Bloomberg BNA

White Collar Crime Report™

BRIBERY

Telecommunications Industry in Government's FCPA Crosshairs




BY RALPH J. CACCIA, SCOTT D. DELACOURT, GREGORY M. WILLIAMS AND P. NICHOLAS PETERSON

Anyone operating in the telecommunications industry should be well aware of the number of enforcement actions brought during the past several years by the Department of Justice and Securities and Exchange Commission involving Foreign Corrupt Practices Act[1] violations.

What is somewhat startling, however, is that of the scores of industries that have been investigated, it is the matters involving the telecommunications sector that seem to implicate every FCPA issue of the moment—from the rising prosecution of individuals to the interpretation of the term ''foreign official'' to liability based on improper payments to third parties.

A Sector at Risk

The sector is particularly at risk for FCPA enforcement actions because telecommunications companies often compete for foreign government contracts and many of the international carriers and equipment manufacturers with which they do business are either partially or wholly state-owned. The concern is not purely hypothetical. As detailed below, the DOJ and the SEC have brought numerous enforcement actions in the telecommunications arena.

The DOJ and SEC, moreover, have been very aggressive with respect to virtually every aspect of those enforcement actions. The government asserts jurisdiction with respect to conduct or actors with minimal contacts to the U.S. It interprets the FCPA to prohibit improper payments not only to officials within traditional government ministries and departments, but to the employees of state-owned or controlled, but otherwise commercial, entities. Further, the DOJ and SEC regard not simply the payment of cash, but also the provision of benefits such as allegedly excessive entertainment or travel expenses, to run afoul of the law. Payments made by agents and other third-party intermediaries are an area of particular concern, as under certain circumstances such payments may be attributed to the telecommunications company.

It is imperative that telecommunications companies implement a well-tailored compliance program, including appropriate due diligence on its agents and business partners, to mitigate the substantial FCPA exposure the industry faces.

FCPA: Recent Enforcement Trends

In November 2012, the DOJ and SEC released a long-awaited FCPA Resource Guide,[2] which compiles and

[1] 15 U.S.C. § 78dd-1, et seq.

[2] *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, DOJ Criminal Division and SEC Enforcement Divsion. See also *Questions Remain over Main FCPA Issues Following Release of Guidance From DOJ, SEC*, 07 WCR 871 (11/16/12),

clarifies important insights relating to the agencies' approach to FCPA enforcement. The guide currently provides the best source of official, published guidance on FCPA enforcement. Unlike other major areas of enforcement, there is dearth of guidance from the courts on even the most basic elements of the FCPA, as there have been very few FCPA cases which have gone to trial. It is, at best, unsettling that the DOJ and the SEC—the agencies responsible for enforcement of the law—are currently the primary interpreters of the statute. Consequently, when navigating risk and assessing compliance priorities, all companies, particularly those in industries like telecommunications that have seen significant enforcement activity, must carefully review this guidance and keep apprised of current enforcement actions and trends.

Focus on Prosecuting Corporate Executives. Virtually every recent article or discussion on the FCPA notes that the statute's enforcement continues to be a major DOJ and SEC prosecutorial priority. In June 2013, then-Acting Assistant Attorney General Mythili Raman stated that fighting global corruption is, and always will be, a core priority of the DOJ.[3] In particular, the intent to focus on prosecuting corporate executives who are ultimately responsible for conduct giving rise to an FCPA violation has been a consistent DOJ refrain. As Raman made clear:

> Our recent string of successful prosecutions of corporate executives is worth highlighting. Those actions show, in concrete terms, that we are not going away—indeed, our efforts to fight foreign bribery are more robust than ever. By redoubling our commitment to bring to justice those individuals who bribe for business, we are sending an unmistakable message to corporate executives around the world—if you engage in corrupt conduct, you should be prepared to face very real consequences, including jail time.[4]

Companies within the telecommunications industry are especially vulnerable, in part because foreign governments often have a prominent role in controlling crucial aspects of telecommunications in their countries. Due to the inherent intermingling of business and government in this arena, there are many occasions for telecommunications companies to run afoul of the FCPA.

