage of the review: *Does this corporation need to be charged?* It may be that the crime or underlying conduct was not enough for the prosecutor to dismiss the relevance of the compliance program out of hand, but, after hearing the corporation out, the prosecutor remains unconvinced that the corporation's compliance program, even if coupled with other factors such as cooperation and remediation, justifies not charging it for the crime. In such cases, the corporation *should* be charged, and the corporation will receive credit for its compliance program at sentencing.

V. Conclusion

Corporations are valid targets of criminal investigations and valid defendants in criminal prosecutions. An appropriate prosecution of a corporation may serve the goals of both specific and general deterrence, *i.e.*, it may deter this corporation (and its employees) from continuing to commit the same crime in the future, and it may persuade other corporations not to start. Such a prosecution may be necessary to change a corrupt corporate culture or to remove corrupt management from an otherwise clean company. In the end, the decision whether to charge is that of the prosecutor. The *Corporate Prosecution Principles* help provide a framework within which to make this decision.❖

ABOUT THE AUTHOR

❑**Philip Urofsky** is a Senior Trial Attorney with the Criminal Division's Fraud Section. He is responsible for the investigation and prosecution of violations of the Foreign Corrupt Practices Act and other white collar crime offenses and participates as one of the United States' designated experts in the Organization for Economic Cooperation and Development Working Group on Bribery's peer review process. Mr. Urofsky was also the principal drafter of the Federal Principles of Corporate Prosecution and

often acts as an adviser on attorney-client and corporate criminal responsibility issues.✠

Ex Parte Contacts with Corporate Employees

Edward I. Hagen
Attorney-Advisor and Assistant Director
Publications Unit
National Advocacy Center

I. Introduction

Difficult ethical issues arise in cases where a company that is the subject of a criminal investigation seeks to extend the coverage of the attorney-client privilege to cooperating employees. General guidance on this topic is provided in an article in last November's *United States Attorneys' Bulletin*, "Know the Professional Responsibility Issues that You May Confront," by Claudia J. Flynn, Director, Professional Responsibility Advisory Office (PRAO), and Joan L. Goldfrank, Senior Legal Advisor, PRAO. The authors of that article noted that the applicable ethical rules differ, depending on the state and local rules adopted by federal district courts, so there can't be any hard and fast guidance. The same approach is taken here. This article will take a closer look at some of the rules, and two recent cases discussing the rules, but the reader should recognize that the final decision in any case will be closely tied to a study of the facts of the instant case, local practice, and advice from your local ethics officer and the PRAO.

II. ABA Model Rules

Most jurisdictions follow the American Bar Association Model Rules. 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.

This wording is substantially identical to DR 7-104(A)(1). The application of Rule 4.2 to contacts with corporate employees is confirmed in the official commentary to the Rule:

> [4] In the case of an organization, this Rule prohibits communications by a lawyer for another person or entity concerning the matter in representation with persons having a managerial responsibility on behalf of the organization, and with any other person whose act or omission in connection with that matter may be imputed to the organization for purposes of civil or criminal liability or whose statement may constitute an admission on the part of the organization. If an agent or employee of the organization is represented in the matter by his or her own counsel, the consent by that counsel to a communication will be sufficient for purposes of this Rule.

It should also be noted that Rule 8.4(a) prohibits an attorney from violating the rules through the acts of another. This means that agents working on the case with a Department attorney may also be bound by Rule 4.2. Finally, ABA Model Rule 4.4 prohibits methods of obtaining evidence that violate the legal rights of another. This may prevent communications that seek the disclosure of information that is protected by a legal privilege or a contractual agreement.

The Rule does not prohibit contact with former employees. ABA Opinion 91-359 (March 22, 1991).

III. The "Authorized by Law" exception and 28 C.F.R. Part 77

In the past, the Department of Justice has attempted to expand the range of permissible contacts by publishing administrative rules in 28 C.F.R. Part 77. The idea was that the conduct outlined by those administrative rules would fall under the "authorized by law" exception in Rule 4.2. The Department could not be bound by stricter state rules, because the Supremacy Clause requires that federal officers be free from state control in the performance of their duties. Courts were generally unsympathetic to the Department's position. *See, e.g.*, *United States v. Ferrara*, 54 F.3d 825 (D.C. Cir. 1995); *In re Howes*, 940 P.2d 159 (D.N.M. 1997). In any event, this approach was abandoned on April 19, 1999, when 28 U.S.C. § 530B (the "McDade Amendment") took effect. McDade requires prosecutors to abide by the laws and ethical rules of the state where they are carrying out their prosecutorial duties. *See United States v. Talao*, 222 F.3d 1133, 1139 (9th Cir. 2000).

> **Note:** On October 21, 2001, the Department promulgated 28 C.F.R. §§ 500 and 501, which expand previous regulations regarding the monitoring of certain communications of inmates. See http://www.epic.org/privacy/terrorism/bop_rule.html for the full text.

IV. Pre-indictment contacts; reports of perjury and obstruction of justice—
United States v. Talao

Litigation in *United States v. Talao*, 222 F.3d 1133 (9th Cir. 2000), began when employees of the San Luis Gonzaga Construction, Inc. (SLGC) filed a complaint with the United States Department of Labor alleging that SLGC did not pay the prevailing wage, had required them to kick back a portion of their wages, and had made false statements to the government. Virgilio Talao was the sole owner of the corporation, and his wife, Gerardina Talao, was the secretary/treasurer. The local United States Attorney's Office initiated a criminal investigation of SLGC and the Talaos after a referral from its civil division. The Talaos were represented by an attorney named Christopher Brose.

A Department of Labor Special Agent served a subpoena on SLGC's bookkeeper, Lita Ferrer, directing her to testify before the grand jury. Virgilio Talao learned of the subpoena and instructed Brose to be present for Ferrer's testimony. Brose telephoned Ferrer and arranged to meet with her prior to her grand jury appearance. After the call Ferrer went to the United States Attorney's Office and asked to have the date of her grand jury appearance changed as she did not want Brose to be present before or during her grand jury testimony. She further stated that she would feel pressured to give false testimony if Brose was there, and recounted a telephone conversation she had with Mr. Talao in which he told her to "stick with the story" she had told while testifying in a related administrative action. Ferrer was told that the schedule would not be changed, but that Brose would not be in the grand jury room during her testimony.

Ferrer later met with Brose, discussed her grand jury appearance, and made plans to talk again at the federal building before she testified. Before that meeting could occur Ferrer saw the AUSA and Agent in the hallway outside the grand jury courtroom, and told them that she did not wish to be represented by Brose. They adjourned to a witness room, where Ferrer told them that she was not (and did not want to be) represented by Brose. The AUSA told Ferrer that she had a right to be represented by an attorney, and offered to arrange for a public defender at no cost, but Ferrer declined representation. Ferrer stated that she wished to tell the truth, that she did not believe she could do so if she had to testify in Brose's presence, and that the Talaos had been pressuring her to testify falsely. Ferrer then gave them detailed information about SLGC's payroll records and other corporate documents, and their possible destruction. While this was going on, Brose knocked on the door demanding an opportunity to speak with Ferrer. Ferrer was told that Brose wanted to talk to her, but she insisted that she did not want to see him.

