

# Prosecutors Without Borders: Emerging Trends In Extraterritorial Enforcement

---

*Douglas N. Greenburg, Barry M. Sabin, Nathan H. Seltzer, Jessica K. Thibodeau<sup>1</sup>*

---

<sup>1</sup> Mr. Greenburg is a partner in the Washington office of Latham & Watkins LLP and a Vice-chair of the Global Litigation Department. Mr. Sabin is a partner in the Litigation Department in the Washington office of Latham & Watkins LLP. Mr. Seltzer and Ms. Thibodeau are associates in the Litigation Department in the Washington office of Latham & Watkins LLP.

Around the beginning of 2000, there were approximately eight federal investigations by the United States related to foreign bribery ongoing at any given time.<sup>2</sup> In 2010, the Department of Justice (“DOJ”) announced that it had more than 130 open Foreign Corrupt Practices Act (“FCPA”) investigations. This is hardly surprising given the Obama Administration’s vow to crack down on global corruption—a continuation of the expanded FCPA enforcement efforts begun under the Bush Administration. Linking corruption to national security issues like terrorism and arms trafficking, Obama Administration officials have characterized corruption as “a scourge on civil society” and “one of the great struggles of our time.” The Administration has allocated the resources—at the DOJ, FBI, SEC, and other agencies—to vigorously investigate and enforce the FCPA and is targeting companies across the world, even ones with little to no material contact with the United States. The head of the Justice Department’s Criminal Division announced on November 16, 2010 that “FCPA enforcement is stronger than it’s ever been – and getting stronger.”

U.S. companies are not the only entities that must be concerned about FCPA compliance. All companies and individuals doing business in foreign markets must be aware of the legal risks the Act presents, particularly as the global reach of the U.S. government’s enforcement continues to expand. The expansion of extraterritorial jurisdiction—a term generally referring to the investigation and prosecution of companies and individuals by U.S. authorities for acts undertaken outside the territorial jurisdiction of the United States—began in earnest with the 1998 amendments to the FCPA. The current position of the U.S. government is that the FCPA can apply to foreign nationals and foreign companies for bribe payments made anywhere in the

---

<sup>2</sup> These statistics were reported by the Washington Post in May 2010. See Mark Brzezinski, *Obama administration gets tough on business corruption overseas*, WASH. POST, May 28, 2010.

world, based on fairly minimal contact with the United States. The new UK Bribery Act, the UK's equivalent of the FCPA, extends even further. Under the UK Bribery Act, a non-UK company that bribes a private non-UK citizen to retain business that is entirely unconnected with the UK could theoretically fall within the Act's purview. The exposure for multinational corporations and international business executives is vast. Coupled with the aggressive appetite for investigation and enforcement through criminal indictments and onerous settlements and fines, no company can afford to be anything less than vigilant.

A vigilant company should assess its risk and take steps to minimize its vulnerabilities. The first step down that road requires a company to understand the aggressive prosecution theories and innovative investigation techniques recently utilized by U.S. authorities. The DOJ has increased its efforts to target particular individual corporate executives. Multinational cooperation is also increasing. In this article, we highlight emerging patterns and issues that companies and individuals—U.S. or otherwise—should be aware of to understand the risks associated with doing business abroad. Once an entity appreciates these risks, it can take necessary steps to respond to potential violations—or better yet, prevent them before they occur.

## **I. THE FCPA AT A GLANCE**

The FCPA criminalizes corrupt payments to foreign officials for the purpose of obtaining or retaining business. Specifically, the Act's anti-bribery provisions prohibit the use of the mail or any instrumentality of interstate commerce in furtherance of a corrupt offer, payment, promise to pay, or authorization to pay money to any foreign official for the purpose of influencing the official in his or her official capacity, inducing the official to violate his or her lawful duty, or securing an improper business advantage. Under the Act's broad reach, U.S. nationals and

companies are covered anywhere in the world, without regard to any nexus to interstate commerce. The term “foreign official” is broadly defined to cover not only officers and employees of foreign governments, but also anyone acting in an official capacity for or on behalf of a government department, agency, or instrumentality. The DOJ’s position is that this includes employees of state-owned and state-controlled commercial entities.<sup>3</sup> The government does not need to prove actual knowledge of a payment’s corrupt purpose to impose liability under the FCPA. The courts have held that the Act’s knowledge requirement incorporates the concepts of willful blindness and conscious disregard. Therefore, corporate executives cannot bury their heads in the sand and ignore the suspicious actions of their agents in an attempt to escape FCPA liability.

When the statute was enacted in 1977, its anti-bribery provisions applied only to U.S. nationals, U.S. firms, and issuers, meaning any companies —foreign or domestic — that issue securities registered in the U.S. or are required to file reports with the SEC. Congress amended the FCPA in 1998 to expand its scope. The FCPA’s anti-bribery provisions now also apply to non-U.S. firms and individuals who cause, either directly or through an agent, an act in furtherance of a corrupt payment within the U.S. Additionally, U.S. parent companies can be held liable for acts of their foreign subsidiaries if the parent authorized, directed, or controlled the activity that constituted the FCPA violation.