Several recent settlements and convictions evince the costs associated with FCPA violations for telecommunications companies and their executives. In December 2010, Alcatel-Lucent paid $92 million to settle FCPA criminal charges and disgorged $45 million to the SEC.[5] In addition, Christian Sapsizian, a former Alcatel executive, pleaded guilty and was sentenced to 30 months in prison in connection with the case.

Two former executives of Miami-based Terra Telecommunications Corp., Joel Esquenazi and Carlos Rodriguez, were sentenced in October 2011 to 15 and seven years in prison, respectively, and ordered to forfeit over $3 million and pay $2.2 million in restitution.[6] Esquenazi's 15-year sentence still constitutes the longest sentence ever imposed in an FCPA case.

More recently, in December 2011, German telecommunications company Deutsche Telekom AG and its Hungarian subsidiary, Magyar Telekom Plc., paid $95 million to resolve criminal and civil FCPA charges.[7] The SEC also filed a complaint against three executives of Magyar Telekom.[8]

As these severe penalties demonstrate, U.S.-based telecommunications companies operating abroad—particularly those with customers in the public sector—and their executives are exposed to significant FCPA-related risks. Non-U.S. telecommunications companies with operations or other links to the U.S. face a similar risk. Failing to mitigate such risks in a hostile enforcement environment through the implementation of an effective corporate compliance program simply cannot be justified to stockholders, customers or, most of all, law enforcement agencies.

Who Are Covered Individuals and Entities?

The FCPA's anti-bribery provisions apply to three categories of individuals and entities:

(1) ''issuers'' and their officers, directors, employees, agents and shareholders;

(2) ''domestic concerns'' and their officers, directors, employees, agents and shareholders; and

(3) other persons and entities acting while in the territory of the U.S.[9]

An ''issuer'' is a corporation, foreign or domestic, that has issued securities registered in the U.S. or who is required to file periodic reports with the SEC.[10] A ''domestic concern'' is any individual who is a citizen, national or resident of the U.S., or any corporation or other business entity with its principal place of business in the U.S., or that is organized under the laws of the U.S.[11]

''Issuers'' and ''domestic concerns'' can be held liable under the anti-bribery provisions even if the relevant conduct occurs entirely outside the U.S. Thus, if the ''issuer'' or ''domestic concern'' is a U.S. company, it can be held liable regardless of where the allegedly prohibited conduct occurred. Similarly, non-U.S. companies may be held liable for allegedly prohibited conduct if they use the U.S. mail or any means or instrumentalities of interstate commerce.[12] The government has interpreted interstate commerce broadly to include telephone calls, e-mails, text messages, facsimiles, wire transfers and interstate or international travel.[13]

Broad Interpretation of Interstate Commerce. The government's broad interpretation of interstate commerce was hammered home in allegations brought against

and *FCPA: What the DOJ and SEC's Long-Awaited Guidance Means for Business*, Wiley Rein (Dec. 2012), available at http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=8&id=8500.

[3] 08 WCR 462 (6/28/13).

[4] Raman's keynote address at the Global Anti-Corruption Congress (June 17, 2012), available at http://www.justice.gov/criminal/pr/speeches/2013/crm-speech-130617.html.

[5] 05 WCR 925 (12/31/10). *United States v. Alcatel-Lucent SA*, No. 1:10-cr-20907 (S.D. Fla. Dec. 27, 2010).

[6] 06 WCR 927 (11/4/11). *United States v. Esquenazi*, No. 1:09-cr-21010 (S.D.Fla. Oct. 25, 2011).

[7] 07 WCR 8 (1/13/12). *United States v. Magyar Telekom Plc*, No. 1:11-cr-00597 (E.D. Va. Dec. 29, 2011).

[8] *SEC v. Straub*, No. 11-cv-09645 (S.D.N.Y.).

[9] 15 U.S.C. §§ 78dd-1, 78dd-2 and 78dd-3.