At this point the AUSA decided to seek guidance from her Criminal Chief. He told her that, in his opinion, Brose was tampering with her witness, and instructed her to continue the interview. As the interview continued, Ferrer gave

examples of dishonest conduct by the Talaos that concealed the truth from federal investigators and Brose. Ferrer further stated that Virgilio Talao had told her to give false testimony to the grand jury, and that Talao had sent Brose to the grand jury to intimidate her. She went directly from that meeting to the grand jury, where these statements were made under oath. The grand jury returned a 20-count indictment against the Talaos and SLGC.

The Talaos and SLGC later filed a Joint Motion to Dismiss the indictment, arguing that the contact between the AUSA and Ferrer had violated California's Ethical Rule 2-100 (which substantially tracks the language of ABA Rule 4.2). The motion was denied, but the judge found that Rule 2-100 had been violated, and indicated an intent to inform the jury of the AUSA's misconduct and instruct the jury to take it into account in assessing Ferrer's credibility if the case went to trial. The AUSA (on her own behalf) appealed the order, and the govemment filed a petition for a writ of mandamus before the Ninth Circuit Court of Appeals to prevent the district court from giving its proposed remedial instruction at trial.

The court first had to deal with a jurisdictional issue; mere criticism of an attorney by a judge is not an appealable sanction. *See Weissman v. Quail Lodge, Inc.*,179 F.3d 1194, 1200 (9th Cir.1999) (words alone will constitute a sanction only "if they are expressly identified as a reprimand"). Here, however, the district judge made a finding and reached a legal conclusion that the AUSA knowingly and wilfully violated a specific rule of ethical conduct. "Such a finding, per se, constitutes a sanction . . . .We have no reluctance in concluding that the district court's finding of an ethical violation . . . is an appealable sanction." *Talao*, *id.* at 1138.

The court then turned to question of whether Rule 2-100 had been violated at all, since the contact involved pre-indictment and non-custodial communications, i.e., it occurred before a constitutional right to counsel had attached. The court adopted the reasoning of a Second Circuit case, *United States v. Hammad*, 858 F.2d 834 (2d Cir.1988). The *Hammad* court rejected the notion that the ethical rule was "coextensive" with the Sixth Amendment, and indicated an intent to take a case-by-case approach, balancing the need to police prosecutorial misconduct while recognizing that prosecutors are "authorized by law" to employ legitimate investigative techniques. *Id.* at 838-39.

Applying the *Hammad* approach to the facts in *Talao*, the Ninth Circuit found that the ethical rule applied; the parties were in "fully defined adversarial roles" even if the events were pre-indictment. *Talao*, *id.* at 1139. Nevertheless, the Ninth Circuit concluded that Rule 2-100 did not prohibit the AUSA's conduct.

> Despite the apparent conundrum created by Ferrer's dual role as employee/party and witness, the interests in the internal integrity of and public confidence in the judicial system weigh heavily in favor of the conclusion that [the conduct of the AUSA] was at all times ethical. We deem manifest that when an employee/party of a defendant corporation initiates communications with an attorney for the government for the purpose of disclosing that corporate officers are attempting to suborn perjury and obstruct justice, Rule 2-100 does not bar discussions between the employee and the attorney. Indeed, under these circumstances, an automatic, uncritical application of Rule 2-100 would effectively defeat its goal of protecting the administration of justice. It decidedly would not add meaningfully to the protection of the attorney-client relationship if subornation of perjury, or the attempt thereof, is imminent or probable.

Id. at 1140 (footnote omitted).

Talao does not suggest that a proper attorney-client relationship may not exist between corporations and employees who wish to cooperate with the government. However, "[o]nce the employee makes known her desire to give truthful information about potential criminal activity she has witnessed, a clear conflict of interest exists between the employee and the corporation. Under these circumstances, corporate counsel cannot continue to represent both the employee and the corporation." *Id.* at 1140-41 (footnote omitted). That conflict would have

prevented further sharing of information between the employee and an attorney representing the corporation. "Under these circumstances, because the corporation and the employee cannot share an attorney, ex parte contacts with the employee cannot be deemed to, in any way, affect the attorney-client relationship between the corporation and its counsel." *Id.* at 1141.

The court concluded by approving the conduct of the prosecutor in advising Ferrer of her right to contact substitute counsel. Although it would be improper to approach an employee represented by corporate counsel and initiate communications just because the prosecutor suspects a possible conflict of interest between the employee and the corporation, in this case there was no prior notice of the representation, and Ferrer initiated the communications with the United States Attorney's office. Far from being an ethical violation, the court formally approved of the AUSA's conduct. The sanction against the AUSA was consequently reversed, and the government's petition for writ of mandamus was dismissed as moot.

V. Conflicts with other federal statutes; application to lower level employees—*Weibrecht v. Southern Illinois Transfer*

Rule 4.2 is sometimes attacked as being in conflict with federal laws encouraging employees to report information to federal agencies, or as being inapplicable to lower level employees. *Weibrecht v. Southern Illinois Transfer*, 241 F.3d 875 (7th Cir. 2001), a wrongful death suit brought after the drowning death of a deckhand employed by the defendant, deals with both of these issues. Two days before a scheduled deposition, the plaintiff and his attorney initiated contacts with the pilot of the boat involved in the accident. These contacts formed the basis of a defense motion to dismiss. The motion was allowed and the plaintiff appealed.

Title 45 U.S.C. § 60 makes void any "contract, rule, regulation, or device whatsoever, the purpose, intent, or effect of which shall be to prevent employees of any common carrier from furnishing voluntarily information . . . as to the facts incident to the injury or death of any employee . . . ." The plaintiff argued that this provision superceded the ex parte contact rule; here, a local version of Rule 4.2 adopted by the local federal court. The Seventh Circuit noted that district courts are authorized to promulgate local rules under both Fed. R. Civ. P. 83 and 28 U.S.C. § 2071, but that both of these provisions state that local rules must be "consistent with Acts of Congress." Consequently, a local rule that conflicts with a federal statute is invalid. There is precedent for the view that 45 U.S.C. § 60 trumps Rule 4.2. *See Harper v. Missouri Pacific R.R. Co.*, 636 N.E.2d 1192 (D.Ill. 1994). Other courts have found that no conflict exists. *White v. Illinois Central R.R. Co.*, 162 F.R.D. 118 (S.D. Miss.1995); *Branham v. Norfolk and Western Ry. Co.*, 151 F.R.D. 67 (S.D.W.Va.1993); *State ex rel. Atchison, Topeka & Sante Fe R.R. v. O'Malley*, 888 S.W.2d 760 (D.Mo. App.1994). The *Weibrecht* court found the latter cases more persuasive. *Weibrecht*, *id.* at 880.

