Trends in Federal White Collar Prosecutions

CAROL A. POINDEXTER, NORTON ROSE FULBRIGHT AND TIMOTHY M. MOORE, SHOOK, HARDY & BACON LLP, WITH PRACTICAL LAW LITIGATION

A Practice Note covering trends and developments in the federal government's prosecution of white collar crime. Specifically, this Note examines the government's tactics and strategies in enforcing federal criminal laws, the elements of several criminal statutes frequently used by the government to prosecute corporate crime, what constitutes criminal intent in white collar cases, company and managerial liability and compliance programs designed to mitigate corporate liability.

Through increased white collar enforcement, the government has achieved broad internal reform within targeted companies and industries. At the vanguard of this corporate scrutiny is the Department of Justice, which is now the preeminent federal overseer of corporate culture. Indeed, the DOJ continues to maximize its leverage over companies and individuals by invoking broad interpretations of criminal statutes and expanding enforcement, all towards the end of encouraging ethical corporate culture. As a result, corporations and their officers, directors and management face enormous risks. Among the risks for companies are:

- Indictment.
- Monumental fines.
- Court-appointed monitors.
- Reputational damage.
- Investigation by regulators, such as the SEC or FINRA.
- Follow-on civil litigation.

For officers, directors and management, the risks similarly include steep fines, debarment, probation, or even incarceration. Those penalties, and the rise in enforcement against both companies and senior corporate executives, make even more important an executive's and a company's assessment of risks related to their business operations. To facilitate the first step towards that end, this Note discusses trends in the federal government's enhanced efforts to prosecute white collar crime.

THE GOVERNMENT'S ENHANCED EFFORTS TO COMBAT WHITE COLLAR CRIME

Over the last decade, companies have witnessed an unprecedented effort by the federal government to identify and prosecute white collar criminal violations. Two of the government's most noticeable tools are:

- Pooling resources through creation of task forces.
- Maximizing opportunities for corporate self-disclosure.

CONSOLIDATION OF ENFORCEMENT POWER TO POLICE CORPORATE FRAUD

In 2002, in response to the WorldCom and Enron scandals, President G.W. Bush created a Corporate Fraud Task Force (CFTF) to enhance the DOJ's prosecution of corporate entities. Taking its cue, the government began a more aggressive enforcement response to corporate fraud. The goals were to improve coordination among federal officials, accelerate investigations and prosecutions, motivate local US Attorneys to bring complex fraud cases and convince corporations to cooperate.

The CFTF's emphasis on "real-time enforcement" netted hundreds of corporate fraud guilty pleas or trial convictions in the years following its creation. For example, months after allegations of accounting fraud at Adelphia Communications Corporation (Adelphia) initially surfaced, and only two weeks after the CFTF's creation, John Rigas, then Adelphia's CEO, was arrested and publically handcuffed before the media. He was later sentenced to 15 years in prison. Moreover, white collar prosecutions, which had traditionally been the province of the Southern District of New York, became a national phenomenon as the CFTF encouraged greater coordination between the Securities and Exchange Commission (SEC) and local US Attorneys across the country. Eventually, in 2009, the Financial Fraud Enforcement Task Force (FFETF) replaced the CFTF. Unlike the CFTF, which relied primarily on the DOJ and the FBI, the FFETF includes representatives from over 20 federal agencies, 94 US Attorney's Offices and state and local agencies. Unsurprisingly, the FFETF's broader reach has enabled it to expand the success of CFTF.

2009 also saw the creation of another task force, but much narrower in scope: the Health Care Fraud Prevention and Enforcement and Action Team, commonly known as HEAT. As the name suggests, HEAT concentrates on health care fraud involving public money. Like CFTF and FFETF, HEAT has achieved great success. Since 2007, investigations in Medicare fraud have led to over 1,400 prosecutions and contributed to the government recovering billions of dollars.

More recently, and in response to increased financial crime in the late 2000s, Congress created the Consumer Financial Protection Bureau (CFPB). The CFPB focuses on enforcement of federal laws impacting consumer lending and finance. Already, the CFPB is augmenting the government's enforcement success. For example, in April 2013, the CFPB filed an enforcement action against four mortgage insurers who allegedly illegally gave kickbacks to lenders. As part of settling that action, the mortgage insurers have agreed to pay $15 million in penalties and to be subject to continuing monitoring by the CFPB.

FORCING CORPORATE SELF-DISCLOSURE

Another enduring legacy of the corporate fraud scandals of the early 2000s is an increasing emphasis on corporate self-disclosure. Indeed, corporate self-disclosure requirements have been codified in several statutes and made a part of certain regulations. For example, the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley) imposed a complex web of certification and self-disclosure requirements on corporate officers, directors and counsel, including the so-called "reporting up" rules that force counsel to report to superiors evidence of financial or fiduciary breaches discovered by counsel, and to report this information to the SEC if the corporate response was unsatisfactory.

Moreover, the DOJ's Principles of Federal Prosecution of Business Organizations (Principles) condition receipt of cooperation credit on self-disclosure of relevant facts. As a result, the Principles spawned a "culture of waiver" as companies used self-disclosure (often by turning over privileged documents) to avoid or mitigate the risks of an enforcement action. In fact, the perceived pressure to provide privileged information became so great that the DOJ revised its guidelines to clarify that receipt of cooperation credit would not be conditioned upon disclosure of privileged information. However, because the DOJ retained its requirement that companies disclose relevant facts, companies still must weigh the hope of receiving cooperation credit against the consequences of providing privileged information. Due to receiving privileged corporate information once deemed off-limits to federal prosecutors, the government has successfully prosecuted those specific individuals whom it deemed responsible for corporate wrongdoing.

In January 2010, the SEC announced that it was implementing a series of measures to further strengthen its enforcement program by encouraging greater cooperation from individuals and companies in the agency's investigations and enforcement actions (see Press Release, SEC Announces Initiative to Encourage Individuals and Companies to Cooperate and Assist in Investigations (Jan. 13, 2010)). As a result of this initiative, in December 2010, the SEC announced that it had entered into a non-prosecution agreement with the children's clothing marketer Carter's, Inc. for providing information to the SEC regarding insider trading and financial fraud committed by its Executive Vice President (see *Press Release, SEC Charges Former Carter's Executive With Fraud and Insider Trading (Dec. 20, 2010)*). Similarly, in 2013, the SEC entered into the first non-prosecution agreement involving a violation of the Foreign Corrupt Practices Act, highlighting "the company's prompt reporting of the violations on its own initiative, the completeness of the information it provided, and its extensive, thorough, and real-time cooperation with the SEC's investigation" (see *Press Release, SEC Announces Non-Prosecution Agreement With Ralph Lauren Corporation Involving FCPA Misconduct (Apr. 22, 2013)*).

