Bloomberg Law Reports® Technology Law

FCPA Enforcement and the Telecom Industry: A Connection You May Have Missed

Z. Scott, Kaye Scholer LLP, and Michael D. Frisch

As companies in the telecommunications industry expand their reach abroad and pursue more opportunities in the developing world, some of those companies have run afoul of the Foreign Corrupt Practices Act ("FCPA"). A review of recent FCPA-related enforcement actions demonstrates that the telecom industry is squarely in the government's crosshairs.

In recent years, while the government regulators in the U.S. Department of Justice and U.S. Securities and Exchange Commission continue to bring corporate and individual cases, they have shifted their FCPA enforcement efforts to focus on entire industries, first targeting oil and gas services companies and medical device makers. Last year, the government announced its intention to target the pharmaceutical industry.[1] But while these industry-wide FCPA enforcement efforts have garnered attention in the press and among compliance professionals, the government's focus on the telecom industry has largely been overlooked. This article provides an overview of FCPA-related enforcement actions against telecom companies, while also providing a brief background on the FCPA. We will address why the FCPA creates a specific risk for the telecom industry and suggest strategies for decreasing that risk through targeted modifications in compliance programs.

An Overview of the FCPA

The FCPA was enacted to prohibit certain classes of persons and entities from making payments to foreign government officials to assist in obtaining or retaining business.[2] The FCPA is a Watergate-era law, passed in the wake of disclosures by over 400 U.S. corporations that they had made illicit payments to foreign government officials. Congress enacted the FCPA to halt bribery overseas and to restore public confidence in the integrity of the American business system. Today, the FCPA plays a large role in the United States' global anti-corruption strategy.

The law has two main parts—anti-bribery provisions and provisions that impose record-keeping and internal control obligations on certain companies. The DOJ and the SEC share responsibility in enforcing the statute.

The anti-bribery provisions of the FCPA make it unlawful for a U.S. person, a company with ties to the United States, and for most foreign companies who are issuers of U.S. securities to make a corrupt payment to a foreign official for the purpose of obtaining or retaining business, or for directing business to any person. Specifically, the law prohibits those under its purview from offering, paying, promising to pay, or authorizing the

payment of money or anything of value to any person, while knowing that all or a portion of such money or thing will be offered, given or promised, directly or indirectly, to a foreign official to influence the foreign official in his or her official capacity, induce the foreign official to do or omit to do an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person. Accordingly, to violate the law, the person offering or authorizing the payment must have a "corrupt intent."[3]

The anti-bribery provisions of the FCPA apply to three categories of persons: "issuers" (companies with U.S. publicly registered securities and those that are required to file reports with the SEC and their employees),[4] "domestic concerns" (U.S. citizens, nationals, and businesses with a principal place of business in the U.S. or that are organized under U.S. law),[5] and any "other person" who takes an act in furtherance of a corrupt payment while within the territory of the United States.[6]

The FCPA also contains provisions that require U.S. issuers to "make and keep books, records, and accounts which, in reasonable detail, accurately and fairly reflect the transactions and disposition of assets."[7] The term "issuer" not only covers publicly traded companies but also covers approximately 1,500 foreign issuers whose American Depository Receipts ("ADRs") are traded on U.S. exchanges. The FCPA also requires that issuers maintain a system of internal accounting controls sufficient to provide reasonable assurances that books are being kept accurately. These provisions essentially codify existing accounting standards.

Violations of the FCPA are subject to serious criminal and civil penalties. Companies are subject to heavy fines—up to $2 million for each violation of the anti-bribery prohibition, up to $25 million for violation of accounting provisions, or up to twice the benefits sought to be obtained and disgorgement of proceeds associated with improper payments. Individuals are subject to heavy fines (up to $250,000 with no indemnification allowed) and prison sentences up to five years for each violation. Companies also may suffer collateral consequences such as damage to reputation and the loss of government contracts or licenses.

Skyrocketing Prosecutions Involving Telecom Companies

While the government's FCPA enforcement efforts have generally trended upwards in recent years, the number of enforcement actions against companies in the telecom industry has skyrocketed.