The plaintiff then argued that, even if there is no direct conflict between the provisions, Rule 4.2 was still not violated, because 45 U.S.C. § 60 brought him under the "authorized by law" exception. Once again the court disagreed. Title 45 U.S.C. § 60 does not "authorize" conduct, rather it prohibits conduct. *Id.*

This left the plaintiff with the argument that the pilot was not a "represented party." The court began by noting that there are a number of tests used in different jurisdictions that determine when an employee is a "represented party". Some courts will ban contacts with any employee, while others only allow coverage of top management employees who have decision-making responsibility. *Id.* at 881-82.The court below had applied the three part test suggested in Comment 4 to American Bar Association Rule 4.2 (quoted at the beginning of this article). A defendant's employee is considered to be represented by the defendant's lawyer if:

1. He or she has "managerial responsibility" in the defendant's organization;

2. His or her acts or omissions can be imputed to the organization for purposes of civil or criminal liability; or

3. The employee's statements constitute admissions by the organization.

Under that test, the pilot fit factors two and three. The appellate court, approving the use of the ABA three part test, consequently affirmed the decision that the pilot was a represented party. Nevertheless, the order dismissing the case was reversed as "too harsh a response to what appears to have been an honest but misguided attempt to comply with the ethical rules." *Id.* at 883.

VI. Conclusion

The rules governing contacts with employees of defendant corporations are complex, and vary from jurisdiction to jurisdiction. Although exceptions to the general no contact rule exist, extreme caution in interpreting these rules is essential. A prudent attorney will carefully research local rules and case authority, and consult with the local ethics officer and the Professional Responsibility Advisory Office.❖

ABOUT THE AUTHOR

❑**Ed Hagen** is an Attorney-Advisor and Assistant Director of Publications for the EOUSA's Office of Legal Education at the National Advocacy Center in Columbia, South Carolina. He is the co-author of *The Prosecution Function* (Lexington Books 1984) and *The Law of Confessions, Second Edition* (Westgroup 1994).✠

Navigating the Evolving Landscape of Medical Record Privacy

Ian C. Smith DeWaal
Senior Counsel
Criminal Division, Fraud Section

I. Introduction

The first compliance deadline for the "Standards for Privacy of Individually Identifiable Health Information"(45 C.F.R. Parts 160 and 164) (the "Medical Privacy Rule") looms little more than a year from now. Health care providers, health care clearinghouses, and large health plans, must comply by April 14, 2003, while small health plans must comply by April 14, 2004. Now is an opportune time to preview the Medical Privacy Rule, as well as review current law and Departmental guidelines concerning the disclosure and handling of individually identifiable medical information in the course of administrative, civil, and criminal matters handled by the Department. Importantly, this discussion applies not just to the investigation of health care fraud, but also to all litigating and investigative components of the Department, which seek or present evidence of written or oral medical information. This article presents a "nutshell" overview of the medical privacy arena for these components.

The Medical Privacy Rule governs only "covered entities" and their "business associates," as defined in the Rule. Typically, these are entities that actually create medical records, such as medical providers and insurance companies (including the Medicare and Medicaid programs). While certain offices or components of the Department may actually be "covered entities" as defined in the Medical Privacy Rule, and therefore must directly comply with the provisions of the rule, most components of the Department are not. For example, the Bureau of Prisons provides health care services to inmates and generates medical records. Nevertheless, the Rule effectively governs the Department's *access* to

medical records maintained by covered entities and their business associates and therefore affects the Department's affirmative and defensive efforts in all areas which require access to medical records. Health care fraud matters constitute a large, but not exclusive segment of these areas. This article does not purport to present a guide to those offices or components that are covered entities. Rather, this article focuses on the ability of the Department to obtain medical records under the Rule.

As with any overview, this article will only provide a general guide. In individual situations, specific reference to potentially applicable provisions will be required. However, awareness of these issues is of paramount importance.

II. Federal statutes and regulations in the medical privacy arena

A. "Standards for Privacy of Individually Identifiable Health Information" (Medical Privacy Rule)

The most recent federal statutes governing medical record privacy are found in the "Health Insurance Portability and Accountability Act of 1996." Pub. L. 104-191 (8/21/1996) (HIPAA). The Secretary of Health and Human Services promulgated the Medical Privacy Rule pursuant to several provisions of HIPAA, namely §§ 262 and 264, found at 42 U.S.C. § 1320d-2 and the Note thereto, respectively.

The Medical Privacy Rule provides an extensive regulatory framework, which will govern when and how the "covered entities," the health care providers, health care clearinghouses, and health plans will be permitted to disclose individually identifiable health information in their possession, termed "protected health information." The covered entities are required to comply with the Privacy Rule by April 14, 2003, with the exception of small health plans, which must comply by April 14, 2004. 45 C.F.R. § 164.534 (as amended 66 Fed. R. 12434 (2/26/2001)). The Medical Privacy Rule prohibits covered entities from disclosing protected health information to any third parties, including law enforcement agencies, unless the rules otherwise permit the disclosure. Therefore, while the Medical Privacy Rule does not directly apply to law enforcement, covered entities will certainly cite provisions of these rules in support of the assertion that they either permit or prohibit disclosures requested by law enforcement agencies.

Covered entities, from whom we seek protected health information, may not be fully conversant with the nuances of the regulations which permit disclosures to law enforcement or be aware that different disclosure rules apply in different situations. Prime examples are when law enforcement investigates a health care fraud matter, governed by the health oversight provisions contained in § 164.52 (d), and when law enforcement investigates a violent drug gang, governed by the general law enforcement provision § 164.512 (f). The entities may also be confused over the provisions of the regulation which state that the federal medical privacy regulations do not pre-empt certain more stringent state laws and regulations (§160.203), even though the courts have concluded consistently in the past that the Supremacy Clause of the United States Constitution insulates federal agencies from state and local laws.

As a general proposition, the covered entities are permitted to disclose protected health information to law enforcement for purposes of "health care oversight," (45 C.F.R.. 164.512(d)). This includes administrative, civil, and criminal investigations of health care payment or treatment fraud, government program fraud where health information is necessary to determine eligibility or compliance, and investigations of violations of civil rights laws where health information is relevant. 45 C.F.R. §§ 164.510 (defining "health oversight agency") and 164.512(d).

The Rule also permits covered entities to disclose protected health information for other types of investigations, unrelated to health care fraud. The provisions of 45 C.F.R. § 164.512 (f) govern general law enforcement investigations. This paragraph permits disclosure, for example, in response to grand jury subpoenas and court orders, but limits disclosures that may be made to locate or identify suspects, material witnesses, missing persons, or fugitives.