FOCUS ON INDIVIDUALS

On September 9, 2015, Deputy Attorney General Sally Yates issued a memorandum on Individual Accountability for Corporate Wrongdoing (Yates Memorandum). The Yates Memorandum lays out measures that the DOJ will take in any investigation of corporate misconduct, civil or criminal, to identify and prosecute the individuals responsible for the illegal corporate conduct.

The Yates Memorandum specifically ties any eligibility for corporate cooperation credit to the corporation providing the DOJ with all relevant facts about the individuals responsible for the misconduct. It requires that federal prosecutors focus on the individuals responsible for the misconduct from the beginning of the investigation and precludes them from releasing responsible individuals from civil or criminal liability when settling the matter with the organization absent special circumstances and approval by DOJ senior officials. The Yates Memorandum also requires prosecutors to have a clear plan for resolving cases with individuals before it resolves the case with the corporation. The memorandum directs the revision of the Principles of Federal Prosecution of Business organizations (the current version of which is the Filip Memorandum) and the commercial litigation provisions in Title 4 of the U.S. Attorney's Manual to reflect these new policies.

The Yates Memorandum officially memorializes an emphasis on individual liability for corporate misconduct which has been increasingly discussed in public statements by DOJ officials. For example, in June 2015, the Medicare Fraud Strike Force announced criminal enforcement actions against 243 individuals across the country alleging $712 million in fraudulent billings, making it the largest criminal healthcare fraud matter in history (see *Department of Justice, National Medicare Fraud Takedown Results in Charges Against 243 Individuals for Approximately $712 Million in False Billing: Most Defendants Charged and Largest Alleged Loss Amount in Strike Force History (June 18, 2015)*).

For more information related to the Yates Memorandum, see *Legal Update, I Want You! DOJ Instructs Prosecutors to Focus on Individuals in Corporate Investigations (http://us.practicallaw.com/w-000-6027).*

SUBSTANTIVE CRIMES

Federal corporate criminal investigations often focus on fraud. These investigations typically involve allegations that an individual or a corporation defrauded shareholders, investors, the government or the public. This section of the Practice Note provides an overview of the various statutes the government uses to combat corporate crime, and how the government has used these statutes against corporations in recent years.

MAIL AND WIRE FRAUD

Allegations of violations of the federal mail and wire fraud statutes are a staple of federal prosecutors. No longer the sole province of the US Postal Service, the FBI now often investigates allegations of mail fraud and its wire fraud analogue.

To convict an individual or a corporation of a mail or wire fraud offense, the government must show beyond a reasonable doubt that the defendant:

- Devised or participated in a scheme or artifice to defraud.
- Acted with the intent to defraud.
- Used (or caused to be used) mail, wire, radio or television communication in furtherance of the scheme or artifice to defraud.

(*18 U.S.C. §§ 1341 & 1343.*)

Each use of the mails or wires is a separate offense and can therefore be a separate count in an indictment. The maximum punishment for each mail and wire fraud conviction is 20 years' imprisonment and the fine prescribed in *18 U.S.C. § 3571* (*18 U.S.C. §§ 1341 & 1343*).

The "In Furtherance" Requirement

The "in furtherance" requirement underscores the breadth of the mail and wire fraud statutes. Generally, this requirement is easily satisfied because the mailing or wire need only be incidental to an essential part of the scheme (see *Schmuck v. United States, 489 U.S. 705, 710-15 (1989)*). A mailing or e-mail designed to conceal the crime, postpone the investigation or deceive the victims into a false sense of security satisfies this standard (see *United States v. Hilton, 701 F.3d 959, 973 (4th Cir. 2012)*; *United States v. Masten, 170 F.3d 790, 796 (7th Cir. 1999)*). Conversely, a mail or wire communication after the scheme is complete will not satisfy the "in furtherance" requirement (see *United States v. Strong, 371 F.3d 225, 229-233 (5th Cir. 2004)*).

Honest Services Fraud

A major component of the government's effort to combat corporate fraud involves the application of the mail and wire fraud statutes to breaches of fiduciary duties in the private sector. In 1988, Congress broadened the definition of a "scheme or artifice to defraud" to include a scheme to "deprive another of the intangible right to honest services" (*18 U.S.C. § 1346*). Federal prosecutors have aggressively used the flexibility inherent in this language to charge corporate executives even where the defendant did not take any money or property from the victim. In one high-profile case, Enron CEO Jeffrey Skilling was convicted for (among other things) honest services fraud because he breached a fiduciary duty owed to Enron by not disclosing to the board of directors material information about how he was using company assets among various corporate entities, and because he and other Enron executives deceived investors about the company's declining financial condition.

In June 2010, however, the Supreme Court dealt a serious blow to the government's ability to prosecute honest services fraud. According to the Supreme Court's ruling in *Skilling v. United States, 561 U.S. 358, 409 (2010)*, the honest services statute criminalizes only schemes to defraud that involve bribes or kickbacks. In other words, mere self-dealing resulting in material omissions or misrepresentations, without more, is insufficient to support a conviction for honest services fraud.

SECURITIES FRAUD

The DOJ and the SEC are the government agencies involved in enforcing the securities statutes. The most commonly prosecuted types of securities fraud involve:

- Material misrepresentations or omissions in connection with the purchase or sale of securities.
- Insider trading.
- Accounting fraud.

Material Misrepresentations or Omissions

Under SEC Rule 10b-5 (*17 C.F.R. § 240.10b-5*), any person who, with fraudulent intent, employs a deceptive device or makes a false statement or omission of material fact in connection with the purchase or sale of a security may be criminally and civilly liable (see *Practice Note, Securities Litigation: Defending a Private Securities Fraud Lawsuit: A Material Misrepresentation or Omission (http://us.practicallaw.com/w-000-3629)*). The government uses Rule 10b-5 to pursue a wide range of fraudulent activities in the financial industry. For example, the SEC recently brought a mortgage fraud case against Countrywide executives for deliberately misleading investors about the credit risks taken by Countrywide to build its market share (see SEC Press Release, SEC Charges Former Countrywide Executives With Fraud (June 4, 2009)).

Insider Trading

Rule 10b-5 also prohibits using material, non-public information obtained in breach of a fiduciary duty to purchase or sell any security.

For example, in 2009 the US Attorney for the Southern District of New York charged Raj Rajaratnam, the founder of the Galleon Group of hedge funds, and others with repeatedly trading on material, nonpublic information pertaining to upcoming earnings forecasts, mergers, acquisitions or other business combinations in what has been called the largest hedge fund insider trading case in history (see *SEC Press Release, SEC Charges Billionaire Hedge Fund Manager Raj Rajaratnam with Insider Trading (Oct. 16, 2009)*). Following a two-month trial in 2011, a jury found Mr. Rajaratnam guilty of all 14 counts of insider trading. He was sentenced to 11 years in prison. Rajat Gupta, former global head of McKinsey &Co. and Goldman Sachs's board member was also convicted of insider trading for passing confidential non-public information heard at Goldman Sachs's board meeting to Mr. Rajaratnam. Mr. Gupta was sentenced to 2 years in prison.