In the 2002-2008 period, 25 enforcement actions involving telecom companies totaled $1.6 billion in FCPA-related settlements and penalties.[8] Since 2007 alone, the DOJ and the SEC have resolved allegations of FCPA violations or charged companies and individuals in the telecom industry in at least seven separate matters. If the recent past is a prelude, more enforcement actions against telecom companies are sure to come.

The criminal and civil cases brought by the DOJ and the SEC in recent years are striking in their factual similarity. Most involve large payments funneled (either through an intermediary, directly, or as the cost of lavish vacations) to foreign officials responsible for awarding contracts or other benefits from the state-owned telecom company. Telecom companies and their employees have acknowledged bribing government officials seemingly in every corner of the developing world, from Haiti to Nigeria to China to Bangladesh.

It is not surprising that the telecom industry continues to have its share of FCPA-related woes. A number of factors put the industry at risk for FCPA enforcement. First, telecom is big business in the developing world. Telecom is one of the fastest-growing and most profitable sectors in developing countries, where cell phone penetration is lower than in industrialized nations.[9] Second, telecom is a

highly-competitive industry, where multiple firms battle for large-dollar contracts. This highly-competitive environment may serve as an attractive inducement for a sales force to resort to illegal methods in order to gain an advantage over the competition. Third, many telecom companies in emerging markets are completely or partially state-owned, so everyone involved in decision-making is a foreign official within the meaning of the FCPA. Indeed, all these forces combine to make telecom business activity in some foreign markets fraught with peril.

An Overview of FCPA-Related Telecom Enforcement Actions, Or the World of Sham Consultants, Shell Companies, Lavish Travel and Entertainment, and Direct Bribes Paid to Government Officials

Despite the clear prohibitions against corrupt conduct, telecom companies in recent years have run afoul of the FCPA by bribing foreign officials in order to obtain contracts. Here are instructive examples of enforcement actions:

Siemens: Siemens AG ("Siemens") is a huge multinational electronics and electrical engineering company, and is one of the world's largest manufacturers of industrial and consumer products. Siemens formerly manufactured communications networks. Part of the SEC's multifaceted complaint filed in 2008 against Siemens alleged that between 2004 and 2006, Siemens COM (the telecom-related division of the company) paid approximately $5.3 million in bribes to Bangladeshi officials in connection with obtaining a contract to install mobile telephone services. The complaint described payments that were made through sham "business consultants" and directed to high-level officials responsible for telecom contracts, such as the Minister of the Ministry of Posts and Telecommunications in Bangladesh and the Director of Procurement of the Bangladesh Telegraph and Telephone Board.[10] The SEC alleged that senior officials in Siemens' regional company in Bangladesh (including a former CEO and the director of the regional company's COM division) were involved in the scheme. The complaint also alleged that Siemens COM paid at least $4.5 million in bribes in connection with four telecom projects (worth $130 million) with government customers in Nigeria in what was characterized as a practice of paying bribes in Nigeria that was "long-standing and systematic."[11] Some bribes were allegedly routed to Nigerian officials through U.S. bank accounts in the names of the officials' relatives. Other bribes included the purchase of $172,000 worth of watches for Nigerian officials. Siemens settled these and a myriad of other allegations in December 2008, pleading guilty to violating the internal controls and books and records provisions of the FCPA. The settlement resulted in the largest-ever combined fine for resolving an FCPA violation—over $800 million.

ITXC: In December of 2006 and July of 2007, three former executives of ITXC Corporation ("ITXC"), a New Jersey-based VOIP company, pleaded guilty to conspiring to violate the anti-bribery provisions of the FCPA. The executives acknowledged bribing foreign officials through means that included offers to share in the profits generated by the contracts. Two executives received probation and hefty fines, and one was fined and sentenced to 18 months in prison followed by two years of supervised release.[12] In April 2008, the executives settled similar charges brought by the SEC.[13] The executives admitted that between September 1999 and October 2004, they conspired to bribe employees of foreign state-owned telecommunications carriers in Nigeria, Rwanda and Senegal to obtain and retain contracts necessary for ITXC to transmit telephone calls to individuals and businesses in those countries. The executives also disguised the payments as legitimate expenses by creating false business records. The SEC's complaint suggests that ITXC perhaps only turned to corrupt business-generation methods once legitimate methods at obtaining business failed. In 2000, one of the executives hired a former Nitel (Nigerian Telecommunications Limited—the formerly state-