Other provisions will permit the disclosure of protected health information in various circumstances important to law enforcement. 45 C.F.R. § 164.512 (f) permits disclosure necessary to avert a serious threat to health and safety. 45 C.F.R. § 164.512 (g) authorizes disclosures to coroners and medical examiners. 45 C.F.R. § 164.512 (b) governs disclosures in matters involving child abuse, while 45 C.F.R. §164.512(d) governs disclosures in matters involving abuse, neglect, or domestic violence, which, in some instances, may require consent of the victim, absent a state law which compels disclosure without consent. A special rule permits covered entities to make disclosures to correctional institutions or in other law enforcement custodial situations. 45 C.F.R. § 164.512 (k)(6).

The Rule urges caution when an important need to protect the secrecy of an investigation exists. Under the Medical Privacy Rule, all covered entities must keep an "accounting" or log of each disclosure of a medical record, in the affected patient's file. 45 C.F.R. § 164.528. The entity must disclose that log to the patient on request. The Medical Privacy Rule provides for a delay in logging disclosures that are made to law enforcement, provided that the covered entity makes an oral request for delay in an urgent situation (e.g. hot pursuit tracking of an injured fugitive by contacting hospital emergency rooms), which will expire after thirty days unless followed up by a written request specifying the length of the delay sought, or the covered entity provides a written request which specifies the length of the desired delay in the first instance in non-urgent circumstances,. Law enforcement will have to act in a timely manner to protect the secrecy. Furthermore, the request will have to meet the strict requirements of the rule by stating that release of an "accounting" to the patient would be reasonably likely to impede the Department's activities, and by setting forth the length of the delay requested. 45 C.F.R. 164.528 (a)(2)(i).

B. HIPAA penalties: 42 U.S.C. § 1320d-5 and 1320d-6

For violation of the provisions of the statute and implementing regulations, HIPAA includes both civil monetary penalties and criminal penalties. The Office of Civil Rights of the Department of Health and Human Services investigates violations and assesses civil monetary penalties. 65 Fed. Reg. 82381 (12/28/2001). Section 1320d-5 of Title 42, United States Code, provides that civil monetary penalties may be assessed by the Secretary of Health and Human Services in the amount of $100 per offense. They may not exceed $25,000 against a single person in a single calendar year for violations of an identical requirement or provision. Section 1320d-5 further provides that civil monetary penalties may not be assessed when an act would constitute an offense under 42 U.S.C. § 1320d-6, the criminal statute.

For purposes of this discussion, the relevant portion of Section1320d-6 provides that: "(a) A person who knowingly and in violation of this part– . . .(2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section." Subsection (b) provides the penalties which may be assessed:

> A person described in subsection (a) of this section shall– (1) be fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

C. Substance Abuse Patient Medical Records Privacy statute and regulations (42 U.S.C. § 290dd-2 and 42 C.F.R. Part 2).

These provisions place strict limits on the disclosures which covered entities may make of substance abuse patients' medical records. Essentially, all disclosures of medical records created by federally-related substance abuse treatment programs are prohibited unless otherwise permitted by the regulations of the Secretary of HHS. 42 U.S.C. § 290dd-2 (b). The scope of medical records covered is broadly

interpreted, such as including billing for medical services with a diagnosis or treatment code for substance abuse. A federally assisted program or activity, or anyone releasing or receiving confidential substance abuse medical records without authorization, is subject to a fine. 42 U.S.C. § 290dd-2 (f); 42 C.F.R. § 2.4.

The mere rendering of substance abuse treatment or counseling does not, of itself, mean a provider's records are protected by this provision. A provider does not qualify as a covered "program" unless it is a physician, a group of physicians, or a unit within a facility, that "hold[s] itself out as providing and provides alcohol or drug abuse diagnosis, treatment, referral for treatment." 42 C.F.R. § 2.11. A "general medical care facility," *viz*., a hospital, will not be considered a covered "program" merely because hospital records may show that the patient is a drug or alcohol abuser, *unless* those records come from "[a]n identified unit within a general medical facility which holds itself out as providing, and provides, alcohol or drug abuse diagnoses, treatment or referral for treatment." 42 C.F.R. § 2.11. Therefore, the key inquiry is whether the provider, or the unit in a facility, holds itself out to the community as rendering substance abuse treatment and/or counseling.

The statute permits disclosure only if the patient consents, if necessary for treatment in a bona fide medical emergency, for scientific research, for program audits or evaluation (subject to limitations on re-disclosure), or if authorized by court order upon a strict showing of good cause. Different standards for obtaining a court order apply to use of substance abuse records: (1) in a criminal proceeding against the patient; (2) in a criminal proceeding against someone other than the patient; (3) in a civil proceeding; or (4) when placing an undercover agent in a substance abuse program. In addition, under the regulations, while a court order may authorize the disclosure of "confidential communications," but only if the disclosure is necessary " . . . to protect against an existing threat to life or of serious bodily harm . . . " as enumerated, or " . . . in connection with investigation of an extremely serious crime, such as one which directly threatens loss of life or serious bodily injury, including homicide, rape, kidnaping, armed robbery, assault with a deadly weapon, or child abuse and neglect ". 42 C.F.R. § 2.63 (a). The court order must set forth how patients, whose records are disclosed, are to be notified of the disclosure and given an opportunity to challenge the disclosure.

Generally, before the court may grant a disclosure order, the provider must give notice to the patients whose records are sought, with an important exception – notice is not required before a disclosure order is granted in a criminal investigation of a program or the person holding the records. 42 C.F.R. § 2.66 (b). However "upon implementation" of the order, the provider must afford the program, the person who held the records, or the patients whose records are disclosed, an opportunity to seek revocation or amendment of the order. Likewise, an order permitting the use of undercover agents or informants, may also be granted without notice on a showing of certain enumerated circumstances. 42 C.F.R. § 2.67 (b).

A court order is not necessary for a government entity to perform an "audit or evaluation" of a program to which it provides federal assistance or is authorized by law to regulate. 42 C.F.R. §§ 2.12, 2.53. Federal assistance can include tax exempt status, certification to participate in the Medicare program, direct grants, or a license to dispense controlled substances or operate a methadone clinic. Further, the term "audit or evaluation" includes a civil or administrative investigation of a program by the Department with respect to its obligation to exercise oversight of the Medicare or Medicaid programs. 42 C.F.R. § 2.53 (c).

