Inside the FCPA: The Corruption & Compliance Quarterly

North America

BAKER & McKENZIE

Newsletter

Spring 2013

In This Issue:

Baker & McKenzie's quarterly corporate compliance publication, "Inside the FCPA," is an electronic and hard copy newsletter dedicated to the critical examination of developments in U.S. and international anti-corruption compliance that are of particular concern to global companies (and their officers and employees). The newsletter is written with the intention of meshing specialized U.S. coverage with a select international viewpoint in order to meet the expectations of an international client base and a discriminating readership. We seek to make our guidance practical and informative in light of today's robust enforcement climate, and we encourage your feedback on this and future newsletters.

If you would like to provide comments, want further information about the matters discussed in this issue, or are aware of others who may be interested in receiving this newsletter, please contact Sue Boggs of Baker & McKenzie at sue.boggs@bakermckenzie.com or +1 214 965 7281. We look forward to hearing from you and to serving (or continuing to serve) your FCPA, international anti-corruption, and corporate compliance needs.

The (Very) Long Arm of the Law: FCPA Jurisdiction Over Non-U.S. Companies and Individuals

By Douglas M. Tween, New York; Jerome Tomas, Chicago; and Joseph P. Rindone, New York

Whether and when non-U.S. companies are subject to the U.S. Foreign Corrupt Practices Act ("FCPA") is a question that has vexed executives and their lawyers since the statute was enacted some four decades ago. Recently, the U.S. Department of Justice ("DOJ") and Securities and Exchange Commission ("SEC") released a 120-page Resource Guide (the "Guide"), which provides a number of clarifications on the FCPA's application to non-U.S. companies. In practice, U.S. authorities can more often than not find a jurisdictional "hook" allowing them to pursue an anti-bribery enforcement action, as evidenced by the numerous FCPA cases brought against non-U.S. companies. Furthermore, recent SEC matters involving foreign nationals illustrate the broad interpretation by U.S. authorities of the scope of conduct sufficient to establish personal jurisdiction in the civil context.

Jurisdictional Reach of the FCPA

The anti-bribery provisions of the FCPA apply to U.S. issuers (*i.e.*, publicly-traded companies required to file reports with the SEC), domestic concerns (a U.S. citizen, resident, or national, or any company organized under the laws of a U.S. territory or having a principal place of business in the U.S.), and foreign nationals and entities who violate the FCPA while in the territory of the U.S. In any FCPA enforcement action, the government must establish that the

alleged conduct meets one of several jurisdictional bases contained in the statute.

Jurisdictional Predicates under the FCPA

In order to comprehend the reach of the FCPA's anti-bribery provisions, it is vital to understand the two primary bases for jurisdiction under the FCPA. The first basis is a form of nationality jurisdiction, which provides for jurisdiction over acts by issuers organized under U.S. law and domestic concerns regardless of where they take place. Prior to the 1998 amendments to the FCPA, the government had to prove that the issuer or domestic concern used a means or instrumentality of interstate commerce (*e.g.*, telephone/fax lines, mail, email, wire transfer) in furtherance of a violation. To conform with the Organization for Economic Cooperation and Development ("OECD") Convention on Combating Bribery, the interstate commerce requirement was eliminated for issuers and domestic concerns in 1998, collapsing the jurisdictional predicate down to a company's status as an issuer organized under U.S. law or a domestic concern. Nevertheless, U.S. authorities must still demonstrate the use of a means or instrumentality of interstate commerce in the case of a non-U.S. agent of a U.S. issuer or domestic concern, such as a foreign subsidiary or an issuer organized under foreign laws.

The second principal basis for jurisdiction is territorial jurisdiction, which provides for jurisdiction when a foreign national or entity uses a means or instrumentality of interstate commerce, or commits an act in furtherance of a violation, while in the territory of the U.S. This basis for jurisdiction was introduced in the 1998 amendments to the FCPA, and greatly expanded the jurisdiction of U.S. authorities to prosecute non-U.S. companies and nationals. In contrast to the nationality jurisdiction provisions of the FCPA relating to issuers and domestic concerns, this provision expressly requires that the use of the mails or means of interstate commerce or some other act in furtherance of an improper payment take place while the foreign person or entity is *in the territory* of the U.S. According to the Guide, the DOJ and SEC maintain that the requisite territorial nexus is satisfied if an agent commits an act in furtherance of an improper payment in the U.S., even if the non-U.S. company itself takes no action in U.S. territory.

The expansive approach to jurisdiction underlying FCPA enforcement has not abated. In the past, FCPA enforcement actions were typically brought against corporate defendants that were either issuers or domestic concerns. In recent years, however, U.S. authorities have increasingly investigated and prosecuted foreign persons and entities using more attenuated bases of jurisdiction, including minimal acts in furtherance of a corrupt payment having taken place in the U.S., aiding and abetting a violation of the FCPA, and participation in a conspiracy to violate the FCPA.