owned Telecom company) official to lobby on his behalf, but the former official only "irritated the current Nitel decision-makers" and the contract was awarded to one of ITXC's competitors. Two years later, the executive hired one of the decision-makers himself, and successfully obtained the sought-after contract.[14] This example shows how the highly-competitive and high-stakes nature of the telecom industry can sometimes lead to corrupt behavior.

Latin Node: In another noteworthy enforcement action, Latin Node, Inc. ("Latin Node"), formerly a provider of telecommunications services using Internet protocol technology, pleaded guilty to violating the anti-bribery provisions of the FCPA and agreed to pay a fine of $2 million over the next three years.[15] The company acknowledged that it made $2 million in payments to third parties knowing that all or part of the money would be passed to officials in Honduran-owned and Yemen-owned telecommunications companies. The corrupt activity came to light only after Latin Node was acquired by a Florida-based public company eLandia International, Inc. According to eLandia's public filings, the cost of terminating Latin Node's management, the FCPA investigation, the likely FCPA fine, and the anticipated loss of customers and vendors as a result of more robust internal controls and legal compliance procedures caused it to allocate $18.2 million of the $22.3 million purchase price as a direct charge to operations for the quarter that ended in June 2007. Although not publicly stated, it is assumed that eLandia relied on the seller's representations rather than conducting its own FCPA due diligence in advance of closing.

The *Siemens* and *IXTC* cases are examples of direct bribes paid to foreign officials in order to obtain telecom contracts. In the next two cases, telecom companies used travel, entertainment and other "things of value" to obtain and retain business from foreign government officials.

Under the FCPA, it is an affirmative defense to the allegations of an anti-bribery violation if the payment or benefit given to a "foreign official" is a *reasonable* and *bona fide* expenditure that is *directly related* to the promotion, demonstration, or explanation of products or services or the execution or performance of a contract. Because the FCPA has no materiality threshold for these expenses, even a modest expenditure could implicate a company in a bribery scheme. Government regulators have not steered away from challenging companies to establish the reasonableness of their expenditures in this area. Specifically, regulators are watching to ensure that these expenses are not just thinly-disguised bribes.

For example, on December 21, 2007, the DOJ and the SEC announced that Lucent Technologies Inc. ("Lucent"), a telecom network systems provider, had agreed to pay a combined $2.5 million in fines to resolve alleged FCPA violations in parallel enforcement actions.[16] From 2000 to 2003, Lucent "spent millions of dollars" on approximately 315 trips to bring Chinese government officials, including the heads of state-owned telecom companies in Beijing and the leaders of provincial telecom subsidiaries, to places such as Disneyland, Universal Studios, the Grand Canyon, Las Vegas, and New York City. Lucent improperly recorded expenses for these trips in its books and records and failed to provide adequate internal controls to monitor the provision of travel and other things of value to Chinese government officials. Specifically, the trips were characterized as "factory inspections" or "training", but actually involved primarily sightseeing, entertainment and leisure. One of the most significant aspects of the scheme was that these violations were approved by high-level executives at the company: the trips were requested by the most senior Lucent Chinese officials and had the approval and assistance of Lucent employees at its U.S. corporate headquarters.[17] While allegations of inappropriate marketing and promotional expenses have been included in past FCPA enforcement actions in recent

years, the Lucent case is an example of FCPA violations based solely on the improper recording of excessive marketing and promotional expenses and related internal control failures. In settlement with the DOJ, Lucent entered into a two-year non-prosecution agreement with the government. The agreement required that the company adopt new, or modify existing, internal controls, policies and procedures. These modified internal controls had to ensure that Lucent makes and keeps fair and accurate books, records and accounts, as well as implement a more robust anti-corruption compliance code, with standards and procedures designed to detect and deter violations of the FCPA and other applicable anti-corruption laws. The company will not face prosecution if it successfully complies with the provisions of the agreement.[18]

The clear compliance lesson here is that government regulators expect global companies to have in place rigorous compliance policies and internal control practices that are capable of both deterring and detecting conduct that crosses over into corruption.