The FCPA also includes important accounting provisions that work in conjunction with its anti-bribery prohibitions. The accounting provisions are not limited in their application to

---

<sup>3</sup> In the closely watched Control Components case in the Central District of California, the defendants have moved to dismiss the indictment, arguing that employees of state-owned enterprises are not “foreign officials” within the meaning of the statute. This is the first time a federal court will squarely address this issue.

international transactions or to deals involving illegal bribe payments. They apply to all the financial dealings, both within and beyond the U.S., of all U.S. and foreign companies required to file reports or register their securities with the SEC. Substantively, the accounting provisions require companies to maintain books and records in reasonable detail that accurately and fairly reflect the transactions and dispositions of their assets. The accounting provisions also mandate that companies devise and maintain adequate internal accounting systems to ensure that their financial statements are accurate and maintain appropriate control of corporate assets. Indeed, although the DOJ and SEC aggressively investigate and seek to enforce the FCPA's anti-bribery provisions, it is often the books and records provisions that make up the ultimate charges against a company.

The FCPA is jointly enforced by the DOJ and the SEC. Corporations and other entities are subject to criminal fines of up to \$2,000,000 per violation. Officers, directors, stockholders, employees, agents, and other individuals can face criminal fines of up to \$100,000 and imprisonment for up to five years. Pursuant to the Alternative Fines Act, actual fines can be even higher – as much as twice the benefit the defendant sought to gain by making the corrupt payment. Individuals and companies are subject to civil fines of up to \$10,000. In SEC enforcement actions, courts may also impose additional fines based on the pecuniary gain to the defendant as a result of the violation and the egregiousness of the violation. Additionally, the government can impose non-monetary sanctions on companies, such as prohibiting companies from engaging in future business transactions with the federal government or from obtaining export licenses.

Recent years have seen FCPA enforcement at an all-time high. That trend continued in 2010. There were several noteworthy FCPA case resolutions in 2010, including a February 2010

plea agreement in which BAE Systems agreed to pay \$400 million to the DOJ and \$47 million to the U.K. Serious Fraud Office stemming from charges that the company, Europe's largest defense contractor, made illegal bribe payments to obtain government contracts in many countries around the world. BAE Systems also agreed to engage an independent corporate monitor for three years. On April 1, Daimler AG agreed to pay \$93.6 million in criminal penalties and disgorge \$91.4 million in profits to resolve allegations of FCPA violations, marking the fourth largest FCPA-related settlement ever at that time. As in the BAE Systems settlement, Daimler agreed to hire a monitor—in this matter former FBI Director Louis Freeh to address its FCPA compliance efforts for a three year period. In November 2010, global freight forwarding company Panalpina, Inc. and six oil companies agreed to pay a total of \$80 million in civil disgorgement, interest, and penalties and \$156.5 million in fines to the DOJ related to allegations that Panalpina bribed foreign officials in order to receive improper benefits during the customs process on behalf of its customers in the oil and gas industry and a host of other issues that arose during the course of the investigations.

## **II. EXTRATERRITORIAL ENFORCEMENT: THE EXPANSIVE REACH OF THE FCPA**

In recent years, U.S. authorities have begun to aggressively use the FCPA and related money laundering statutes to target conduct that seemingly has very little connection with the U.S. Recent high-profile cases against German conglomerate Siemens AG and Norwegian oil giant Statoil are examples of the U.S. government's push to expand the territorial reach of the FCPA. Siemens is listed on the New York Stock Exchange and therefore qualifies as an "issuer" under the FCPA. In December 2008, Siemens and three of its subsidiaries pleaded guilty to violating the FCPA and agreed to pay a record-setting \$1.6 billion in criminal and civil fines and penalties. Although as an issuer, Siemens is subject to the FCPA, in its complaint against

Siemens, the SEC suggested that the necessary territorial connection to the U.S. was also achieved by way of illegal payments funneled through U.S.-based “correspondent accounts.” When funds in U.S. dollars are transferred from one foreign bank account to another, they generally pass through correspondent accounts in the U.S. If the mere act of funds passing through U.S. correspondent accounts is considered a sufficient basis for FCPA jurisdiction, it would mean that all companies could be subject to the FCPA’s anti-bribery provisions for bribes paid by foreign entities outside of the U.S. to foreign government officials if—even without the bribe promisor’s knowledge or intent—those payments travel through a correspondent account in the U.S.

In 2006, Statoil, a Norwegian oil company, agreed to pay \$21 million to settle charges alleging that it violated the FCPA by bribing an Iranian official to win oil and gas contracts. At the time, the fine against Statoil was the largest fine ever imposed on a foreign company in an FCPA case. Statoil also agreed to retain an independent compliance monitor to examine its FCPA compliance for a three year period. Although the bribe payments in question were paid by a foreign company to a foreign official outside of the U.S., Statoil was subject to U.S. jurisdiction because the company is listed on the New York Stock Exchange and the bribe payments were routed through a New York bank. The case against Statoil marked the first DOJ action against a foreign issuer with no U.S. operations, and U.S. authorities have continued to aggressively target foreign companies for violating the FCPA.