Penalties for Violating Rule 10b-5

Section 32(a) of the Securities Exchange Act of 1934 (Exchange Act) (*15 U.S.C. § 78a -78pp*) imposes stiff penalties on those who "willfully" commit fraud in connection with the purchase or sale of securities or engage in insider trading. Under Section 32(a), an individual found guilty of violating Rule 10b-5 may be imprisoned for up to 20 years and fined up to $5 million. Corporations found guilty of violating Rule 10b-5 may be fined up to $25 million. (*15 U.S.C. § 78ff(a)*.)

Enhanced Liability and Punishment under Sarbanes-Oxley

Sarbanes-Oxley goes further than Rule 10b-5 in policing securities fraud. Rule 10b-5, on its face, only prohibits frauds committed "in connection with the purchase or sale of any security." Section 807 of Sarbanes-Oxley (*18 U.S.C. § 1348*), however, takes this a step further and criminalizes frauds "in connection with any [] security." This provision expands liability because it does not require that the fraud be connected with the "purchase or sale" of a security.

Moreover, unlike Section 32(a) of the Exchange Act, the criminal penalties for violating Sarbanes-Oxley § 807 (which include up to 25 years imprisonment) may be triggered without a showing that the defendant acted "willfully" (*18 U.S.C. § 1348*).

Accounting Fraud and Obstruction of Justice

Accounting fraud, euphemistically referred to as "creative accounting," involves the deliberate manipulation and falsification of financial information to achieve an operating profit so the company appears more profitable than it actually is. Accounting fraud takes many forms, including:

- Overstating the company's income revenue, assets or both.
- Concealing assets to avoid paying taxes.

- Understating expenses, losses or liabilities.
- Executing false trades designed to inflate profits or hide losses.
- Making false transactions designed to evade regulatory oversight.

For example, in 2002, the SEC alleged that the cable television company Adelphia Communications committed accounting fraud by excluding certain bank debt from its financial statements (see *SEC Press Release, Litigation Release No. 17627, Accounting and Auditing Enforcement Release No. 1599 (July 24, 2002)*).

More recently, the SEC continued to aggressively prosecute accounting fraud, charging executives at TheStreet Inc. in 2012 with accounting fraud for artificially inflating company revenues and misstating operating income to investors (see *SEC Press Release, SEC Charges Financial Media Company and Executives Involved in Accounting Fraud (Dec. 18, 2012)*).

Additionally, as in the Enron and WorldCom debacles, a company, its accountants, or both, may engage in conduct designed to conceal accounting fraud, hoping to impede regulatory inquiries by the SEC or other agencies. In the wake of the Enron scandal, the accounting firm Arthur Andersen was convicted in 2002 of obstructing justice by destroying documents related to its audit of Enron. Even though the Supreme Court later reversed the conviction due to flaws in jury instructions, the Congress saw it fit to address this conduct by creating a new criminal law, the Sarbanes-Oxley act of 2002. Sarbanes-Oxley requires any accountant who conducts an audit of a public company to maintain all audit workpapers for a period of five years from the end of the fiscal period in which the audit or review was concluded (*18 U.S.C. § 1520(a)(1)*). A willful violation of this provision can result in a fine, imprisonment for not more than ten years or both.

Aggressive Investigation Techniques Used to Combat Securities Fraud

The government's prosecution of securities fraud underscores a major trend in its war on corporate crime. In the *Galleon* case, for example, the government obtained part of its evidence through the use of wiretaps, an enforcement tool historically limited to organized crime and narcotics-related investigations. After announcing the *Galleon* charges, then SEC Enforcement Director Robert Khuzami (also a former federal prosecutor) warned that the agency would employ wiretap evidence more widely in its enforcement of security fraud statutes. In 2009, Khuzami said that individuals involved in securities fraud "now must rightly consider whether their conversations are under surveillance" (*Speech, Remarks by Robert Khuzami at AICPA National Conference on Current SEC and PCAOB Developments (Dec. 8, 2009)*).

In addition to wiretapping, the government has recently increased its use of technology to identify potentially fraudulent conduct. The DOJ, SEC and others, now leverage powerful databases and data analytics tools to expose fraudulent schemes and use the information to present a clear money trail to juries.

Increased Use of Corporate Whistleblowers

Under the Dodd-Frank Act, the SEC will pay individuals who provide the SEC with information about securities law violations (whistleblowers) cash rewards of between 10% and 30% of any monetary sanctions in excess of $1 million that the government, because of whistleblowers' assistance, recovers through either civil or criminal proceedings (see *Practice Note, Whistleblower Protections under Sarbanes-Oxley and the Dodd-Frank Act (http://us.practicallaw.com/7-501-7799)*). In the fiscal year 2014, the SEC received 3,620 tips, complaints and referrals. In Fiscal year 2015, the SEC received 3,923 tips, complaints, and referrals and made over $37 million in award payments to whistleblowers. (*SEC Annual Report on the Dodd-Frank Whistleblower Program (2015)*).

FRAUD AGAINST THE GOVERNMENT

The FBI is the federal agency normally assigned to investigate fraud against the government, although it often partners with the Inspector General of the allegedly defrauded agency. The FFETF, by merging with the former National Procurement Fraud Task Force, obtained an experienced cadre of inspectors general who possess the institutional knowledge of how to prevent and investigate procurement and grant fraud. Procurement fraud may include mischarging the government for cost and labor or failing to disclose to the government cost or pricing data that is accurate, complete and current prior to reaching a price agreement.

False Claims Act

The False Claims Act (FCA) (*31 U.S.C. §§ 3729-3733*) is the principal tool used by the government to combat fraud against the United States, although the government also prosecutes procurement fraud under various other statutes, including the mail and wire fraud statutes, the Racketeer Influenced and Corrupt Organizations Act and, within the health care context, the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The FCA generally requires the government to prove that:

- The defendant presented, or caused to be presented, a claim to the government seeking payment for services or goods.
- The claim was false, fictitious or fraudulent.
- The defendant knew the claim was false.

(*31 U.S.C. § 3729(a)-(b)*.)