Finally, even if disclosure of protected substance abuse medical records would otherwise be permitted, special rules apply to "confidential communications," which may be included in the protected records, and which limit the circumstances under which confidential communications may be disclosed. 42 C.F.R. § 2.63. One court has ruled that fraudulent billing is not "automatically" an "extremely dangerous crime" warranting the enforcement of a grand jury subpoena seeking records which include confidential communications and that it is highly unlikely that the government could ever make a

factual showing that fraud is sufficient to overcome the broad prohibition against disclosure of confidential communications contained in § 2.63(a). *In re The August, 1993 Regular Grand Jury*, 854 F. Supp. 1380, 1384-85 (S.D. Ind. 1994). A recent decision by the United States Court of Appeals for the Seventh Circuit held that even in the context of discovery in a civil proceeding, discovery orders issued by the district court must comply with the substance abuse patient medical records privacy regulations. *United States, ex rel Chandler v. Cook County, Illinois*, 277 F. 3d 969, 981-83 (7th Cir. 2002).

D. The Federal Privacy Act of 1974 (5 U.S.C. 552a)

While the Privacy Act does not single out individually identifiable medical information held by Federal Government agencies for any unique protection beyond other records maintained on individuals, it is relevant when the Department seeks identifiable medical information from other Federal Government agencies. The Privacy Act protects information about an "individual," that is collected and maintained by government agencies in a "system of records" ("covered records"). The Act defines a system of records as a system in which the information stored about an individual is retrieved by means of a personal identifier, such as a name, social security number, or driver's license registration number.

The Privacy Act protects covered records from disclosure, unless a specific provision of the Privacy Act permits disclosure. An individual may file a written request or provide a written consent for disclosure of his or her own covered records. Otherwise, authorization to disclose is provided by a statutory provision of the Act or by a "routine use," published by the agency holding the covered records. When Department attorneys or investigators seek medical information from an agency which maintains it in a covered system of records, then the Department's request and the disclosure by the agency, must comply with Privacy Act requirements.

Currently, agencies may disclose information subject to the Privacy Act, including medical information, to the Department under a number of provisions: 1) pursuant to 5 U.S.C. § 552a (b)(3) for a routine use as defined in §552a (a)(7) and described in § 552a (e)(4)(D); 2) for a civil or criminal law enforcement activity, provided that a written request specifying the particular portion of the record which is needed and the law enforcement activity for which the record is sought, § 552a (b)(7); or 3) pursuant to the order of a court of competent jurisdiction. § 552a (b)(11).

Some federal agencies have published additional routine uses for disclosing evidence of criminal activity to a law enforcement agency. For example, the Department of Health and Human Services has published a routine use which permits the disclosure of personal information concerning individuals to the Department of Justice, as needed for the evaluation of potential violations of civil or criminal law and for detecting, discovering, investigating, litigating, addressing, or prosecuting a violation or potential violation of law, in health benefits programs administered by the Center for Medicare and Medicaid Services (formerly the Health Care Financing Administration or HCFA). *See* 63 Fed. Reg. 38414 (July 16, 1998) (adding new routine uses).

Another important provision of the Privacy Act concerns computer database matching of covered records. A Privacy Act covered computer database may not be disclosed to the Department by another federal agency for use in a computer matching program, except pursuant to a written agreement meeting the enumerated statutory requirements between the source agency and the recipient agency. 5 U.S.C. § 552a (o). A "matching program" includes the computerized comparison of two or more automated systems of records or a system of records, with a non-federal system of records, to establish or verify the eligibility of, or continuing compliance with statutory and regulatory requirements by applicants, recipients or beneficiaries, participants, or providers of services with respect to Federal benefit programs, or for recouping payments or delinquent debts under Federal benefit programs. § 552a (a)(8). However, the term "matching program" does not include matches done by an agency which performs any function relating to the enforcement of the criminal laws as its

principle function, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against that person or persons. 5 U.S.C. § 552a (a)(8)(B)(iii). Questions of whether the computer database matching provisions of the Privacy Act apply in specific situations, should be directed to Barbara Bush, Deputy General Counsel of the Justice Management Division. Covered database matching projects are reviewed by the Data Integrity Board in the Department.

E. Peer Review Organizations 42 U.S.C. § 1320c:

Peer Review Organizations ("PRO") are tasked with reviewing and evaluating the performance of certain medical institutions or providers, and therefore, may have medical information that could be useful to Department attorneys or investigators. The Department can obtain the information held by peer review organizations only in a limited number of circumstances.

The general rule prohibits disclosure of any data or information acquired by a PRO in the exercise of its duties and functions, except where otherwise permitted. 42 U.S.C. § 1320c-9 (a). Nevertheless, an organization having a contract with the Secretary of HHS to engage in PRO activities, is permitted to disclose data and information which identifies specific providers or practitioners as may be necessary: "to assist Federal and State agencies recognized by the Secretary as having responsibility for identifying and investigating cases or patterns of fraud or abuse, which data and information shall be provided by the peer review organization to any such agency at the request of such agency relating to a specific case or pattern". 42 U.S.C. § 1320c-9 (b)(1)(A). However, a patient record in the possession of a PRO operating under a contract with the Secretary shall NOT be subject to subpoena in a civil proceeding. 42 U.S.C. § 1320c-9 (d).

F. Executive Order 13181

While Congress included rules governing the derivative use of medical records against a patient which were disclosed to the Department, in the first instance, in response to an administrative subpoena issued under 18 U.S.C. 3486 to investigate health care fraud offenses, it did not extend this protection to medical records disclosed in response to other compulsory process during a health care fraud investigation, such as a grand jury subpoena or a search warrant. Executive Order 13181, signed on December 20, 2000, filled this gap. 65 Fed. Reg. 81321-3 (12/26/2000).

Because of concern expressed by privacy advocates about potential re-use of data obtained by the Department of Justice in health care fraud investigations against patients, President Clinton issued an Executive Order on December 28, 2000, governing the "re-use" by DOJ of protected health information obtained during the course of an investigation. This Executive Order requires, among other things, that an individual patient's protected health information, discovered during the course of health oversight activities, shall not be used against that individual patient in an unrelated civil, administrative, or criminal investigation of a non-health oversight matter unless the Deputy Attorney General or, insofar as the protected health information involves members of the Armed Forces, the General Counsel of the Department of Defense, has authorized such use.

The Executive Order applies to federal law enforcement agencies that obtain personally identifiable health information disclosed during a health oversight investigation, by means other than a § 3486 administrative subpoena for the investigation of health care offenses. It imposes an administrative approval process on the derivative use of personally identifiable health information, similar to the judicial approval process in § 3486(e). Within the Department, only the Deputy Attorney General can grant approval. The General Counsel of the Department of Defense must approve the derivative use of military medical records involving members of the Armed Forces. However, the Executive Order, does not apply to protected health information initially obtained by a federal law enforcement agency in a non-health oversight investigation.

The Executive Order includes a standard for approving an application, namely, does the balance of relevant factors weigh clearly in favor

of its use? Disclosure for the derivative use shall be permitted "if the public interest and the need for disclosure clearly outweigh the potential for injury" to the patient, which includes injury to the privacy of the patient, to the physician-patient relationship, or to the treatment services. 65 Fed. Reg. 81321-3. Finally, a decision to permit the derivative use must include appropriate safeguards against unauthorized use.