[10] 15 U.S.C. § 78c(a)(8).

[11] 15 U.S.C. § 78dd-2(h).

[12] 15 U.S.C. §§ 78dd-1(a), 78dd-2(a).

[13] See FCPA resource guide at 11, supra n. 2.

  WCR ISSN 1559-3185

Deutsche Telekom.[14] The DOJ charged that a subsidiary of Deutsche Telekom, Hungarian telecommunications company Magyar Telekom, had bribed Macedonian officials to delay the licensing of a competitor and provide other regulatory benefits. As Deutsche Telekom was a foreign ''issuer'' under the FCPA, the government claimed FCPA jurisdiction simply by virtue of the fact that e-mails regarding the conduct were transmitted through servers located in the U.S.—even though none of the senders or recipients were located in the U.S.

What Conduct Implicates FCPA?

What Constitutes a Payment? The FCPA prohibits the corrupt ''offer, payment, promise to pay, or authorization of the giving of anything of value'' to a foreign official to obtain or retain business. While cash is the most obvious form of payment, gifts, travel and entertainment may also constitute things ''of value.'' For example, in a 2009 case against UTStarcom Inc., a California-based telecommunications company, the SEC alleged that UTStarcom paid for more than 225 ''training'' trips for employees of Chinese government-owned telecommunications companies.[15] These trips were to locations such as Hawaii, Las Vegas and New York, and primarily involved sightseeing, not training.

In a similar case in 2007, the government alleged that New Jersey-based telecommunications company Lucent Technologies Inc. provided approximately 315 such ''training'' trips to Chinese officials.[16] As with the UTStarcom trips, the Lucent Technologies-sponsored trips were found to be primarily for entertainment and sightseeing purposes.

Notably, the FCPA does not have a minimum value threshold. Thus, gifts or entertainment of any value could potentially constitute a prohibited payment. In practice, the government has recognized that gifts of minimal value would probably not trigger an FCPA violation, as such items ''are unlikely to improperly influence an official.''[17] However, the government has based some FCPA prosecutions, at least in part, on a series of relatively small payments or gifts.[18]

Who is a Foreign Official? The FCPA covers corrupt payments to foreign officials, foreign political parties or party officials, candidates for foreign political office, and officials of public international organizations.[19] The FCPA defines a ''foreign official'' as ''any officer or employee of a foreign government or any department, agency, or instrumentality thereof or of a public international organization or any person acting in an official capacity for or on behalf of'' such governments or organizations.[20] Thus, the FCPA covers high-ranking officials, as well as low-level employees. Indeed, ''foreign official'' is interpreted so broadly that determining who qualifies as a foreign official can be less than clear. Such determinations may turn on whether the person works for or is employed by an ''instrumentality'' of a government.

The DOJ and the SEC have maintained that state-owned or state-controlled entities are considered ''instrumentalities'' of the government and that their employees can fall within the FCPA's definition of ''foreign official.''[21] The FCPA resource guide lists a series of factors that provide guidance on when the agencies would view an entity to be an instrumentality of a foreign government.[22]

These factors include the:

- extent of government ownership,
- degree of the government's control over the entity,
- government's characterization of the entity,
- circumstances surrounding the entity's creation, and
- level of financial support the entity receives from the government.

In the Lucent Technologies and UTStarcom cases described above, the government interpreted the term ''foreign official'' to include employees of telecommunications companies owned by the Chinese government.[23]

Similarly, the DOJ alleged in 2011 that Comverse Technology Inc. violated the FCPA when its subsidiary made cash payments to employees of the Hellenic Telecommunications Organization, which is partially owned by the Greek government.[24]

This issue may receive clarification when the U.S. Court of Appeals for the Eleventh Circuit decides *United States v. Esquenazi*[25]. Oral argument was heard in the case in October.