While the prosecution of Lucent was instructive, another U.S. telecom company also ran afoul of the FCPA in much the same way. On December 31, 2009, California-based telecom equipment maker UTStarcom Inc. ("UTStarcom") agreed to pay $3 million in fines for almost exactly the same conduct that was alleged against Lucent just two years earlier.[19] The company was charged with violations of the anti-bribery, books and records, and internal controls provisions of the FCPA arising from its operations in China, Mongolia and Thailand. UTStarcom entered into a non-prosecution agreement with the DOJ and settled a civil action with the SEC to resolve the charges. According to the SEC complaint, between 2002 and 2007, the company spent close to $7 million on 225 post-sale trips that were permitted under the sales contract terms. The trips to destinations including Hawaii, Las Vegas and New York City were purportedly for "training" at UTSI facilities but, in fact, UTSI had no facilities in those locations and conducted no training. UTS-China falsely recorded these trips as "training" expenses, while the true purpose for providing these trips was to obtain and retain lucrative telecom contracts. The complaint also stated that on at least seven occasions from 2002 to 2004, the company paid more than $4 million for foreign government employees to attend sponsored executive training programs. UTStarcom's conduct went beyond travel and entertainment. The company also on at least ten occasions offered or provided full-time employment to employees of government customers or their family members. Further, the company funneled money directly to "sham consultants" in China and Mongolia while "knowing that they would pay bribes to foreign government officials."[20] Again, this conduct was sanctioned at the highest levels of the company—the management of UTStarcom's China subsidiary directly approved the trips.[21]

In agreeing to enter into a non-prosecution agreement with the company, the DOJ explained that the agreement was appropriate because of the company's "voluntary disclosure, thorough self-investigation of the underlying conduct, the cooperation provided by the company to the Department, and the remedial efforts undertaken by the company."[22] In the agreement, the company acknowledged that it "was standard practice to include as part of its systems contract a provision for UTS-China to pay for some of the government controlled . . . employees to attend purported training overseas."[23] Between 1995 and 2004, more than 75% of UTStarcom's sales were to publicly-owned telecom companies in China.[24]

Most recently, on June 29, 2010, the SEC announced that Veraz Networks, Inc., a San Jose, California-based VOiP company, paid $300,000 to settle charges brought by the SEC that it violated the books and records and internal controls provisions of the FCPA by making illegal payments to foreign officials in China and Vietnam.[25] According to the SEC's complaint, Veraz engaged a consultant in

China who in 2007 and 2008 gave gifts and offered improper payments, valued together at approximately $40,000, to officials at an unidentified government-controlled telecommunications company in China in an attempt to win business for Veraz.[26] A Veraz supervisor who approved the gifts described them in an internal Veraz email as the "gift scheme." The complaint alleged that Veraz had submitted a higher bid than other firms but still received the contract. The company canceled the sale after discovering the bribes, according to the complaint. The complaint also alleged that in 2007 and 2008, another Veraz employee made improper payments to the CEO of a government-controlled telecommunications company in Vietnam to win business for Veraz, including flowers sent to the wife of that company's CEO.

Veraz's settlement with the SEC only came after a long and expensive process of investigation and voluntary disclosure. Veraz reported in November 2009 that it had spent $2.5 million to that point to investigate and handle the FCPA compliance issues.