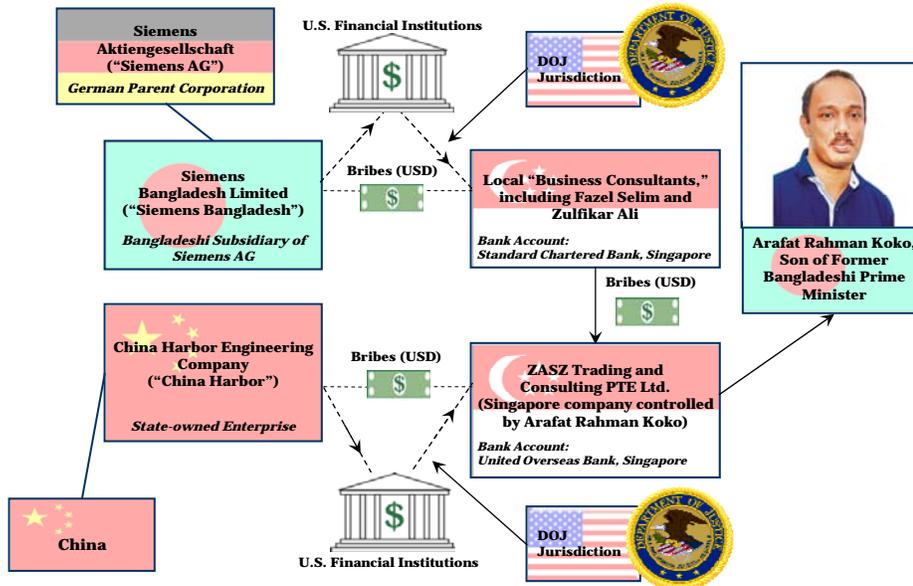
Recent DOJ and SEC actions indicate that U.S. authorities may seek to enforce the FCPA against wholly-owned foreign subsidiaries of U.S. issuers based on conduct of the subsidiary that occurred completely outside of the U.S. and without any knowledge or involvement of the parent corporation. In July 2010, the SEC pursued Snamprogetti Netherlands B.V. (“Snamprogetti”), a

Dutch company indirectly owned by ENI, S.p.A. (“ENI”), a U.S. issuer, for violating the FCPA. Although SEC jurisdiction was based on the assertion that Snamprogetti acted as an agent of ENI, the complaint did not assert any specific facts demonstrating the existence of an agency relationship beyond a typical parent-subsidary relationship. Although the government will likely face legal impediments, both statutory and constitutional, to charging a foreign subsidiary under the FCPA for such conduct, this is yet another example of U.S. law enforcement authorities pushing the jurisdictional limits of the FCPA’s anti-bribery provisions.

In a new development, foreign government officials are now also being targeted by U.S. authorities for accepting bribe payments. Because the FCPA only applies to the supply-side of bribe transactions—that is, to the bribe-promiser—the FCPA does not provide a basis for punishing foreign officials who accept bribes. But, as part of its overall FCPA enforcement, the DOJ has recently begun using money laundering and forfeiture laws to pursue the ill-gotten gains of foreign officials that have been bribed in violation of the FCPA. During the African Union Summit in July 2010, Attorney General Holder announced the DOJ’s Kleptocracy Asset Recovery Initiative. This Initiative, led by DOJ’s Asset Forfeiture and Money Laundering Section (“AFMLS”), and a continuation of a kleptocracy initiative started under the Bush Administration, aims to recover assets from high-level foreign officials on behalf of countries that are victimized by public corruption. In the aftermath of the recent political turmoil in Tunisia, several countries, including Switzerland and Canada, have joined forces to freeze the assets of former President Ben Ali and his associates to prevent his misuse of the funds. These moves send a clear message to corrupt public officials that they cannot use other countries as safe havens for their stolen gains.

One of the AFMLS's first actions was related to the Siemens matter. Less than one month after Siemens pleaded guilty to violating the FCPA and agreed to pay record-setting fines, AFMLS filed a related forfeiture action to confiscate approximately \$3 million from multiple bank accounts located in Singapore. The DOJ alleged that these funds were the proceeds of the bribe payments that Siemens, Siemens Bangladesh Limited, and China Harbor Engineering Company paid to Bangladeshi government officials to secure government contracts. On April 7, 2010, a federal judge ordered the forfeiture of funds from three bank accounts in Singapore belonging to Arafat Rahman Koko, son of former Bangladeshi Prime Minister Khaleda Zia, and two of Koko's "business consultants." Although the funds were paid by Bangladeshi and Chinese entities and deposited into the Singaporean accounts of non-U.S. citizens, they were nonetheless subject to the DOJ's jurisdiction under U.S. money laundering laws because they were paid in U.S. dollars and therefore moved through the U.S. financial system before being deposited in Singapore. The diagram below depicts the links between the various foreign entities involved in Koko's bribery scheme and the jurisdictional hook that allowed the DOJ to pursue a forfeiture action.

## The Arafat Rahman Koko Forfeiture Action



Similarly, in December 2009, two former Haitian officials were indicted on money laundering charges for accepting bribes from three U.S. telecommunications companies. Robert Antoine, the former Director of International Affairs for Haiti Teleco, pleaded guilty to conspiracy to commit money laundering in March 2010. Antoine was sentenced to 48 months in prison and ordered to pay more than \$1.8 million in restitution and forfeit an additional \$1.6 million. Jean Rene Duperval, also a former Director of International Relations for the company, was charged with conspiracy to commit money laundering and 12 counts of money laundering. Duperval, who has not yet pled, is scheduled to face trial on these charges in 2011. U.S. authorities will undoubtedly continue to prosecute foreign companies and officials for paying and receiving bribes, regardless of where the bribes were paid.

### **III. A WARNING FROM THE DOJ TO CORPORATE EXECUTIVES: YOU WILL BE HELD PERSONALLY ACCOUNTABLE FOR YOUR COMPANY'S FCPA VIOLATIONS**

Prosecution of individual corporate executives and the imposition of hefty prison sentences are cornerstones of the DOJ's multi-pronged FCPA enforcement strategy. A leading DOJ enforcement official warned in late 2009 that the DOJ will impose significant prison sentences on individuals for FCPA violations they participated in or oversaw – “[p]ut simply, the prospect of significant prison sentences for individuals should make clear to every corporate executive, every board member, and every sales agent that we will seek to hold you personally accountable for FCPA violations.” The DOJ has indicated that it believes putting executives in prison may be an effective means of curbing FCPA violations. From 2007 to 2008, the DOJ and the SEC brought FCPA cases against over 30 individuals. In 2009 alone, 28 individual executives were prosecuted for FCPA violations—ten more than the number of FCPA prosecutions of corporations in 2009. Targeted enforcement against individuals continued in 2010 and the number of indictments against individuals will almost certainly continue to grow as the DOJ has emphasized individual accountability.