The defendants—the aforementioned terra Communication executives Esquenazi and Rodriguez—contend in part that payments made to individuals at Haiti Teleco, the country's state-owned national telecommunications company, did not constitute bribes to ''foreign officials'' because the telecom is not a government instrumentality. Esquenazi and Rodriguez argue that Haiti Teleco does not perform any governmental functions and that the FCPA's failure to define ''instrumentality'' renders it unconstitutionally vague.

What 'Indirect' Payments Are Prohibited? The FCPA also prohibits payments that are not made directly by the company or individual subject to the FCPA to a ''for-

[14] See Magyar Telekom, supra n. 7.

[15] 05 WCR 41 (1/15/10). *SEC v. UTStarcom, Inc.*, No. 09-cv-6094 (N.D. Cal. Dec. 31, 2009).

[16] 03 WCR 22 (1/4/08). *SEC v. Lucent Technologies Inc.*, No. 07-cv-2301 (D.D.C. 2007).

[17] See FCPA resource guide at 15, supra n. 2.

[18] See, e.g., *SEC v. Avery Dennison Corp.*, No. 2:09-cv-5493 (C.D. Cal. 2009) (government alleged that defendant paid a bribe of approximately $25,000 and hosted sightseeing trips); *SEC v. Dow Chemical Co.*, No. 07-cv-336 (D.D.C. 2007) (government alleged that defendant paid approximately $87,000 to agricultural inspectors, in addition to payments made to other Indian officials); *United States v. Paradigm BV*, 02 WCR 569 (9/28/07) (government alleged that defendant paid between $330,000 and $430,000 in bribes throughout the world over a five-year period).

[19] 15 U.S.C. §§ 78dd-1(a) (1)-(3), 78dd-2(a)(1)-(3), and 78dd-3(a)(1)-(3).

[20] 15 U.S.C. § 78dd-2(h)(2)(A).

[21] See FCPA resource guide at 29, n. 2.

[22] Id. at 20.

[23] See *Lucent Technologies Inc.*, supra n. 16; *UTStarcom Inc.*, supra n. 15.

[24] 06 WCR 332 (4/22/11). See also DOJ press release, *Comverse Technology Inc. Agrees to Pay $1.2 Million Penalty to Resolve Violations of the Foreign Corrupt Practices Act* (April 7, 2011), available at http://www.justice.gov/opa/pr/2011/April/11-crm-438.html.

[25] No. 11–15331 (11th Cir.). See also 07 WCR 489 (6/15/12)

eign official'' but through a third party or intermediary. Specifically, the FCPA covers payments made to ''any person, while knowing that all or a portion of such money or thing of value will be offered, given, or promised, directly or indirectly,'' to a foreign official.[26]

A very common FCPA fact pattern involves a company hiring a local individual or company to help navigate the nuances of conducting business in a foreign location. That third party then pays a government official or instrumentality a bribe to secure that company business opportunities, with or without the company's direct knowledge. The government interprets the above ''knowing'' standard to encompass not only actual knowledge, but also a conscious disregard for the truth (i.e., ''willful blindness''), including situations in which a company ignores ''red flags.''[27] Accordingly, a company may be liable when its agents or other business partners are paying bribes even if the company has no actual knowledge that these payments are occurring, at least in the absence of an effective compliance program and an appropriate level of due diligence. Indeed, the majority of FCPA enforcement actions, including the Alcatel-Lucent and Magyar Telekom matters discussed above, feature payments made by third parties.

Similarly, a number of cases involve payments to relatives of foreign government officials. If such payments are considered things of value to the foreign official, the payment can constitute a violation of the FCPA. Such a scenario occurred in the Lucent Technologies case described above, as the SEC alleged that Lucent paid or offered to pay for education opportunities for the relatives of Chinese officials.[28]

A more recent example involves JPMorgan Chase & Co., which is currently under FCPA investigation for allegedly hiring the relatives of top Chinese officials in order to win underwriting and other work.