Each false claim can qualify as a separate offense, which carries a penalty of up to $11,000 (as adjusted from time to time) per claim, plus treble damages (*31 U.S.C. § 3729(a)*). For more information on the FCA, see *Practice Note, Understanding the False Claims Act (http://us.practicallaw.com/7-561-1346).*

Fraud Enforcement and Recovery Act of 2009

Congress passed the Fraud Enforcement and Recovery Act of 2009 (FERA) in response to the subprime mortgage and credit market crisis. FERA substantially broadened the FCA by:

- Including within the FCA's reach false claims submitted by subcontractors to contractors for work done on federal projects where the false statement is "material" to the government's decision to pay a false claim, even though the subcontractor did not make the false claim directly to the government.
- Creating liability for concealing a government overpayment.
- Expanding the number of whistleblowers who may be able to file suit on behalf of the government.

(*FERA, S. 386 § 4.*)

Federal Acquisition Regulations

In addition to the FCA and various other anti-fraud statutes, the government also uses the Federal Acquisition Regulations (FAR) to identify and punish procurement fraud. Under the FAR, contractors face debarment if they do not timely disclose to the government that a principal of the contractor has credible evidence of a:

- Violation of the FCA (or certain federal criminal laws) in connection with a federal contract or subcontract.
- "Significant overpayment" for all current or previous contracts for which the contractor has received final payment within the last three years.

(*48 C.F.R. § 9.406-2(b)(1)(vi)*.)

Moreover, many government contractors with contracts above a $5 million/120 day threshold will see contract and subcontract clauses requiring "internal control" systems with minimum features.

Determining whether a criminal violation or a violation of the FCA has occurred frequently turns on the knowledge and intent of third parties. These issues are inherently difficult to assess. As a result, there is a risk that a contractor may not deem evidence of possible FCA or criminal violations to be credible, only to have that determination later called into question by a prosecutor or *qui tam* relator (that is, a whistleblower who sues on the government's behalf). To protect itself from liability for not reporting possible violations of the law, a contractor should contemporaneously document the steps taken to investigate these matter, and any resulting credible evidence determinations. This documentation may be useful in demonstrating the adequacy and reasonableness of the contractor's process and decision-making in the glow of hindsight.

OBSTRUCTION

Federal obstruction of justice statutes have traditionally criminalized misleading statements made with a corrupt intent to impede the administration of justice (*18 U.S.C. § 1503* (obstructing grand jury); *18 U.S.C. § 1505* (obstructing pending federal investigations); *18 U.S.C. § 1512(c)* (obstructing official proceedings)). In addition, a mainstay of many federal criminal investigations is *18 U.S.C. § 1001*, which criminalizes the making of a false, material statement to the government. Moreover, prosecutors have new tools to enhance corporate accountability for obstruction. For example:

- Sarbanes-Oxley created new obstruction charges that eliminate some of the technical requirements of the traditional obstruction of justice statutes (see *Obstruction under Section 802(a) of Sarbanes-Oxley*).
- The government has increasingly used false statements made to corporate counsel (which, in turn, are relayed to the government) to expand the reach of traditional obstruction of justice statutes (see *Misleading Statements to Corporate Counsel Communicating with the Government*).
- The government has applied heightened scrutiny to the handling of internal corporate investigations, raising the potential for charges against in-house counsel and other employees who were involved in investigating alleged corporate wrongdoing (see *Close Scrutiny of Internal Investigations*).

Obstruction under Section 802(a) of Sarbanes-Oxley

Section 802(a) of Sarbanes-Oxley punishes a person who knowingly alters, destroys or falsifies documents or other tangible things with the intent to obstruct an investigation or "proper administration" of any matter "within the jurisdiction of any department or agency of the United States" or "in relation to or contemplation of any such matter" (codified at *18 U.S.C. § 1519*).

Known as the "anticipatory obstruction" statute, Section 802(a) has been interpreted by courts not to include the technical nexus requirements of the more traditional obstruction of justice statutes, like a pending or imminent proceeding or matter, or some linkage between the defendant's knowledge and the nature of the government's jurisdiction. Because of its broad wording and scope of application, Section 802(a) may even be used to prosecute individuals for obstruction of justice in the course of a company's own internal investigation.

Misleading Statements to Corporate Counsel Communicating with the Government

In connection with a government investigation into corporate fraud, FBI agents and other federal law enforcement officers sometimes conduct surprise interviews of the investigation's target, hoping the startled target will make a false statement that the government can later use as leverage. The government has been using corporate counsel to the same effect. In 2004, for example, the government indicted and eventually convicted employees of Computer Associates for obstruction based on misleading statements made by a corporate executive to company counsel during an internal investigation, where company counsel later shared the defendant's statements with the government (see *DOJ Press Release, Former Computer Associates Executives Indicted on Securities Fraud, Obstruction Charges (Sept. 22, 2004)*).

Close Scrutiny of Internal Investigations

The government's increased focus on obstruction also presents significant risks to today's company counsel charged with managing internal investigations. Regulators closely scrutinize in-house counsel's management of an internal investigation. Therefore, mishandling an internal investigation can ultimately implicate corporate counsel as a target in any corporate criminal probe. For example, in 2010, the DOJ indicted an associate counsel at GlaxoSmithKline for allegedly obstructing justice and making false statements during an investigation (see *DOJ Press Release, Pharmaceutical Company Lawyer Charged with Obstruction and Making False Statements (Nov. 9, 2010)*). Although that case was dismissed, the government's close scrutiny of in-house counsel continues.

FINANCIAL INSTITUTION FRAUD

Several agencies enforce the various statutes that govern offenses by or against financial institutions. These agencies include the Treasury Department, the Office of the Comptroller of the Currency (OCC), the Federal Reserve and the Federal Deposit Insurance Corporation (FDIC). The FBI is frequently the lead investigative agency for criminal banking violations. Moreover, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) maintains a database for, and analyzes information received from, financial institutions.

The two main statutes used to combat financial institution fraud are the Bank Fraud Statute and the Bank Secrecy Act (BSA).

Bank Fraud Statute

The Bank Fraud Statute, which is analogous to the wire and mail fraud statutes, prohibits the use of a scheme or artifice to defraud a financial institution. Penalties for violating the bank fraud statute include fines of up to $1 million and 30 years imprisonment (*18 U.S.C. § 1344*).

Bank Secrecy Act

The BSA uses strict record keeping requirements to guard against the use of financial institutions to launder unreported income or to structure transactions to avoid detection by law enforcement. Specifically, the BSA requires US financial institutions to:

- Keep records of cash purchases of negotiable instruments.
- File reports of cash transactions exceeding a daily aggregate amount of $10,000.
- Report suspicious activity that might signify money laundering (that is, using a financial transaction to make illegal income appear legitimate), tax evasion or other criminal activities.

The provisions of the BSA are scattered among various sections of the US Code and agency regulations promulgated thereunder (see FinCEN website). Shortly after 9/11, in an attempt to combat terrorist financing and other illegal activity, Congress amended the BSA through the USA Patriot Act to require financial institutions to implement programs to detect and deter instances of money laundering (*Pub. Law 107-56 (Oct. 26, 2001)*).