III. Federal case law:

A. General medical records

Despite some variance in the caselaw from circuit to circuit, the federal courts, with the important exception of the Supreme Court decision in *Jaffee v. Redmond*, 518 U.S. 1 (1996), which created a privilege under Fed. R. Evid. 501 for psychotherapy counseling records, including records of counseling sessions with licensed psychiatric social workers, have been reluctant to adopt broad-reaching medical privacy rights. However, when the Medical Privacy Rule becomes enforceable in 2003 and 2004 as described above, it will supercede existing case law to the extent that the case law provided weaker protection to medical records than the new Medical Privacy Rule.

In light of modern medical practice and third party payors, an individual no longer possesses a reasonable expectation that his or her medical history will remain completely confidential. *Whalen v. Roe*, 429 U.S. 589 (1977) (rejecting a challenge by physicians and patients to a New York State statute, which required copies of all prescriptions for controlled substances to be sent to the New York Department of Health to be recorded in a centralized computer file). The Court observed that disclosures to the New York State Department of public health were

> not meaningfully distinguishable from a host of other unpleasant invasions of privacy that are associated with many facets of health care . . . disclosures of private medical information to doctors, to hospital personnel, to insurance companies and to public health agencies are often an essential part of modern medical practice, even when the disclosure may reflect unfavorably on the character of the patient.

Id. at 602.

In the course of investigating health care fraud, the government interest in combating fraud outweighs patient privacy interests. *In re Subpoena Duces Tecum*, 51 F. Supp.2d 726, 738 (W.D. Va. 1999). In fact, by authorizing the use of administrative subpoenas to criminally investigate health care offenses, Congress explicitly evinced its intent to override patient privacy by including a provision which limits the derivative use of records which were disclosed for a health care fraud investigation against the patient. 18 U.S.C. § 3486 (e).

Some courts have held that a search warrant or subpoena seek a qualified privilege for medical records. This protection is not absolute and must be balanced against the legitimate interests of others in obtaining disclosure. *E.g.*, *United States v. Polan*, 970 F.2d 1280, 1285 (3d Cir. 1992). Other courts have adhered to the *Whalen* conclusion, that in light of modern medical practice which requires multiple disclosure to doctors, hospital personnel, public health agencies, and presumably, a host of third-party payors as well, patient charts have a public aspect not protected by a right of privacy. *In re Grand Jury Proceedings*, 867 F.2d 562, 565 (9th Cir. 1989)(*per curiam*).

B. Psychiatric medical records

In *Jaffee v. Redmond*, 518 U.S. 1(1996), the Supreme Court recognized a psychotherapist privilege under Fed. R. Evid. 501 for psychotherapy counseling records, including records of counseling sessions with licensed psychiatric social workers. The Court rejected the lower court's adoption of a case by case balancing test to determine whether psychotherapy notes should be disclosed because " . . . an uncertain privilege, or one which purports to be certain but results in widely varying application by the courts, is little better than no privilege at all." *Id* at 18, *citing*, *Upjohn Co. v. United States*, 449 U.S. 383, 393 (1981). Thus, *Jaffee* prohibited the compelled testimony of the "psychotherapist" through the therapist's case notes of confidential communications against the patient. However, *Jaffee* does not erect an impenetrable barrier to obtaining psychiatric records in civil or criminal health care fraud cases where the patient is not the target. Also, as elsewhere, if the patient consents

to the disclosure of therapeutic counseling records, then the privilege is waived. *Jaffee* also states that, notwithstanding the Court's discussion of the need for a predictable and reliable privilege, ". . . we do not doubt that there are situations in which the privilege must give way. . .," such as a serious threat of harm to the patient or to others which can only be averted by means of disclosure. 116 S. Ct. at 1932, n.19. In addition, a crime-fraud exception to the *Jaffee* privilege has been recognized. *In re Grand Jury Proceedings (Gregory P. Violette)*, 183 F.3d 71 (1st Cir. 1999).

IV. Interaction of federal and state confidentiality protections under the Medical Privacy Rule

Once the Medical Record Privacy Rule becomes enforceable, it will provide that state privacy rules, which are more stringent and more protective of privacy rights, will not be preempted. This should not have a significant impact on the Department's conduct of investigations or litigation, insofar as it will not operate to suspend the Supremacy Clause of the United States Constitution.

State laws do not ordinarily limit or govern the actions of federal agencies. *See Gibbons v. Ogden*, 22 U.S. (9 Wheat.) 1, 210-11 (1824) (stating that the Supremacy Clause invalidates state laws that "interfere with, or are contrary, to the laws of Congress."); *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941); *Jones v. Rath Packing Co.*, 430 U.S. 519, 526, 540-41 (1977) (finding a conflict where state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."); *United States ex rel. Agency for International Development v. First National Bank of Maryland*, 866 F. Supp. 884, 886-87 (D. Md. 1994) (stating that a federal subpoena need not comply with notice requirements in Maryland's Right to Financial Privacy Act); *St. Luke's Regional Medical Center, Inc. v. United States*, 717 F. Supp. 665, 666 (N.D. Iowa 1989) (stating that federal subpoena for medical peer review records need not comply with Iowa state prohibition against peer review records disclosure); *In re Grand Jury Matter*, 762 F. Supp. 333, 334-35 (S.D. Fla. 1991) (finding that a Florida state statute prohibiting state government from disclosing names of physician's patients did not affect a grand jury subpoena); *United States v. Wettstein*, 733 F. Supp. 1212, 1214 (C.D. Ill. 1990) (finding that Illinois state protection for psychologist client lists did not affect a grand jury subpoena); *In the Matter of Grand Jury Proceedings (Krynicki)*, No. 92-2227 1993, WL 318867 (7th Cir. Aug. 20, 1993) (finding meritless a physician's assertion that compliance with a federal grand jury subpoena for medical records would be oppressive because it would force him to violate a state medical record privacy law. The Supremacy Clause of the United States Constitution renders state law without effect in the context of a federal grand jury investigation, *citing, Memorial Hospital for McHenry County v. Shadur*, 664 F.2d 1058, 1063-64 (7th Cir. 1981)).

The new Privacy Rule specifically provides that, if the Secretary of HHS determines that the state laws are necessary to prevent fraud and abuse, ensure appropriate regulation of state health and insurance plans for state reporting on health delivery and "other purposes," then state laws may control. 65 Fed Reg. 82462, 82480. Relevant inquiries will include whether the state laws are more stringent in protecting protected health information, and if the state statute addresses controlled substances. *Id.*

V. DOJ guidelines and guidance on medical record privacy

Beginning in 1996, the Department adopted guidelines and guidance on protecting medical record privacy, which apply to all the investigative and litigating components of the Department. Links to these guidelines can be found in the "Health Care Fraud Policy Manual" (HCF Manual), which can be accessed from a link on the Health Care Fraud page of the USA Book intranet page.