Executives cannot afford to be dismissive. Albert “Jack” Stanley, the former chairman of Kellogg, Brown & Root, Inc., was charged with conspiracy to violate the FCPA and conspiracy to commit mail and wire fraud for his role in overseeing and participating in a scheme to bribe Nigerian government officials in order to obtain more than \$6 billion in government contracts. In September 2008, Stanley pleaded guilty to both counts and agreed to serve a seven year prison sentence and pay \$10.8 million in restitution. At the time it was imposed, Stanley's seven year jail sentence was the longest ever imposed on an individual under the FCPA. Since then, Charles Jumet, the former Vice President of Ports Engineering Consultants Corporation, pleaded guilty to

conspiring to violate the FCPA and to making a false statement to federal agents related to bribes his company paid to secure maritime contracts in Panama. On April 19, 2010, Jumet was sentenced to 87 months in prison and fined \$15,000. Jumet must also serve three years of supervised release following his prison term.

Stanley and Jumet were both involved in and aware of their company's bribery schemes. However, corporate executives have also been targeted in cases brought under the theory of willful blindness. On July 10, 2009, a federal jury found Frederic Bourke Jr., co-founder of handbag designer Dooney & Bourke, guilty of conspiracy to violate the FCPA.

In the late 1990s, Bourke invested \$8 million in Oil Rock Group Ltd., a company established by his friend Viktor Kozeny that was set up to induce the Azeri government to privatize Azerbaijan's state-owned oil company. According to the indictment, investors grew concerned and suspicious after Kozeny began to make excuses to explain delays in the privatization plan. The prosecution alleged that Bourke was a knowing participant in Kozeny's scheme. To establish knowledge, the government presented two theories – that Bourke had actual knowledge of the bribe payments, or alternatively, that Bourke buried his head in the sand and ignored red flags that arose as his business relationship with Kozeny developed. Although it is not clear on which theory the jury based its guilty verdict, an opinion by the judge permitting the government to introduce circumstantial evidence of general red flags related to Kozeny was novel and could have broad implications on future FCPA cases. The prosecution recommended a 10 year jail sentence for Bourke. Notwithstanding this recommendation, a federal judge sentenced Bourke to just one year and one day in prison and ordered him to pay a \$1 million criminal fine.

No corporate executives, even Hollywood film producers, are immune from the FCPA. On September 11, 2009, a California jury found producers Gerald and Patricia Green guilty on 19 counts, including conspiracy to violate the FCPA and nine substantive counts of violating the FCPA. The indictment alleged that the Greens, owners of Film Festival Management Inc., paid \$1.8 million in bribes to the head of the Tourism Authority of Thailand in order to win contracts to run the annual Bangkok International Film Festival. Gerald Green faced more than 30 years in prison, while Patricia could have received a 19 to 24 year prison term. The court held several sentencing hearings over the course of eight months before deciding on appropriate punishments for the Greens. On August 12, 2010, Judge George Wu sentenced the couple to six months in prison, followed by six months of home confinement. Judge Wu also ordered the couple to pay \$250,000 in restitution. Gerald's advanced age and poor health and Patricia's role as Gerald's primary caretaker likely contributed to this relatively lenient sentence.

The sentences imposed on Bourke and the Greens were far lower than those recommended by the prosecution. Those cases represent two examples where federal judges may not have viewed the violations as severely as the DOJ. But, both cases also had unique facts that may have justified the relatively lenient sentences. Regardless, the U.S. government's increased focus on individual prosecutions means that companies and individual executives can no longer view monetary fines imposed for FCPA violations as just another cost of doing business. The threat that individual executives may be deprived of their liberty for violating the FCPA may deter violations in a way that even astronomical fines cannot.<sup>4</sup>

---

<sup>4</sup> The SEC has also utilized creative legal theories to aggressively target individual executives. In July 2009, the SEC filed a settled enforcement against Nature's Sunshine Products, Inc. and its CEO and former CFO. The SEC did not allege that the officers were involved in or even aware of the alleged misconduct of the company's Brazilian subsidiary. Rather, the officers were charged with violating the FCPA's books and

#### IV. INDUSTRY-WIDE INVESTIGATIONS: WILL YOUR INDUSTRY BE NEXT?

FCPA risk exists for all companies conducting business abroad. However, companies in certain industries with more significant interactions with government officials may prove more vulnerable to FCPA liability than others. The pharmaceutical and energy industries – due in part to the distinct nature of these industries and the countries in which they operate – have received intense scrutiny from investigators in recent years. Companies operating in these industries, and others with similar characteristics, should be particularly vigilant about their FCPA compliance efforts and closely monitor the activities of their competitors. And in the end, all companies must be prepared for the day authorities move on to their industry.

In November 2009, the Justice Department announced it will enhance its FCPA enforcement efforts geared towards the pharmaceutical industry—an industry that generates roughly one-third of its total sales outside the U.S. The DOJ’s focus on this industry stems mainly from the fact that many foreign health systems are regulated, operated, and financed by government entities, creating countless contact points between pharmaceutical companies and foreign government officials. Competition within the industry is also very intense. These two factors create considerable opportunities and pressure for illegal bribery to occur, resulting in a perceived need for greater industry supervision.