Government Prosecution of Financial Institutions

Historically, most financial fraud investigations occurred where the financial institution was the victim. However, several high-profile cases have focused on the financial institution as a target. Two significant cases involving deferred prosecutions and heavy fines for American Express Bank International and Union Bank of California reflect the government's aggressive prosecution of financial institutions that fail to maintain an effective anti-money laundering program (see *FinCEN Press Release, FinCEN and OCC Assess Civil Money Penalties Against Union Bank of California (Sept. 17, 2007)*; *DEA Press Release, American Express Bank International Enters Into Deferred Prosecution Agreement And Forfeits $55 Million To Resolve Bank Secrecy Act Violations (Aug. 6, 2007)*). A third, more recent case, involves HSBC. In late 2012, it agreed to forfeit $1.256 billion in a deferred prosecution agreement with the DOJ because HSBC failed to maintain an effective anti-money laundering program (see *DOJ, Press Release, HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement (Dec. 11, 2012)*).

Another example where a financial institution was targeted by the government involves the income tax evasion case against the Swiss bank, UBS AG. In February 2009, UBS AG agreed to pay $780 million to settle a claim that it conspired to defraud the US by impeding IRS investigations (see *DOJ Press Release, UBS Enters Into Deferred Prosecution Agreement (Feb. 18, 2009)*). The government alleged that UBS's employees and managers helped US taxpayers open new UBS accounts in the names of nominees or sham entities to avoid reporting requirements, thereby concealing their assets from the IRS. The UBS case also resulted in multiple convictions against individual tax evaders for financial fraud and tax evasion.

FOREIGN CORRUPT PRACTICES ACT

The Foreign Corrupt Practices Act (FCPA) contains two separate provisions. It:

- Criminalizes the bribery of a foreign official to secure or maintain business (*15 U.S.C. §§ 78dd-1 to 78dd-3*).
- Requires companies to maintain accurate books and records and internal controls (*15 U.S.C. § 78m(b)*). This provision is designed to ensure that shareholders receive an accurate assessment of the company's expenditures by preventing accounting fraud associated with improper payments.

In the past several years, there has been an explosion of FCPA enforcement actions brought by the DOJ and the SEC. This trend continues unabated as aggressive US enforcement is coupled with enhanced international cooperation arising from heightened international anti-bribery standards and active parallel investigations in foreign jurisdictions. As a result, US companies doing business abroad now face the greatest level of government resources to combat bribery since the passage of the FCPA more than 30 years ago. Indeed, as detailed below, FCPA enforcement is a prime example of the government's increased efforts to combat corporate crime generally.

The DOJ has historically expected that companies wishing to receive full cooperation credit in FCPA matters would engage in widespread cross-border investigations of the misconduct, often resulting in staggering legal and consultancy fees. However, the DOJ appears to have shifted its position recently and announced that to receive full cooperation credit, companies need only conduct a focused investigation in countries where an actual FCPA issue has been identified or is likely to have occurred, rather than investigate additional jurisdictions based on mere speculation (see *Leslie R. Caldwell, Assistant Attorney General, Criminal Division, Remarks at the N.Y. City Bar Ass'n Fourth Annual White Collar Crime Institute (May 12, 2015)*).

In addition, in November 2015, the SEC announced that companies subject to FCPA enforcement actions would need to self-report their potential misconduct in order to be eligible for deferred prosecution agreements (DPAs) and non-prosecution agreements (NPAs) (see *Andrew Ceresney, Director, SEC Division of Enforcement, Remarks at the American Conf. Institute's 32nd Annual FCPA Conf. (Nov. 17, 2015)*).

Additional Resources Devoted to FCPA Enforcement

The federal government has devoted additional resources to fight foreign bribery. For example, the SEC created a specialized unit that focuses specifically on new and proactive approaches to identify FCPA violations (see *SEC Press Release, SEC Names New Specialized Unit Chiefs and Head of Office of Market Intelligence (Jan. 13, 2010)*).

Strict Liability under the FCPA

Enforcement of the FCPA's accounting provisions broadly relies on strict liability. A US parent may therefore be liable for the accounting fraud of its foreign subsidiary whether or not the parent has knowledge of the accounting fraud (see *SEC Press Release, SEC Charges Nature's Sunshine Products, Inc. with Making Illegal Foreign Payments (July 31, 2009)*).

Industry-wide FCPA Enforcement

The government is using an industry-based approach to target all similarly-situated corporate players. In the energy sector, for example, illegal kickbacks to the Iraqi government in exchange for contracts under the UN's Oil for Food Program netted numerous convictions or settlements against several energy-related companies for essentially the same conduct (see, for example, *DOJ Press Release, Flowserve Corporation to Pay $4 Million Penalty for Kickback Payments to the Iraqi Government under the U.N. Oil for Food Program (Feb. 21, 2008)*; *SEC Press Release, Chevron to Pay $30 Million to Settle Charges For Improper Payments to Iraq Under U.N. Oil For Food Program (Nov. 14, 2007)*; *SEC Press Release, SEC Files Settled Books and Records and Internal Controls Charges Against Ingersoll-Rand Company Ltd. For Improper Payments to Iraq Under the U.N. Oil for Food Program—Company Agrees to Pay Over $4.2 Million and to Make Certain Undertakings Regarding its Foreign Corrupt Practices Act Compliance Program (Oct. 31, 2007)*).

Increased Self-reporting

There is an increase in FCPA self-reporting by corporations, mainly due to the voluntary disclosures mandated by Sarbanes-Oxley's internal control requirements. Self-reporting has enabled companies to avoid charges and pay reduced fines (see *SEC Press Release, SEC Announces Non-Prosecution Agreement With Ralph Lauren Corporation Involving FCPA Misconduct (Apr. 22, 2013)*).

More Severe Penalties

There also has been a sharp increase in the penalties imposed for FCPA violations. For example, in 2008, Europe's largest engineering company, Siemens AG, was ordered to pay a $1.6 billion penalty arising from an FCPA settlement (see *SEC Press Release, SEC Files Settled Foreign Corrupt Practices Act Charges Against Siemens AG for Engaging in Worldwide Bribery With Total Disgorgement and Criminal Fines of Over $1.6 Billion (Dec. 15, 2008)*).

Prosecution of Corporate Executives

Federal prosecutors have aggressively targeted senior corporate executives for FCPA violations. The number of individuals prosecuted continues to outpace the number of corporate entities. Since 2008, the DOJ has charged 99 individuals and 67 corporate entities with FCPA violations. The DOJ has also recently issued a new prosecutorial guidance, instructing its prosecutors to focus on individuals when investigating corporate misconduct (see *Focus on Individuals*), indicating that the trend of increased individual prosecutions is likely to continue.