The HIPAA Fraud and Abuse Control Program Guidelines (1/1997) (HIPAA Fraud Guidelines) (HCF Manual, Tab D) jointly adopted by the Attorney General and the Secretary of Health and Human Services, imposed a number of privacy practices on health care fraud investigations. These guidelines may be found in Section VI "Confidentiality Procedures: Provision and Use of Information and Data" of Tab D.

These guidelines provide appropriate confidentiality by maintaining information securely and by limiting access. When disclosing information to an expert, witness, or consultant, redact identifying information when practicable and incorporate the guidelines into contracts concerning medical records.

The HIPAA Fraud Guideline suggests the redaction of personally identifying information in court documents and in trial, when practicable, subject to Court approval, and when appropriate for the purpose of minimizing public dissemination of personal information. When disclosure is required in any judicial, administrative, court, or public proceeding, redact when practicable, seek a court order limiting public disclosure, get patient consent, return or destroy the information when the need for the information ends.

The reach of the HIPAA Fraud Guidelines confidentiality section was extended by the Memorandum of the Deputy Attorney General titled "Protection and Confidentiality of Individually Identifiable Health Information," dated October 15, 1998, beyond protected health information disclosed to the Department and used in health care fraud matters, to all uses and disclosures involving the litigating and investigating components of the Department. HCF Manual, Tab Z-1. This Memorandum directed that the HIPAA confidentiality guidelines apply to all cases, not just our health care fraud cases. The Memorandum explained that the term "individually identifiable health information" was broadly defined beyond traditional concepts, and would include billing records with diagnostic and treatment codes. The Memorandum additionally provided suggestions regarding the minimization of publically-disclosed individually identified health information by redacting medical records attached to motions, filing pleadings with such information under seal, or blind coding patient information entered in evidence, but including a conversion table, in some instances. For example, a conversion table is included when necessary for the jury to compare and contrast pieces of documentary evidence.

Finally, a further Memorandum from the Deputy Attorney General, titled "Suggested Practices for Maintaining the Confidentiality of Medical Records" ("Suggested Practices"), was signed on August 30, 2000 (HCF Manual Tab Z-4). It states: "Taking all practicable steps to protect the confidentiality of individually identifiable pieces of medical information is the responsibility of each and every Department employee." The Suggested Practices include a review of legal requirements concerning medical record confidentiality, which must be followed; a catalogue of concerns with respect to handling, storing, reviewing and using individually identifiable medical records; a discussion of especially sensitive medical information, such as psychiatric records, substance abuse records, and other sensitive medical conditions and treatments; and a discussion of issues related to the Privacy Act of 1974. The Suggested Practices memorandum states that it is not for creating any private rights or defenses, or a right of judicial review.

VI. Conclusion

Special care and planning is required whenever personally identifiable medical information is sought or used by Department attorneys and investigators in any type of investigation or litigative forum. In particular, a review of statutory and regulatory requirements, Department memorandum and guidance, and up-to-date case law regarding individually identifiable health information is required. Also, be prepared to confront and address a new constellation of medical privacy issues after the enforcement date for the Medical Privacy Rule. Specific up-to-date expertise on medical record privacy practice issues is available in the Civil Division by contacting Dan Anderson, Senior Counsel, Commercial Litigation Branch, (202) 616-2451, or the author of this article, Ian C. Smith DeWaal, Senior Counsel, Fraud Section, Criminal Division: (202) 514-0669.❖

ABOUT THE AUTHOR

❑**Ian C. Smith DeWaal** came to the Fraud Section in July, 1990, from the Insurance Division of the Massachusetts' Attorney General Offices which was responsible for enforcing consumer protections against the insurance industry and

representing consumer interests at rate setting hearings. After three years with the Dallas Bank Fraud Task Force, Mr. DeWaal was assigned in 1993 to health care matters including litigation, and legislative and regulatory analysis. Mr. DeWaal developed an expertise in medical record privacy issues and regularly provides advice to the OUSAs and other agencies which obtain and use health records. He represented the Department at several interagency working groups on medical record privacy issues, and testified on law enforcement concerns at a roundtable to the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics. Mr. DeWaal was also a member of the HIPAA Interagency Working Group which has drafted the regulations on the confidentiality of medical Records and participated in the drafting of medical record privacy best practices recommendations for the AGAC Health Care Fraud Subcommittee.✠

Primer for Using Sentencing Guidelines Enhancement for Identity Theft-Related Conduct

Paula J. Desio
Deputy General Counsel
United States Sentencing Commission

Donald A. Purdy, Jr.
Chief Deputy General Counsel
United States Sentencing Commission

In the November 2001 issue of the United States Attorney's Bulletin, identity theft and related offenses were featured in an article that examined this emerging crime problem and the response of the federal law enforcement community. Late last year, the United States Sentencing Commission consolidated the fraud, theft, and property sentencing guidelines. The article below offers a timely and concise overview of relevant sentencing provisions for identity theft-related crimes under the revised guidelines.

I. Historical context

The Identity Theft and Deterrence Act of 1998 (ITDA), Pub. L 105-318(b)(1), Oct. 30, 1998, 112 Stat. 3007, codified at 18 U.S.C. § 1028(a)(7), criminalized the unauthorized use or transfer of a means of identification with the intent to commit or to aid or abet any federal violation or state felony. This new law is extremely broad; it can apply to a wide range of offense conduct, which can also be independently prosecuted under numerous existing statutes (upwards of 180 by an informal count).

Prior to ITDA, only the unauthorized use or transfer of *documents* was illegal under 18 U.S.C. § 1028(a)(1)-(6), while the unauthorized use of credit cards, PINs, ATM codes and other electronic access devices was illegal under 18 U.S.C. § 1029. Under ITDA, *identification means* include *information*, such as social security numbers, dates of birth, as well as electronic access devices and routing codes used in telecommunications and financial sectors. 18 U.S.C. § 1028(d)(4).

The United States Sentencing Commission solicited public comment on whether enhancements relating to identity theft should be confined to the context of the fraud and related economic crime guidelines, or should apply also to conduct such as immigration fraud and firearms violations. No strong support was voiced in favor of the broader approach, and most executive agencies and DOJ supported proposed guideline

language for identity theft within the context of existing economic crime guidelines.

In addition, despite the broad statutory language enacted, the legislative history of the ITDA, and witness testimony before Congress, focused on individuals whose credit history and general reputation had been damaged by unknown and unauthorized use of their identification means. As a result, on May 1, 2000, the Sentencing Commission provided enhanced punishment under the fraud guideline at §2F1.1 for those offenders who obtain identification means in another individual's name or identity, in essence, for those who "breed" identification means, and those who take over another's identity.