Telecom Companies and FCPA Compliance

Compliance Programs and Policies

Telecom companies can take away some key lessons from these enforcement actions. In general, these actions show that operating in countries where the risk of corruption is high requires that companies proactively put in place compliance policies that are designed to educate employees (including executives at the highest levels of the company) as well as third parties who will act on their behalf. These polices should be backstopped by internal controls that serve to detect corrupt conduct when policies have failed. In the UTStarcom non-prosecution agreement, the government set forth its requirements, and therefore guidance to others, for FCPA compliance policies and practices:

1. A clearly articulated corporate policy against violations of the FCPA, including anti-bribery, books and records, and internal controls provisions, and other applicable counterparts.
2. Promulgation of compliance standards and procedures designed to reduce the prospect of violations of the anti-corruption laws and the company's compliance code. These standards should apply to all directors, officers, and employees and, where necessary and appropriate, outside parties acting on behalf of the company in a foreign jurisdiction.
3. The assignment of responsibility to one or more senior corporate officials for the implementation and oversight of compliance with policies, standards, and procedures regarding the anti-corruption laws. Such corporate official(s) should have the authority to report directly to the board of directors or committee thereof.
4. Mechanisms designed to ensure that the policies, standards, and procedures of the company regarding the anti-corruption laws are effectively communicated, including (a) periodic training and (b) annual certifications certifying compliance with the training requirements.
5. An effective system for reporting suspected criminal conduct and/or violations of the compliance policies, standards, and procedures regarding the anti-corruption laws.
6. Appropriate disciplinary procedures to address violations of the anti-corruption laws and the company's compliance code.
7. Appropriate due diligence requirements pertaining to the retention and oversight of agents and business partners.

8. Standard provisions in agreements, contracts, and renewals thereof with all agents and business partners that are reasonably calculated to prevent violations of the anti-corruption laws and
9. Periodic testing of the compliance code, standards, and procedures designed to evaluate their effectiveness in detecting and reducing violations of anti-corruption laws and the company's compliance code.

In addition, the compliance policies should address entertainment and promotional expenditures. As the Lucent and UTStarcom cases demonstrate, there is a line between what is a *bona fide* promotional expense and what is a bribe. Although the term "anything of value" is not defined in the FCPA, it is very clear that the regulators view the facts and circumstances underlying these cases as falling within the scope of corrupt behavior.

Responding to Allegations of FCPA Violations

Government regulators expect that when a company detects a violation of the law within its operations, it will take steps to investigate and, if appropriate, remediate the issues. How far a company must go to investigate and what resources are necessary for the undertaking depends on the scope of the FCPA investigation. The government expects that a company will follow the leads developed in an independent internal investigation typically managed by its audit committee or special committee of the board of directors. These leads may necessitate an investigation that begins in one foreign country to conclude with multiple inquiries across the globe where the company has operations. An internal investigation can be expensive and it is by its nature time-consuming.

There may come a time in an investigation when a company concludes that there is sufficient evidence of corrupt conduct that requires consideration of disclosure to government regulators. In evaluating whether to self-disclose, public companies also have to consider the requirements of Sarbanes-Oxley. In some instances, FCPA-related investigations are first revealed in the public filings of publicly traded companies. Also, in at least one instance, a private company that is required to file periodic reports with the SEC filed a Form 8-K revealing the existence of an FCPA investigation.[27] Both DOJ and SEC officials have made public statements encouraging companies to come forward and cooperate. For example, in a recent speech, Assistant Attorney General Lanny Breuer stated:

> I also want to assure you that the Department's commitment to meaningfully reward voluntary disclosures and full and complete corporate cooperation will continue to be honored in both letter and spirit. I know that many of you often grapple with the difficult question of whether to advise your client to make a voluntary disclosure. I strongly urge any corporation that discovers an FCPA violation—or any other criminal violation, for that matter—to seriously consider making a voluntary disclosure and to cooperate with the Department. The Sentencing Guidelines and the Principles of Federal Prosecution of Business Organizations obviously encourage such conduct, and your clients will receive meaningful credit for that disclosure and cooperation.[28]

Dispositions in many foreign bribery cases, including those from the telecom industry, show that the benefits of voluntary disclosure are real. These benefits can be seen in well-crafted dispositions and settlements for companies that have acknowledged long-standing corrupt behavior in their dealings with foreign government officials. The example that is most instructive arises from the disposition of a case involving the criminal prosecution in *United*

States v. Latin Node. There, the government credited successor corporation eLandia with full cooperation, noting that the company produced thousands of non-privileged documents, voluntarily strengthened its own compliance program and, most importantly, ceased doing business relating to the tainted contracts at a cost of millions of dollars. Through its prompt, extensive, and authentic cooperation with the government, eLandia avoided all criminal charges and organizational probation, and its newly acquired asset, Latin Node, received a fine of only $2 million—less than half of the guideline-recommended range.