Clandestine Investigative Techniques

The government is using clandestine investigative techniques in FCPA cases. For example, it used a sting operation involving an informant to indict 22 corporate executives in a foreign bribery case (see *DOJ Press Release, Twenty-Two Executives and Employees of Military and Law Enforcement Products Companies Charged in Foreign Bribery Scheme (Jan. 19, 2010)*).

New DOJ & SEC FCPA Guide

On November 14, 2012, the DOJ and the SEC published their first FCPA guidance document: A Resource Guide to the U.S. Foreign Corrupt Practices Act (FCPA Guide) and revised it in June 2015. The FCPA Guide outlines and reaffirms the government's enforcement policies and interpretations of key elements of the FCPA including, among other things, principles governing:

- The application and interpretation of key FCPA terms, including:
  - the business purpose test;
  - instrumentalities of a foreign government;
  - facilitating payments;
  - foreign officials; and
  - the "anything of value" provision.
- Parent and successor liability.
- The settlement and penalty phases of FCPA prosecutions.
- The elements necessary to demonstrate an effective anti-corruption compliance program.

While the FCPA Guide states that it is "non-binding, informal, and summary in nature, and the information contained herein does not constitute rules or regulations," it does provide valuable insights into how the government approaches enforcement decisions, evaluates a corporation's conduct and assesses the effectiveness of a corporation's compliance program.

For example, the FCPA Guide dedicates an entire chapter on the government's enforcement and settlement policies. The FCPA Guide emphasizes that the DOJ and SEC consider a broad range of potential resolutions of FCPA enforcement actions, including:

- Plea agreements.
- Deferred prosecution agreements.
- Non-prosecution agreements.
- Injunctive relief.
- Administrative remedies.
- Declinations (declining to bring an enforcement action).

The FCPA Guide also affirms that a decision to bring or decline an enforcement action continues to be a matter of prosecutorial discretion, guided by the DOJ's Principles of Federal Prosecution and the Principles of Federal Prosecution of Business Organizations, and the SEC's Enforcement Manual. Although the FCPA Guide provides very little additional detail on the factors the agencies consider in making a declination decision, it does provide six anonymous examples where the DOJ and the SEC declined to bring charges against a company. The companies' actions in the illustrative cases share several characteristics. Each company:

- Initiated an internal investigation and voluntarily disclosed the potential misconduct.
- Terminated the employees involved.
- Had effective internal controls and compliance policies and procedures.

The FCPA Guide also demonstrates that the DOJ and the SEC use different criteria to determine whether a company or an individual will receive credit for self-reporting, cooperation, or remedial efforts: the DOJ looks to the aforementioned Principles, and the SEC uses the Seaboard Report and guidance it issued in 2001. However, the FCPA Guide emphasizes that both the DOJ and the SEC "place a high premium on self-reporting, along with cooperation and remedial efforts."

Additionally, the FCPA Guide provides clarity about what constitutes an "effective" anti-corruption compliance program, specifically rejecting a one-size-fits-all approach, and focusing instead on a risk-based approach appropriate to the organization's size and complexity. The FCPA Guide also offers factor-based criteria that a company should consider for several high-risk areas, including:

- Gifts and entertainment.
- Charitable contributions.
- Due diligence on third parties.
- Merger and acquisitions due diligence.

While the FCPA Guide may not answer every question or criticism concerning the government's enforcement and interpretation of the FCPA, it does provide valuable insights for outside and in-house counsel on how the government approaches key enforcement decisions and assesses the company's anti-corruption compliance efforts in the FCPA arena.

For more information about the FCPA, see *Practice Notes, The Foreign Corrupt Practices Act: Overview (http://us.practicallaw.com/0-502-2006)* and *Mapping an FCPA Strategy: Internal Investigations and Enforcement Proceedings (http://us.practicallaw.com/7-606-5911).*

CONSPIRACY

Another staple of federal prosecutions are conspiracy charges. The federal government's general conspiracy statute makes it illegal to agree to commit any offense against the US (*18 U.S.C. § 371*). In addition to Section 371, numerous other federal statutes proscribe conspiracies to violate specific federal laws (see, for example, *18 U.S.C. § 24* (health care laws); *18 U.S.C. § 1962(d)* (racketeering laws); *15 U.S.C. § 1* (antitrust laws)). Federal prosecutors frequently use Section 371 to persuade defendants to plead guilty because the five-year statutory cap on the conspiracy charge is generally less than the underlying white collar offense.

CRIMINAL ANTITRUST VIOLATIONS

The Sherman Antitrust Act is the primary tool used by the government to combat antitrust violations (*15 U.S.C. §§ 1-7*). The Sherman Act makes it illegal to enter into a combination or conspiracy in restraint of trade. Examples of conduct that may constitute antitrust violations include bid-rigging, price-fixing and tying arrangements (see *Practice Note, US Antitrust Laws: Overview: Per Se Illegality (http://us.practicallaw.com/9-204-0472)*). The DOJ's Antitrust Division is responsible for enforcement of the Sherman Act.

Aggressive antitrust enforcement can often converge with FCPA enforcement, as evidenced by a string of bid-rigging convictions in the marine hose market (see *DOJ Press Release, Japanese Executive Pleads Guilty, Sentenced to Two Years in Jail for Participating in Conspiracies to Rig Bids and Bribe Foreign Officials to Purchase Marine Hose and Related Products (Dec. 10, 2008)*; *DOJ Press Release, Eight Executives Arrested on Charges of Conspiring to Rig Bids, Fix Prices, and Allocate Markets for Sales of Marine Hose (May 2, 2007)*; *DOJ Press Release, Bridgestone Corporation Agrees to Plead Guilty to Participating in Conspiracies to Rig Bids and Bribe Foreign Government Officials (Sept. 15, 2011)*). As the marine hose cases illustrate, collusive cartel agreements to engage in bid-rigging or price-fixing may also involve payments to foreign officials to ensure that a particular cartel member is awarded a certain contract. Moreover, the government's examination of collusive conduct among industry partners may result in close scrutiny of company payments, which in turn, may have been used to support a bribe payment in violation of the FCPA.

CRIMINAL INTENT IN WHITE COLLAR CASES

With the exception of certain strict liability regulatory offenses that dispense with the element of intent, most successful white collar prosecutions turn on whether the government can prove that the defendant intentionally broke the law. Criminal intent is also called *mens rea* (Latin for "guilty mind"). This section of the Practice Note discusses some of the key issues that arise in white collar prosecutions concerning whether the defendant possessed sufficient criminal intent to support a conviction.