Likewise, particular qualities specific to the energy sector help explain why oil and gas companies have been and will continue to be highly vulnerable to the FCPA. As noted above, six multinational oil and oil services companies, including Pride International, Inc., Royal Dutch Shell plc, and Transocean Inc., agreed to massive settlements with the SEC and DOJ in November 2010 to resolve charges involving their freight forwarding company’s bribery of

---

records and internal controls provisions based on their roles as “control persons” under Section 20(a) of the Securities Exchange Act of 1934.

foreign government officials. Energy companies do much of their business in resource-rich countries throughout Africa, Latin America, and the Middle East that are seen as high risk areas for bribery and corruption. Moreover, like the pharmaceutical industry, the oil and gas industry involves a high degree of state-owned companies whose employees are considered foreign officials under the FCPA. Additionally, it is common practice for energy companies to hire agents and foreign consultants to handle their on-the-ground transactions with host country officials. Companies are responsible for the acts of their agents for purposes of FCPA liability and can therefore be prosecuted for bribe payments made by their agents to foreign officials.

**V. NEW LEGISLATION AND A MAJOR SHAKE-UP WITHIN THE SEC'S ENFORCEMENT DIVISION: A PROACTIVE APPROACH TO ENCOURAGING COOPERATION**

Congress recently increased the incentives for whistleblowers to come forward and report FCPA violations to the SEC. The Dodd-Frank Wall Street Reform and Consumer Protection Act, signed into law by President Obama on July 21, 2010, includes a “whistleblower bounty” provision that provides monetary benefits for whistleblowers who report securities law violations to the SEC. Specifically, whistleblowers who provide information that leads the SEC to a successful enforcement action or settlement can receive anywhere from 10 to 30 percent of the amount of the settlement that exceeds \$1 million. For purposes of calculating the bounty payment, the settlement amount is the aggregated amount of the recoveries by the SEC, DOJ, and any other federal and state agencies in related actions. The law does not restrict the type of persons who can receive whistleblower status or require that the whistleblower be a U.S. person. Foreign employees of foreign subsidiaries of U.S. companies are eligible for the whistleblower bounty. Although SEC rules implementing the new provision remain forthcoming, the whistleblower bounty provision will undoubtedly lead to more disclosures of FCPA violations to

the SEC—from both domestic and foreign sources. Anecdotal reports suggest the SEC is already awash in such reports.

A major shake-up within the SEC's organizational structure will also enhance the SEC's ability to process an increased flow of information from the public. On January 13, 2010, the SEC announced the reorganization of its Enforcement Division, including the creation of a specialized national FCPA unit. The SEC Enforcement Division Chief, in an August 2009 speech introducing the changes, announced that the FCPA unit would “focus on new and proactive approaches to identifying violations” and would “work more closely with foreign counterparts and take a more global approach to violations.” Another new office within the Enforcement Division, the Office of Market Intelligence, will act as a nerve center for information coming into the SEC from tips, complaints, and referrals. The Office of Market Intelligence will harness the specialized knowledge within the FCPA unit to better analyze and utilize this incoming information.

In conjunction with the reorganization, the SEC has formally expanded its investigative toolbox through a new initiative. According to the SEC, the Enforcement Cooperation Initiative “has the potential to be a game-changer for the Enforcement Division.” The three new tools in the SEC's FCPA arsenal—tools long used by the DOJ—are cooperation agreements, deferred prosecution agreements, and non-prosecution agreements. The adoption of these tools to incentivize and credit cooperation marks a shift in the SEC's *modus operandi*. In the past, the SEC has relied on its information-gathering powers to compel cooperation without providing any incentives or rewards.

Cooperation agreements are written agreements under which the Enforcement Division agrees to recommend that a cooperating individual or company receive credit in exchange for providing substantial assistance in an investigation and waiving any applicable statutes of

limitation. The Director of the Enforcement Division can enter into cooperation agreements without the Commission's approval; however, the Commission is not bound by the Division's recommendation in its ultimate enforcement decision.

Under a deferred prosecution agreement, the SEC agrees to defer an enforcement action against the cooperator for a set period of time not exceeding five years. In exchange, the individual or company agrees to cooperate fully and truthfully with the SEC's investigation and related enforcement actions. Deferred prosecution agreements must be approved by the Commission. If the cooperator satisfies the terms of the agreement, the Commission will not to pursue any enforcement actions against it. However, if the agreement is violated, the Enforcement Division can recommend that the Commission commence an enforcement action. Any factual admissions made by the cooperator during the course of cooperation can be used against it in the enforcement action.

Lastly, non-prosecution agreements are written agreements that are entered into only in limited circumstances. The Commission will agree not to pursue an enforcement action if an individual or company agrees to cooperate fully and truthfully, pay any disgorgement or penalties, and comply with other express provisions of the agreement. Non-prosecution agreements typically are not available during the early phases of an investigation or where the individual or company is likely to enter into a plea agreement. If the cooperator violates the agreement, the SEC can pursue enforcement actions against it without limitation, using any statements, information, or materials provided by the cooperator against it.

In 2010, the SEC revised its enforcement manual to lay out a framework for evaluating cooperation. The Enforcement Division will take four considerations into account when making its determination: (1) the value and nature of the assistance provided by the cooperator; (2) the seriousness and importance of the underlying matter; (3) the societal interest in ensuring that the

cooperator is held accountable for the misconduct; and (4) the appropriateness of cooperation credit based upon the profile of the cooperator. The SEC claims to have demonstrated the upshot of cooperation in its recent settlement with Siemens AG. Although this settlement occurred before the roll-out of its formal cooperation initiative, the SEC cited Siemens' full cooperation as influencing its decision to settle.