The identity theft enhancements under §2F1.1 became effective on November 1, 2000. The Commission's data files for FY 2001, which will be available in mid-2002, will contain information on the use of this guideline by sentencing courts during the first year of its implementation.

II. Current application highlights

On November 1, 2001, three guidelines – Theft (§2B1.1), Property Destruction (§2B1.3) and Fraud (§2F1.1) – were consolidated at §2B1.1 as part of the "Economic Crime Package."

A. Fundamental aspects of §2B1.1 guideline that may apply to identity theft offenses

Some of the key aspects of the consolidated guideline, as it applies to identity theft offenses, are as follows:

The Base Offense Level is set at 6.

The "more-than-minimal planning" enhancement has been deleted.

The alternative prong of "more than minimal planning" for "more than one victim" has been replaced with a specific offense characteristic for offenses that involve large numbers of victims. *See* §2B1.1(b)(2)(A) and (B). Thus, if there are

- 10 to 49 victims or "mass-marketing," a two-level enhancement applies; or
- 50 or more victims, a four-level enhancement applies.

There is a two-level enhancement, or a "floor" (minimum of 12) if any of the following circumstances are present:

- relocation to another jurisdiction to avoid detection;
- a substantial part of the scheme was committed from outside the United States; or
- the offense otherwise involved "sophisticated means."

See §2B1.1(b)(8) and Application Note 6.

In addition to the changes noted above, the loss tables have been revised. The new tables:

- expand previously existing one-level increments to two levels;
- provide substantial increases in penalties for moderate and higher loss amounts (> $70,000);
- apply some smaller increases even when losses are under $40,000 due to the elimination of the more than minimal planning enhancement; and
- reduce levels for some lower loss offenders who previously would have received the two-level enhancement for more than minimal planning.

The definition of "loss" has been revised in a number of significant ways. Under the revised "loss" definition:

- the core rule that loss is *the greater of actual or intended loss* is retained *(see* Application Note 2(A));
- intended loss includes intended pecuniary harms that would have been impossible or unlikely to occur (*see* Application Note 2(A)(ii));
- "actual loss" is defined as "reasonably foreseeable pecuniary harm" that resulted from the offense (*see* Application Note 2(A)(i));
- "reasonably foreseeable pecuniary harm" includes pecuniary harm that the *defendant knew, or under the circumstances, reasonably should have*

known, was a potential result of the offense (*see* Application Note 2(A)(iv));

- "pecuniary harm" excludes emotional distress, harm to reputation, and other non-economic harm *(see* Application Note 2(A)(iii));
- credits against loss include money and property returned and services rendered by the defendant to the victim, before the offense was detected (*see* Application Note 2(E)(i);
- certain credits are not allowed in Ponzi and other investment schemes (*see* Application Note 2(F)(iv); and
- no crediting at all is allowed in schemes in which (i) services were fraudulently rendered to the victim by persons falsely posing as licensed professionals; (ii) goods were falsely represented as approved by a governmental regulatory agency; or (iii) goods for which regulatory approval by a governmental agency was required but not obtained, or was obtained by fraud (*see* Application Note 2(F)(v)).

Finally, loss *excludes* interest, late fees, finance charges, and costs to government of prosecution and aid to victims. *See* Application Note 2(D). A reasonable, not exact, estimate of the loss, remains the standard. *See* Application Note 2(C).

B. Additional §2B1.1 guideline provisions specifically applicable to identity theft offenses

A conviction under 18 U.S.C. § 1028(a)(7) is not necessary to apply the identity theft-related enhancements. Once Appendix A sends a statutory violation to a particular Chapter Two guideline, the sentencing guidelines generally apply on the basis of the offense conduct, rather than the statute of conviction. As long as a conviction is obtained under any of the many federal criminal laws that refer to the fraud and theft guidelines (now consolidated at §2B1.1), the following enhancements and principles will apply. For example, a conviction obtained under the mail fraud statute at 18 U.S.C. § 1341 that involves identity theft offense conduct, as defined in the guidelines, is eligible for the following treatment.

There is an enhancement of two levels OR floor (minimum level) of 12 if:

> the offense involved the unauthorized transfer or use of any means of identification of an actual individual, other than the defendant himself or herself, to produce or obtain any other means of identification. "Means of identification" has the meaning defined in 18 U.S.C. § 1028(d)(4).

There are two prongs to the application of this enhancement for identity theft:

> 1) the defendant must transfer or use the identification means of another person without that person's authority, and
>
> 2) the defendant must use the initial identification means to produce or obtain another different means of identification.

This activity has been described as "breeding" documents. For example, using the defendant's picture and another person's name, address, and date of birth to obtain a state driver's license would qualify for this enhancement, if it occurred in the course of any federal crime that is sentenced under the theft and fraud guideline at §2B1.1. This conduct is distinguished from merely using a stolen credit card and signing the card holder's name in order to purchase goods and services. The latter, while a crime, does not constitute "breeding" documents so as to qualify for the identity theft enhancement. *See* Application Notes 7 (A), (B), and (C).

This two-level enhancement, or floor of 12, also applies if the offense involved the possession or five or more means of identification that were unlawfully produced or obtained by use of another means of identification. For example, a defendant might be arrested before actually using the "bred" documents, but has, in his or her possession, six driver's licenses from six different states that contain the defendant's picture but someone else's name and address.

If the primary purpose of the offense under 18 U.S.C. § 1028 was to violate the law pertaining to naturalization, citizenship, or legal resident status,

apply §2L2.1 rather than the §2B1.1 guideline. *See* Application Note 7(B) to §2B1.1.❖

ABOUT THE AUTHORS

❑**Paula J. Desio** is Deputy General Counsel to the United States Sentencing Commission in Washington D.C., where she is responsible for money laundering, identity theft, and other economic crime issues, as well as organizational sentencing and compliance issues under the federal Sentencing Guidelines. She is a frequent speaker and author on matters relating to business and organizational ethics.

Prior to joining the Sentencing Commission in January 1997, Ms. Desio was Of Counsel to the Washington, D.C. law firm of Crowell & Moring, where for ten years she specialized in internal investigations and the defense of businesses involved in federal criminal and agency enforcement proceedings and congressional hearings.

❑**Donald A. (Andy) Purdy, Jr.** is the Chief Deputy General Counsel to the United States Sentencing Commission, where he has worked since 1987. He served as Acting General Counsel from November 1999 to January 2001. He served as Chair of the Commission's Economic Policy Team that formulated the Economic Crime package of amendments that went into effect November 1, 2001.

Mr. Purdy served as an Assistant United States Attorney in Philadelphia, Special Counsel to the House Ethics Committee, Counsel to the Senate Impeachment Trial Committee, and Assistant Attorney General in Missouri. He also worked as Senior Staff Counsel to the House Select Committee on Assassinations' investigation of the assassination of President Kennedy.✠

Notes

UPCOMING PUBLICATIONS

May, 2002 - Terrorism

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.