When Does Payment Retain or Obtain Business? An FCPA violation occurs only when a corrupt payment is made to a foreign official for the purpose of retaining or obtaining business. This is known as the ''business purpose test'' and, again, is broadly interpreted by the government enforcement agencies.[29] As the name implies, this element focuses on the purpose of the payment offered or made to the foreign official. Common examples of ''business purposes'' include payments to:

- win a contract,
- influence a procurement process,
- circumvent the rules for importation of products,
- gain access to non-public bid tender information,
- evade taxes or penalties,
- influence the adjudication of lawsuits or enforcement actions,
- obtain exceptions to regulation, and
- avoid contract termination.[30]

In the telecommunications context, the government has considered a variety of actions to satisfy the business purposes test.

For example, in a 2011 FCPA investigation into Cinergy Telecommunications, the DOJ claimed that payments to Haitian officials to obtain preferred telecommunications rates and credits, among other objectives, were for the purpose of obtaining or retaining business.[31] Similarly, in the Alcatel-Lucent case, the SEC claimed that the defendant paid officials in Costa Rica, Honduras, Taiwan and Malaysia to obtain or retain contracts to provide telephone services in those respective countries.[32] Additionally, in the UTStarcom case, the SEC alleged that UTStarcom bribed Mongolian officials to help it obtain a favorable ruling in a license dispute.[33]

In sum, a variety of actions, especially in a heavily regulated industry like telecommunications, can be interpreted as being made for the purpose of obtaining or retaining business.

How to Avoid a Violation, And Why a Compliance Program Makes Good Business Sense

The single best way of mitigating risk in the FCPA arena, including for telecommunications companies, is to develop an effective corporate compliance program. With regard to the need for compliance and how to appropriately tailor a compliance program, there is plenty to be learned from the experiences of companies that have been forced to enter FCPA settlements with the government. Frequently, these settlements have come in the form of a deferred prosecution agreement. While these agreements are carefully tailored to address the specific conduct that was the subject of the violation, there are some generally applicable lessons that can be drawn from them.

First, involvement of executive and senior management in the compliance program is critical. As stated in the FCPA resource guide, ''[w]ithin a business organization, compliance begins with the board of directors and senior executives setting the proper tone for the rest of the company.''[34] Many DPAs also require that senior management must provide explicit and visible support for compliance with anti-corruption laws. This involvement extends to direct oversight of the compliance program. For instance, Magyar Telekom's DPA required a group compliance officer to be responsible for implementing and overseeing the compliance program and reporting directly to an autonomous audit committee.[35]

In Alcatel-Lucent's DPA, responsibility for its compliance program was assigned to ''one or more senior corporate executives'' who are to have direct reporting obligations to ''independent monitoring bodies'' or any appropriate committee of the board of directors.[36]

Second, an effective compliance program should have an internal process for reporting violations. Both

[26] U.S.C. §§ 78dd-1(a)(3), 78dd-2(a)(3), and 78dd-3(a)(3).
[27] See FCPA resource guide at 21-22, supra n. 2.
[28] See *Lucent Technologies Inc.*, supra n. 16.
[29] See FCPA resource guide at 12, supra n. 2.
[30] Id.
[31] See *United States v. Cruz*, No. 1:09-cr-21010 (S.D. Fla. 2011).
[32] See *SEC v. Alcatel-Lucent, S.A.*, No. 10-cv-24620 (S.D. Fla. 2010).
[33] See *UTStarcom Inc.*, supra n. 15.
[34] resource guide at 57, supra n. 2.
[35] Magyar DPA, available at http://pub.bna.com/cl/MagyarDPA.pdf
[36] *United States v. Alcatel-Lucent SA*, No. 1:10-cr-20907, DPA (S.D.Fla. Dec. 20, 2010).

  WCR ISSN 1559-3185

Magyar Telekom's and Alcatel-Lucent's DPAs specifically provide that an internal, and preferably confidential, reporting system be installed for directors, officers, employees, and even agents and business partners. Further, the internal process should protect those reporting suspected violations from retaliation.