## **VI. WIRETAPS AND STING OPERATIONS: NO LONGER RESERVED FOR MOB INVESTIGATIONS**

The FBI has traditionally used wiretaps, informants, and undercover agents to catch hardened criminals like Mafia bosses and drug lords. However, corporate executives should be aware that the FBI is beginning to use these tactics in white collar investigations. In a May 2010 speech, Assistant Attorney General Lanny Breuer announced that the DOJ intends to start using "aggressive law enforcement techniques" like court-authorized wiretaps in financial fraud, bribery, and corruption cases. Two recent cases demonstrate the potential payoffs of putting these methods to use in the white collar arena.

On October 16, 2009, Galleon Group founder Raj Rajaratnam was arrested on charges that he ran the biggest insider trading scheme ever involving a hedge fund. Taped phone conversations between Rajaratnam and a cooperating witness, Roomy Khan, helped crack open the investigation and led to broader court-ordered wiretaps that produced critical evidence in the case. In 2007, an SEC attorney discovered a suspicious text message sent to Rajaratnam by Khan, a former Galleon employee, while sifting through documents voluntarily disclosed by Rajaratnam in connection with an unrelated investigation. The text urged Rajaratnam not to buy stock in a video-conferencing firm called Polycom until Kahn provided "guidance." Confronted with the incriminating text message, Khan agreed to cooperate with investigators and record her phone conversations with Rajaratnam. Kahn's phone recordings produced enough evidence to

allow prosecutors to obtain a court-authorized wiretap of Rajaratnam's cell phone in 2008.

According to the DOJ, the wiretap revealed a vast insider trading scheme and ultimately yielded over 2,400 recordings that serve as the centerpiece of the government's case.

The use of court-authorized wiretaps in the Galleon Group investigation provided valuable information to authorities but raised novel legal issues that were heavily litigated in federal court in New York prior to Rajaratnam's trial, currently scheduled to begin on March 8, 2011. First, while the Wiretap Act specifically includes wire fraud and money laundering as enumerated grounds for obtaining a court-ordered wiretap, it does not list securities fraud as a basis. Rajaratnam's defense team asserted that the government misled the court in its request for a wiretap when it claimed that the bases for the wiretap were wire fraud and money laundering, when insider trading was the charge ultimately filed. In November 2010, a federal judge denied Rajaratnam's motion to suppress on this basis, concluding that an insider trading scheme conducted using interstate wires qualified as wire fraud. Similarly, the judge was not convinced by Rajaratnam's assertion that the DOJ's wiretap application failed to establish the inadequacy of conventional investigative procedures, as required by the Wiretap Act. The court held that wiretaps were necessary and appropriate, despite the fact that the SEC was pursuing a civil case against Rajaratnam without wiretaps, because the Galleon insider trading scheme was conducted primarily via phone conversations. Whatever the outcome of the trial, the U.S. Attorney for the Southern District of New York made clear that the Galleon case should be viewed as a wake-up call for corporate executives. "Today, tomorrow, next week, the week after, privileged Wall Street insiders who are considering breaking the law will have to ask themselves one important question: Is law enforcement listening?"

The January 2010 large-scale sting operation that resulted in the indictment of 22 corporate executives for violating the FCPA is yet another example of how the FBI is putting traditional investigative tactics to work in the white collar area. FBI agents posing as representatives of the Ministry of Defense of an unidentified African country approached the defendants, all of whom worked at companies that supply military and law enforcement products, and offered them a \$15 million dollar contract to provide equipment for the unnamed country's presidential guard. According to the indictment, the defendants agreed to pay a 20 percent commission to the fictitious country's Defense Minister in return for securing the contract. Although this was not the first time undercover agents were used in an FCPA investigation, this case is notable for the fact that the government completely fabricated the existence of the foreign officials, their country of origin, and the government contract at issue.

In the more than one year since this sting operation was carried out, commentators have noted that sting operations in FCPA cases may be challenged in court under the entrapment defense. To successfully argue entrapment, it must be established that the government induced the crime and the defendants were not predisposed to commit the crime. Another potential hurdle for the prosecution in this case involves whether the fact that the defendants did not attempt to bribe actual "foreign officials" —because the FBI agents posed as officials from a fictitious country—will create potential legal issues as the case moves forward. At any rate, corporate executives must be aware that the U.S. will not shy away from the use of novel and innovative investigative tactics to quash corruption. In the DOJ press release announcing the results of the sting operation, the government cautioned that "[f]rom now on, would-be FCPA violators should stop and ponder whether the person they are trying to bribe might really be a federal agent."