Conclusion

The writing is on the wall: The slew of recent FCPA enforcement actions shows that regulators are focused on rooting out bribery in the global telecommunications industry. As telecommunications companies expand their reach abroad, they must take care that their compliance programs and policies are well-tailored to mitigate the serious risks of operating in the industry. And when problems arise, recent examples show that telecom companies benefit when they move quickly to investigate the allegations, and if appropriate, cooperate fully with the government in addressing them.

Z. Scott is a Partner in the Chicago office of Kaye Scholer LLP and a member of the firm's Complex Commercial Litigation and White Collar Litigation and Internal Investigations practices. Ms. Scott, a former federal prosecutor and seasoned trial lawyer, focuses her practice on complex commercial litigation, global and domestic internal investigations and corporate compliance counseling.

Michael D. Frisch is a graduate of Northwestern University and Northwestern Law School. Until recently, Michael was an associate in the litigation department of Mayer Brown LLP.

---

[1] *See* November 12, 2009 Keynote Address of Lanny A. Breuer to the Tenth Annual Pharmaceutical Regulatory and Compliance Congress and Best Practices Forum, *available at* http://www.justice.gov/criminal/pr/speeches-testimony/documents/11-12-09breuer-pharmaspeech.pdf.

[2] *See* 15 U.S.C. §§ 78dd-1, et seq.

[3] *See, e.g., U.S. v. Kay*, 513 F.3d 461 (5th Cir. 2008).

[4] *See* 15 U.S.C. § 78dd-1(a).

[5] *See* 15 U.S.C. § 78dd-2(h)(1).

[6] *See* 15 U.S.C. § 78dd-3(a).

[7] 15 U.S.C. § 78m(b)(2).

[8] Pricewaterhouse Coopers Report, *Corruption Crackdown: How the FCPA is Changing the Way the World Does Business*, July 27, 2009, *available at* http://pwccn.com/webmedia/doc/633862908465493306_forensic_fcpa_corrupt_aug2009.pdf.

[9] *See, e.g.*, Heather Timmons and Kevin J. O'Brien, *Third World Moves to the Front*, THE NEW YORK TIMES, May 27, 2008, available at http://www.nytimes.com/2008/05/27/business/worldbusiness/27telecom.html.

[10] *See* SEC Complaint, *U.S. Securities and Exchange Commission v. Siemens Aktiengesellschaft*, No. 1:08-cv-02167, ¶¶ 47-48 (filed D.D.C. Dec. 12, 2008).

[11] *Id*.

[12] *See Former ITXC Corporation Executives Sentences for Roles in Foreign Bribery Scheme*, DOJ Press Release No. 08-766, dated 9/2/2008, *available at* http://www.justice.gov/opa/pr/2008/September/08-crm-766.html.

[13] See Former Executives of ITXC Corp. Settle Foreign Bribery Charges, SEC Litigation Release No. 20556.

[14] SEC Complaint, *U.S. Securities and Exchange Commission v. Steven J. Ott and Roger Michael Young*, No. 06-4195, ¶¶ 16-17 (filed D.N.J. Sept. 6, 2006).

[15] *See Latin Node Inc., Pleads Guilty to Foreign Corrupt Practices Act Violation and Agrees to Pay $2 Million Criminal Fine*, DOJ Press Release No. 09-318, dated 4/7/2009, *available at* http://www.justice.gov/opa/pr/2009/April/09-crm-318.html.

[16] *See Lucent Technologies Inc. Agrees to Pay $1 Million Fine to Resolve FCPA Allegations*, DOJ Press Release No. 07-1028, dated 12/21/2007, *available at* http://www.justice.gov/opa/pr/2007/December/07_crm_1028.html.