Third, prior to acquiring new business entities or completing a merger, a company should perform a thorough FCPA and anti-corruption due diligence review on the intended target. Upon acquisition, the compliance program should be applied to the new entity as quickly as possible. In the Magyar Telekom DPA, Magyar Telekom was required not only to train personnel from newly acquired entities as soon as practicable, but also to conduct an anti-corruption specific audit of the new entity.

Fourth, as the UTStarcom nonprosecution agreement sets forth, a compliance program should involve an appropriate level of third-party due diligence.[37] The range of such due diligence can vary widely from the basic, such as know your customer/partner questionnaires and specially designated nationals screening, to the robust, including due diligence reports prepared by qualified outside counsel. The government has shed little light on what degree of review is ''appropriate,'' and if not handled correctly, such measures can become quite costly.

Targeting Compliance Resources. To balance appropriately the competing concerns of potential liability and expense, a telecommunications company should perform a risk-based analysis identifying the third-party relationships that represent the most significant exposure based on such factors as the level of corruption in the country or region in question; the nature of the business transaction and level of interaction the third party has with ''foreign officials'' (including employees of state-owned entities); the type of third party (e.g., sales agent or joint venture partner) and compensation structure; and possible business and personal connections between the third party and foreign officials. More significant due diligence is warranted for those entities that potentially pose a greater risk.

Creating and implementing an effective compliance program is not only necessary to prevent violations of the FCPA and other anti-corruption laws, it may also help a company avoid liability in the event an employee or third party is found to have made improper payments. In one major FCPA investigation, the DOJ declined to bring an enforcement action against Morgan Stanley due to its strong internal controls, which were found to have provided the company ''reasonable assurances that its employees were not bribing government officials.''[38]

Business Benefits of Strong Compliance. Over and above its important FCPA implications, a strong compliance program may also provide opportunities in certain business situations. In many of the most promising emerging markets, bribery is not unusual and may appear to be a common means of carrying out business. Having a robust corporate compliance program, as well as the FCPA resource guide, to present to foreign officials to explain why inappropriate payments are not permissible can pay dividends.

Business may be completed more quickly, as the foreign official will be more easily convinced that a bribe simply will not be paid. Importantly, developing a reputation as a clean company can enhance the corporate reputation and bolster a company's credibility in the international marketplace. Such a reputation can be advantageous, as most responsible customers and companies prefer to do business with such companies.

The enforcement of the FCPA continues to be vigorous, and there is every indication that the telecommunications sector will continue to find itself in the crosshairs of the DOJ and SEC. This should serve as no surprise given the heavy participation of foreign governments in the telecommunications arena and the need for a provider to obtain licenses and other government authorizations to operate in a foreign country. An effective compliance program can help prevent improper payments, preserve a company's reputation and ethics, and potentially insulate the company from culpability in the event that an employee, agent, or third-party business partner may have transgressed the FCPA.

Ralph J. Caccia is a partner in Wiley Rein's White Collar Defense & Government Investigations Practice and co-chairs the firm's FCPA Practice. A former federal prosecutor, he focuses on defense of criminal and civil government enforcement actions, corporate internal investigations and congressional investigations. He can be reached at rcaccia@wileyrein.com.

Scott D. Delacourt is a partner in the firm's Communications Practice. He advises clients on FCC regulatory and transactional matters and has broad experience in wireless, telecom, mobile marketing and data privacy issues. He can be reached at sdelacourt@wileyrein.com.

Gregory M. Williams is a partner in White Collar Defense & Government Investigations and Litigation Practices. He has extensive FCPA experience managing international internal investigations, designing anti-corruption policies and conducting third-party due diligence. He can be reached at gwilliams@wileyrein.com.

P. Nicholas Peterson is an attorney in the White Collar Practice and represents clients facing civil and criminal investigations. He can be reached at npeterson@wileyrein.com.

[37] *SEC v. UTStarcom, Inc.,* No. 09-cv-6094, NPA (N.D. Cal. Dec. 31, 2009).

[38] DOJ press release, *Former Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA* (April 25, 2012), available at http://www.justice.gov/opa/pr/2012/April/12-crm-534.html.