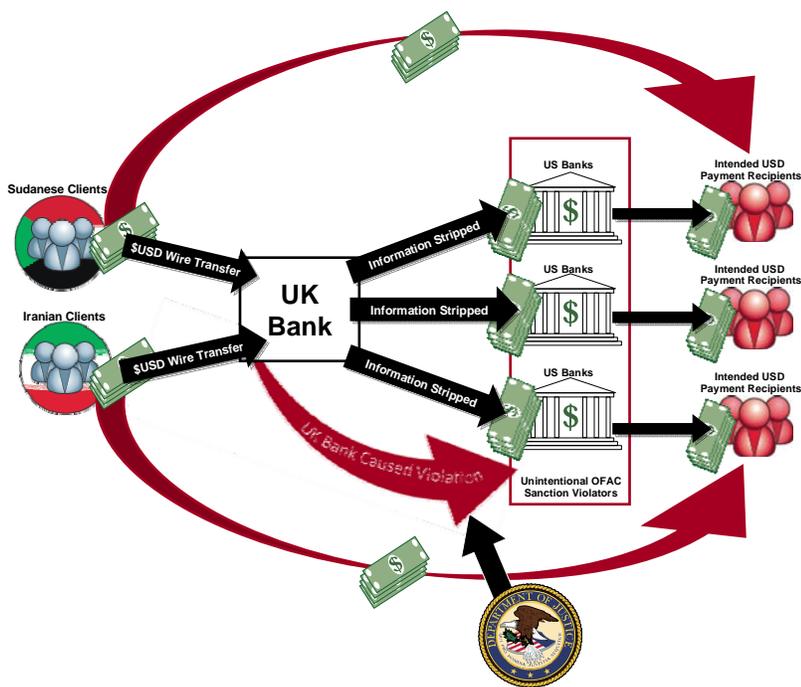
## **VII. THE EXTRATERRITORIAL REACH OF TRADE SANCTIONS: OFAC'S REACH ALSO EXTENDS BEYOND U.S. BORDERS**

Multinational companies should also be aware that trade sanctions administered by the Treasury Department's Office of Foreign Assets Control ("OFAC") are yet another tool in the U.S. government's international arsenal. OFAC implements and administers sanctions programs under the International Emergency Economic Powers Act ("IEEPA"). Many OFAC sanctions are related to particular countries, such as Iran, Sudan and Cuba. Others are targeted at entities and individuals with links to terrorism, drug-trafficking, and nuclear non-proliferation. OFAC sanctions apply to all U.S. persons and entities, wherever located. A 2007 amendment to the IEEPA expanded the application of OFAC sanctions to any person who causes a sanctions violation. Two recent settlements with foreign financial institutions demonstrate that OFAC's reach extends well beyond U.S. entities and persons.

On January 9, 2009, Lloyds TSB Bank plc ("Lloyds"), a U.K. bank headquartered in London, entered into deferred prosecution agreements with the DOJ and the New York County District Attorney's Office related to its role in causing U.S. banks to violate the Sudanese and Iranian Sanctions Regulations. In December 2009, OFAC reached a settlement agreement based on the same conduct. Lloyds agreed to forfeit \$350 million to the U.S. and the state of New York and hire an independent consultant to conduct a five year historical review of payment messages. Under the OFAC settlement agreement, Lloyds agreed to pay \$217 million in civil penalties. This appears to be the first time an enforcement action has been brought against a non-U.S. financial institution for causing OFAC violations in the United States by a non-affiliated U.S. person.

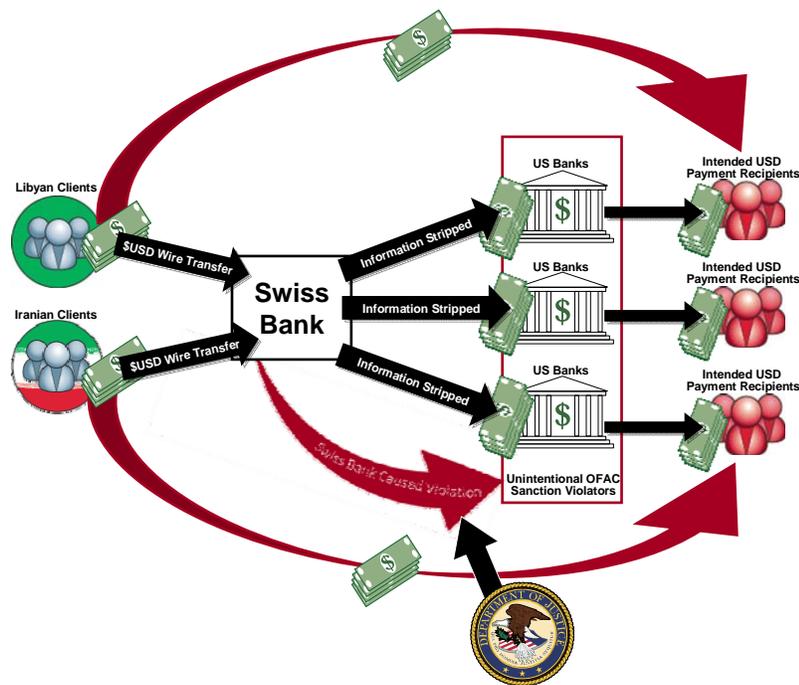
According to the settlement documents, between 1995 and 2007, Lloyds systematically falsified U.S. dollar payment instructions received from Iranian and Sudanese clients. Lloyds

instructed its employees to manually remove data identifying the originator of the payment from the payment message—a process known as “stripping.” As illustrated in the chart below, Lloyds then forwarded the payments to non-affiliated U.S. correspondent banks for processing. Because of Lloyds’ stripping, the U.S. banks were unable to detect that these payments originated in sanctioned countries. Although the 2007 IEEPA amendment extending the application of OFAC sanctions to any person who causes a sanctions violation was not enacted until after the conduct in question occurred, that provision is believed to be the basis for Lloyds’ liability. Thus, U.S. jurisdiction was asserted over a non-U.S. entity for conduct that occurred entirely outside of the U.S. and without participation by the entity’s U.S. affiliates. The chart below illustrates the somewhat tenuous links between Lloyds’ conduct and the U.S.