DEFINING "WILLFULLY"

To support a conviction under most of the US anti-fraud statutes, the government must prove that the defendant acted "willfully." However, the term "willfully" has been given various meanings. One definition of "willfully" (as used in tax cases) requires proof that the defendant intentionally violated a known legal duty. Another more general definition of "willfully" requires only proof that the defendant knowingly committed the criminal act, regardless of whether she also knew that her actions were illegal. Under a third definition, "willfully" means that an individual acted with the intent to do something unlawful (that is, acted with a bad purpose), but does not require proof that she knew the specific law that she violated. Because defining the level of "willfulness" sufficient to support a conviction under a particular statute may significantly affect the government's burden of proof, that issue can be a major battleground in white collar criminal prosecutions. Thus, the outcome of that battle can be a deciding factor in whether or not a defendant fights the charges or agrees to a plea agreement.

NEGATING CRIMINAL INTENT

To negate the "willful" element of a criminal charge, defendants typically argue that they acted in good faith. A defendant may have acted in good faith, for example, where she made an honest mistake in judgment or an honest error in management.

Acquittals in the Bear Stearns case (the government's most prominent criminal case against Wall Street executives) underscore the importance of the good faith defense in complex white collar prosecutions (see *United States v. Cioffi & Tannin, 08-cr-0415 (E.D.N.Y., indictment filed Jun. 18, 2008)*). In *Cioffi & Tannin*, prosecutors alleged that the defendants "lied over and over" and misled investors about the stability of their funds. Although the prosecutors relied on an e-mail saying "the entire subprime market is toast," defense lawyers successfully accused prosecutors of taking evidence out of context and argued that just about everyone was blindsided by the financial crisis.

A variation of the "good faith" defense involves reliance on the advice of counsel, whereby the defendant claims an honest misunderstanding of her legal duties based on advice she received from her lawyer. To qualify for the "advice of counsel" defense, however, the defendant must have fully disclosed all relevant facts to her lawyer. In addition, courts generally hold that a defendant impliedly waives the attorney-client privilege by advancing an advice of counsel defense. For more information on waiver of the attorney-client privilege and the advice of counsel defense, see *Practice Note, Attorney-Client Privilege: Waiving the Privilege: Reliance on Legal Advice (http://us.practicallaw.com/0-503-1204).*

COMPANY AND MANAGERIAL LIABILITY FOR THE UNLAWFUL ACTS OF CORPORATE EMPLOYEES

It is well-established that company employees may be liable for the crimes they commit while acting within the scope of their employment. That an employee commits a crime in her "corporate" capacity does not insulate her from personal liability. It is also just as clear that, under certain circumstances, an employee's illegal acts may be imputed to the corporation and corporate management. Corporate and managerial liability for wrongdoing committed by company employees (or agents) stretches across the spectrum of vicarious, successor and strict liability.

VICARIOUS LIABILITY: HOLDING THE CORPORATION LIABLE FOR AN EMPLOYEE'S ILLEGAL ACTS

Vicarious liability, rooted in common law principal-agency concepts, allows an agent's criminal conduct and intent to be imputed to the corporation. Generally, a company may be criminally liable for the conduct of a single low-level employee if the employee acted within the scope of her employment and the employee was, at least in part, motivated to benefit the corporation.

STRICT LIABILITY: HOLDING CORPORATE EXECUTIVES LIABLE FOR AN EMPLOYEE'S ILLEGAL ACTS

In addition to holding corporations liable for the illegal acts of their employees, company officers and directors may also be held liable for an employee's criminal acts under certain circumstances. In the white collar context, the two main bases for holding corporate executives strictly liable for the acts of their employees are the "responsible corporate officer" doctrine and "control person" liability under Section 20(a) of the Exchange Act.

For information about handling a government investigation of a corporate executive, see *Checklist, Handling a Government Investigation of a Senior Executive Checklist (http://us.practicallaw.com/9-501-9764).*

"Responsible Corporate Officer" Doctrine

Under the "responsible corporate officer" (RCO) work doctrine, individual corporate agents with supervisory responsibility may be criminally liable for failing to prevent the commission of corporate crimes, regardless of their knowledge or intent, where they were personally responsible for, or had knowledge of, the criminal violation (see *United States v. Park, 421 U.S. 658 (1975)*; *United States v. Dotterweich, 320 U.S. 277 (1943)*). The RCO doctrine is generally confined to statutes that expressly provide for vicarious personal liability, like the Federal Food, Drug and Cosmetic Act (see *Meyer v. Holley, 537 U.S. 280, 287 (2003)*).

In 2007, the government used the RCO liability theory to obtain massive financial penalties against three corporate executives of Purdue Frederick Company, the manufacturer of the prescription painkiller OxyContin (see *DOJ Press Release, The Purdue Frederick Company, Inc. and Top Executives Plead Guilty to Misbranding Oxycontin; Will Pay Over $600 Million (May 10, 2007)*). The executives were convicted of misdemeanor misbranding charges and were ordered to disgorge millions of dollars of income. Unlike their employer, the executives were not charged with personal knowledge of the misbranding or any personal intent to defraud. Since 2007, the government has become more aggressive with its use of the RCO doctrine; that trend likely will continue.

Control Person Liability

Under Section 20(a) of the Exchange Act, a person who "controls" another person or entity subject to regulation under the Exchange Act may be held jointly and severally liable for the unlawful acts of the "controlled" person or entity. However, Section 20(a) exempts from liability "control persons" who acted in good faith and did not directly or indirectly induce the act constituting the violation (*15 U.S.C. § 78t(a)*.)

Control person liability also applies to violations of the FCPA, which has been incorporated into the Exchange Act. Traditionally, the SEC targeted as "control persons" only executives who had direct knowledge of FCPA violations, like bribe payments or books and records violations. However, that is no longer the case. Now, a company's senior executives may be personally responsible for the misconduct of subordinate employees and managers who have much greater day-to-day responsibility for ensuring that the company's books and records are accurate.

In July 2009, for example, the SEC charged the nutritional and personal care products company Nature's Sunshine Products, Inc. with various FCPA violations committed by its Brazilian subsidiary (see *SEC Press Release, SEC Charges Nature's Sunshine Products, Inc. with Making Illegal Foreign Payments (July 31, 2009)*). Moreover, the SEC took the additional step of charging Nature's Sunshine's executives with violations of the FCPA based on their positions as "control persons" under Section 20(a), even though they had no knowledge of the subsidiary's actions or even direct responsibility for the company's records and filings at issue in this case. The SEC charged the executives with failing to supervise their personnel to ensure the company's books and records were accurately prepared and that an adequate system of internal controls was in place. The expansive use of strict liability in the Nature's Sunshine case is consistent with the government's stated policy to use individual prosecutions as a means to deter and punish corporate crime (see *US top cop says Justice Department using new tools (Feb. 25, 2010)*).