[17] Less than a year later, Alcatel-Lucent again found itself in FCPA-related trouble. On September 23,

2008, a former assistant V.P. for the Latin American region was sentenced to 30 months in prison for paying more than $2.5 in bribe money to a board director for the state-run telecom authority in order to obtain a $149 million telecom contract. *See Former Alcatel CIT Executive Sentenced for Paying $2.5 Million in Bribes to Senior Costa Rican Officials*, DOJ Press Release No. 08-848, dated 9/23/2008, *available at* http://www.justice.gov/opa/pr/2008/September/08-crm-848.html.

[18] As disclosed in public filings, Alcatel-Lucent acknowledged that it has engaged in settlement discussions with the DOJ and the SEC with regard to an ongoing FCPA investigation. Alcatel, once a primarily French company, merged with Lucent in late 2006. Below is an excerpt from the company's Form 20-F for the period ending December 31, 2009.These discussions have resulted in December 2009 in agreements in principle with the staffs of each of the agencies. There can be no assurances, however, that final agreements will be reached with the agencies or accepted in court. If finalized, the agreements would relate to alleged violations of the FCPA involving several countries, including Costa Rica, Taiwan, and Kenya. Under the agreement in principle with the SEC, Alcatel-Lucent would enter into a consent decree under which Alcatel-Lucent would neither admit nor deny violations of the antibribery, internal controls and books and records provisions of the FCPA and would be enjoined from future violations of U.S. securities laws, pay U.S.$45.4 million in disgorgement of profits and prejudgment interest and agree to a three-year French anticorruption compliance monitor to evaluate in accordance with the provisions of the consent decree (unless any specific provision therein is expressly determined by the French Ministry of Justice to violate French law) the effectiveness of Alcatel-Lucen's internal controls, record-keeping and financial reporting policies and procedures. Under the agreement in principle with the DOJ, Alcatel-Lucent would enter into a three-year deferred prosecution agreement (DPA), charging Alcatel-Lucent with violations of the internal controls and books and records provisions of the FCPA, and Alcatel-Lucent would pay a total criminal fine of U.S. $92 million—payable in four installments over the course of three years. In addition, three Alcatel-Lucent subsidiaries—Alcatel Lucent France, Alcatel-Lucent Trade and Alcatel Centroamerica—would each plead guilty to violations of the FCPA's antibribery, books and records and internal accounting controls provisions. The agreement with the DOJ would also contain provisions relating to a three-year French anticorruption compliance monitor. If Alcatel-Lucent fully complies with the terms of the DPA, the DOJ would dismiss the charges upon conclusion of the three-year term.

[19] *See UTStarcom Inc. Agrees to Pay $1.5 Million Penalty for Acts of Foreign Bribery in China*, DOJ Press Release No. 09-1390, dated 12/31/2009 ("UTStarcom DOJ Press Release"), *available at* http://www.justice.gov/opa/pr/2009/December/09-crm-1390.html; Non Prosecution Agreement dated 12/31/2009 ("UTStarcom NPA"), *available at* http://www.justice.gov/criminal/fraud/fcpa/cases/docs/12-31-09utstarcom-agree.pdf.

[20] *SEC Charges California Telecom Company with Bribery and Other FCPA Violations*, SEC Press Release No. 2009-277, dated 12/31/2009.

[21] *See* UTStarcom DOJ Press Release, *supra* n.19.

[22] UTStarcom NPA, *supra* n.19.

[23] UTStarcom NPA, *supra* n.19.

[24] *See* SEC Complaint, *U.S. Securities and Exchange Commission v. UTStarcom, Inc.*, No. 09-cv-06094 (N.D. Cal. Dec. 31, 2009) at ¶¶ 9-10.

[25] *See SEC Charges California Telecommunications Company with FCPA Violations*, SEC Litigation Release No. 21581, dated June 29, 2010.

[26] Id.

[27] *See* PBSJ Corporation Form 8-K, dated 12/30/2009.

[28] *Remarks by Lanny A. Breuer, Assistant Attorney General for the Criminal Division At the American Bar Association National Institute on White Collar Crime*, Feb. 25, 2010, *available at* http://www.justice.gov/criminal/pr/speeches-testimony/2010/02-25-10aag-AmericanBarAssosiation.pdf.