In December 2009, DOJ and the New York County District Attorney’s Office entered into similar deferred prosecution agreements with Credit Suisse AG (“Credit Suisse”), a Swiss bank, for its role in causing U.S. banks to violate sanctions regulations. Credit Suisse entered

into a civil settlement agreement with OFAC the same day. From as early as 1986 until late 2007, the settlements allege that Credit Suisse systematically falsified thousands of U.S. dollar payment instructions it received from Iranian and Libyan banks before forwarding them on to U.S. banks for processing. Over time, Credit Suisse refined its stripping methods with the goal of evading OFAC filters put in place by the U.S. banks. Credit Suisse allegedly instructed Iranian clients on how to evade the sanctions by distributing pamphlets entitled “How to transfer USD payments.” This chart depicts the alleged practices.



For its role in causing U.S. banks to process payments for Iranian and Libyan clients, Credit Suisse agreed to forfeit \$536 million and hire an independent consultant to conduct an internal investigation of its historical U.S. dollar payments. This case represents the largest forfeiture ever entered into for IEEPA violations. The actions against Credit Suisse and Lloyds demonstrate the extraterritorial reach of OFAC sanctions and show that U.S. trade sanctions can apply to non-U.S. entities that did not directly violate the sanctions themselves. In announcing

the Credit Suisse settlement, Treasury Under Secretary Stuart Levy warned that “banks that do business with Iran expose themselves to the risk of becoming involved in Iran’s proliferation and terrorism activities” and noted that “the overwhelming majority of major banks and an increasing number of other companies are foregoing business with Iran altogether.”

### **VIII. OTHER COUNTRIES ARE GETTING INTO THE MIX: THE NEW UK BRIBERY ACT’S EXPANSIVE COVERAGE CREATES FURTHER RISK FOR MULTINATIONAL COMPANIES**

Fighting corruption is not just a priority for the U.S. Thirty-eight countries have ratified the OECD Anti-Bribery Convention, which entered into force in 1999. By signing onto the Convention, these countries pledged to enact national legislation to criminalize the bribery of foreign government officials. The passage of the UK’s Bribery Act of 2010 reinforced the UK’s commitment to create a comprehensive legal scheme to combat corruption. The Act is even more expansive and comprehensive than the FCPA—and as a result, could increase compliance costs for companies. Although the Bribery Act is not set to take effect until later this year, it is sure to have widespread implications for all companies based in or carrying out business in the UK.

The Act provides for two general types of bribery offenses—bribing and being bribed—as well as the specific offense of bribing a foreign public official. Unlike the FCPA, which only targets bribe-promisers, the UK Bribery Act provides the opportunity to punish both sides of the bribe transaction. The Bribery Act’s core offense of bribing another occurs where a person offers, promises, or gives a financial or other advantage to another person with the intent to induce that person or another to perform improperly a relevant function or activity or to reward improper performance. The offense of being bribed largely mirrors the bribing offense.

“Relevant functions or activities” include, with limited exceptions, anything connected with a

business, trade, or profession, even if entirely in the private sphere. This is a key distinction from the FCPA, which only addresses bribery in the public sector.

Bribing a foreign public official is a specific offense laid out in Section 6, but also can be seen as a species of the general offenses set forth in Sections 1 and 2. In essence, a person is guilty of this offense where the person bribes a foreign public official, if the intention is to influence the official and to obtain or retain business a business advantage. As in the FCPA, a foreign public official is broadly defined to include anyone in any kind of legislative, administrative, or judicial position with the state.

A company may be liable under the new law even if it did not commit any bribery offenses itself. Relevant commercial organizations, defined as UK corporate bodies carrying on business anywhere or as foreign corporate bodies carrying on business in the UK, violate the Act if a person associated with the organization bribes another person with the intent to obtain or retain business or a business advantage. This is the case even if the person associated with the organization has no “close connection” with the UK and the bribery falls outside of the application of the law’s extraterritorial rules. The Act provides for just one defense – that the organization “had in place adequate procedures designed to prevent persons associated with the organization from undertaking [the bribery].” The burden of proving that there were adequate procedures in place, a term not defined by the Act, rests with the commercial organization. Therefore, the Bribery Act effectively criminalizes the failure of any entity based in or carrying out business in the UK to have adequate procedures in place to prevent bribery.

The potential scope of the UK Bribery Act is vast. The Act applies to any behavior that takes place within the UK, regardless of where the company or individual committing the act is based. Even broader, the Act applies to any behavior that takes place outside of the UK if committed by a person or entity with a “close connection” to the UK—including all UK citizens,

residents, and UK entities. In July 2010, the UK Ministry of Justice announced that the implementation of the Bribery Act would be pushed back until April 2011. Earlier this year, Justice Secretary Kenneth Clarke announced that the implementation of the Act may be further delayed. UK companies and all companies and individuals carrying out business in the UK should immediately begin to consider how best to minimize their potential exposure under the Act.

## **IX. CONCLUSION**

Multinational companies and their executives must be aware of these enforcement trends and take steps to minimize their potential exposure. The Bush and Obama administrations have allocated huge amounts of resources to the DOJ, SEC, Treasury Department, and other agencies to crack down on global corruption. U.S. law enforcement agencies are using new and aggressive techniques in white collar investigations. They are also aggressively targeting companies, business executives, and foreign officials around the globe for actions that have very little connection to the U.S. Companies in certain industries, such as the oil and gas and pharmaceutical industries, face even higher risks due to the unique nature of those industries that make them particularly vulnerable to investigations of corruption allegations. The UK Bribery Act is even more expansive than the FCPA and, once implemented, will create further risks for all global companies. Proactive companies will want to assess their risks and implement policies and procedures that position the company to effectively respond to allegations of corruption and, better yet, prevent violations of anti-corruption laws before they occur.