SUCCESSOR LIABILITY: HOLDING THE CORPORATION LIABLE FOR ITS PREDECESSOR'S CONDUCT

Successor liability has also become an increasingly important issue in white collar prosecutions, particularly in the mergers and acquisitions context. US enforcement authorities do not view a merger or acquisition (whether by way of stock or asset purchase) as extinguishing liability for past illegal conduct and will hold the new company or newly acquired subsidiary responsible for the predecessor's conduct. For example, in February 2009, Kellogg Brown & Root (KBR) pleaded guilty to violations of the FCPA even though it had been set up as a new company after the

bribery scheme ended, its new owners did not profit from the bribery and its new management had no knowledge of the bribery (see *DOJ Press Release, Kellogg Brown & Root LLC Pleads Guilty to Foreign Bribery Charges and Agrees to Pay $402 Million Criminal Fine (Feb. 11, 2009)*).

IMPUTING CRIMINAL INTENT TO THE CORPORATION

As noted above (see *Criminal Intent in White Collar Cases*), the US anti-fraud statutes generally require some level of criminal intent to support a conviction. The intent element applies whether the defendant is a natural person or an organization, like a corporation. Therefore, to hold a corporation criminally liable for its employees' misdeeds, the government must show that the corporation also possessed the requisite criminal intent. This is typically done by imputing the employee's *mens rea* to the corporation because the corporation is a fictional entity with no thoughts or will of its own. In the corporate context, there are essentially three ways to impute the criminal intent of corporate employees to the company:

- Vicarious liability.
- The collective knowledge doctrine.
- The willful blindness doctrine.

Vicarious Liability

Even if the company itself did not possess actual knowledge of its employee's (or agent's) illegal activities, some courts allow the *mens rea* of the offending employee to be imputed to the company under a vicarious liability theory. For courts that use this theory, the only criminal intent that the prosecution must prove is that of the employee.

Collective Knowledge Doctrine

A variant on vicarious liability is the collective knowledge doctrine. Under the collective knowledge doctrine, the cumulative knowledge of several corporate employees (or agents) may be imputed to the corporation, even if no single actor knows all of the facts necessary to constitute the requisite *mens rea* to commit a particular crime. In other words, the corporate employer may be found to possess the requisite criminal intent to support a conviction by aggregating the knowledge of each of its employees (see *United States v. Bank of New England, 821 F.2d 844, 856 (1st Cir. 1987)*).

Willful Blindness Doctrine

Under the willful blindness doctrine, the criminal intent of a corporate employee or agent may be imputed to the corporation if the corporation and its management purposefully avoided learning of the illegal conduct. Willful blindness essentially serves as a substitution for negligence.

The government now construes a breakdown in internal compliance controls as an effort to adopt a "head in the sand" approach to legal compliance. For example, in an enforcement action against Halliburton, the SEC charged the company with a civil violation of the FCPA's anti-bribery provisions without alleging that Halliburton had any knowledge of the bribe payments at issue. Instead, the government premised Halliburton's liability on its failure to conduct sufficient due diligence of a foreign agent who, while working on behalf of Halliburton's joint venture, made illegal bribe payments (see *Complaint, SEC v. Halliburton Co. and KBR, Inc., No. 09-cv-0399, at 31 (S.D. Tex. Feb. 11, 2009)*).

EFFECTIVE COMPLIANCE PROGRAMS MAY BE THE BEST DEFENSE TO WHITE COLLAR PROSECUTIONS

Today's enforcement climate underscores the need for an effective compliance program. For many prosecutors, the lack of an effective compliance program that could have averted the wrongdoing suggests a corporate intent to enable and benefit from the wrongdoing. This section of the Practice Note discusses the main points to consider in developing an effective compliance program.

COMPLIANCE PROGRAMS REQUIRED FOR CERTAIN COMPANIES

Compliance has now become a part of the statutory and regulatory landscape. For example, Section 404 of Sarbanes-Oxley requires certain executives of publicly held companies to file with the SEC internal control reports on the effectiveness of the company's internal controls structure. Section 404 also requires the company's auditor to attest to, and report on, the company's assessment of its internal controls over financial reporting.

COMPLIANCE PROGRAMS AS A WAY TO REDUCE CRIMINAL SANCTIONS

Having an effective compliance program is not a legal defense to charges of corporate wrongdoing. However, a company can potentially reduce the penalties that may be assessed against it for errant corporate misconduct if it can prove that it had an effective compliance program in place during the relevant time period. Furthermore, the existence (or non-existence) of an effective compliance program is one of the factors that a prosecutor will take into consideration in determining whether to bring charges against a company (see *US Attorney's Manual 9-28.300(A)(5)*).

What is an "Effective" Compliance Program?

The US Sentencing Guidelines (USSG) identify seven specific criteria that constitute an "effective" compliance program. These criteria require the organization to:

- Establish written standards and procedures to prevent and detect criminal conduct.
- Assure that its senior board and executive leadership are knowledgeable about the content and operation of the compliance program, exercise reasonable oversight of the implementation and effectiveness of the compliance plan and designate a specific individual with direct reporting responsibility to the board or a subgroup of the board.
- Use reasonable efforts not to include within the management team any individual the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance plan.
- Communicate periodically and in a practical manner its compliance standards and procedures by conducting effective training programs involving board members, senior executives, management, employees and agents of the organization.
- Devote sufficient resources to audit and monitor the effectiveness of the compliance plan, including implementing a confidential whistleblower process allowing employees and others to report criminal conduct without fear of retribution.

- Enforce the compliance program throughout the organization by using appropriate incentives and consistently applied disciplinary measures.
- Take reasonable steps to implement reasonable remediation efforts once criminal conduct has been detected by:
  - remedying the harm caused by the criminal conduct (including restitution, self-reporting and cooperation with authorities); and
  - assessing the organization's existing compliance program to make relevant changes to the program (which may include potentially engaging outside professional advisors as necessary).

(*USSG § 8B2.1(b).*)

2010 Amendments to the USSG Make It Potentially Easier to Obtain Leniency

Traditionally, corporations with "effective" compliance programs could not obtain leniency under the USSG if high-level company executives were involved in the illegal conduct at issue. However, amendments to the USSG (effective November 1, 2010) allow a company to obtain credit for an effective compliance program even where a high-level executive was involved in the misconduct, as long as:

- The head of compliance reports directly to the board.
- The compliance program detected the criminal conduct before it was discovered or was reasonably likely to be discovered outside of the organization.
- The organization promptly reported the offense to the government.
- No corporate compliance officers were involved with, condoned or were willfully ignorant of the criminal offense.

(*USSG § 8C2.5(f).*)