Jurisdiction Based on Acts Committed on U.S. "Territory"

As stated above, a non-U.S. person or company may face liability under the FCPA for using U.S. mails or emails that touch a U.S.-based server, or taking some other act in furtherance of an improper payment *while in the territory* of the U.S. In practice, U.S. authorities have asserted in numerous precedents that any action undertaken by a foreign company abroad that causes something to be done in the U.S. (*e.g.*, wire transfer, phone call, correspondent banking transaction) is sufficient for establishing jurisdiction, no matter how minimal the nexus of the U.S. conduct. In this context, U.S. authorities seem intent on pushing the jurisdictional bounds of the FCPA, and the link between the behavior in question and U.S. territory is becoming increasingly tenuous.

One example of the extraterritorial application of the FCPA is the DOJ's criminal enforcement actions brought against three non-U.S. subsidiaries of Siemens. The prosecutions appear to have been based on conduct only loosely connected to the U.S., including the employment of a U.S. agent, the use of U.S. bank accounts, and the use of U.S. mails and telephone lines. Such conduct may be viewed as satisfying the traditional interstate commerce requirement, which is one of the elements on which territorial jurisdiction may be based under the FCPA. What is less clear is whether, if tested in litigation, this conduct could withstand a challenge to the requirement that a company or individual acted *while in the territory* of the U.S.

Another example is the prosecution of individuals related to TSKJ, a Nigerian joint venture formed by Technip, Snamproghetti Netherlands, Kellogg Brown & Root ("KBR"), and JGC Corp. The DOJ and SEC charged that KBR executives acted in furtherance of the bribery scheme within and outside the territory of the U.S., which is more than sufficient to establish jurisdiction. In each of the charged financial transactions, the funds in question were transferred from a bank account in Amsterdam to agents' accounts in Japan, Monaco, or Switzerland. The pleadings did not allege that any of the relevant banks were located in the U.S. or that funds were held at U.S. banks; instead, the sole alleged jurisdictional connection for the substantive FCPA counts was that the transfers were denominated in U.S. dollars and therefore were transferred "via a correspondent bank account in New York, New York."

Aiding and Abetting and Agency Theories

U.S. authorities have also stretched the notion of jurisdiction under the FCPA by employing the theory of aiding and abetting liability. The Guide states that a "foreign national or company may . . . be liable under the FCPA if it aids and abets, conspires with, or acts as an agent of an issuer or domestic concern, regardless of whether the foreign national or company itself takes any action in the United States."

The SEC ploughed new precedential ground when it charged Panalpina, Inc., a U.S.-based company that was neither a U.S. issuer nor part of a U.S.-listed foreign company. The case marked the first instance of the SEC asserting jurisdiction over a non-issuer company that was not a subsidiary of an issuer. The SEC based its assertion of jurisdiction over Panalpina on the fact that the company was an agent of issuer clients and aided and abetted FCPA violations committed by those clients. In addition to this theory of liability, the SEC also charged Panalpina with primary liability under the FCPA as a result of its actions as an agent for certain of its issuer-customers.

Conspiracy

Conspiracy can also be used to establish FCPA jurisdiction over companies or individuals. Under U.S. law, each co-conspirator is liable for all of the foreseeable acts in furtherance of the conspiracy by every other conspirator. If U.S. authorities can establish jurisdiction over one conspirator, they have jurisdiction over all members of the conspiracy, regardless the location of the latter members. This concept has been applied in several recent FCPA enforcement actions, including one against Alcatel, where several non-U.S. subsidiaries were charged with conspiracy to violate the FCPA, and the DOJ alleged that "at least one of the co-conspirators committed or caused to be committed" various acts in the U.S. In support, the DOJ cited meetings, emails, and phone calls that Alcatel personnel had with individuals in Miami, Florida. They also detailed a series of wire transfers that included payments made from U.S. bank accounts and payments made from foreign accounts routed through U.S. correspondent accounts.

Personal Jurisdiction in Civil Actions

In order to bring a civil enforcement action, the SEC must establish personal jurisdiction over a corporate or individual defendant. Personal jurisdiction is typically not an issue when defendants are U.S. residents or companies organized or operating in the U.S. In the case of foreign individuals and corporations, however, it may be more difficult to demonstrate that personal jurisdiction exists.

The touchstone of personal jurisdiction is "minimum contacts," which in the federal context means contacts with the U.S. as a whole. A court will find that a defendant has the requisite minimum contacts with the U.S. if (i) the claim against the defendant arises out of or relates to those contacts and (ii) the defendant deliberately took advantage of the opportunity to do business in the U.S. If a defendant's conduct meets that standard, a court will likely find that it has personal jurisdiction unless the defendant can show that doing so would be unreasonable (*e.g.*, due to an undue burden on the defendant, or the interests of a different forum).

Two recent civil FCPA actions against individual defendants tested the question of personal jurisdiction and provide useful insight into the broad view of jurisdiction held by U.S. enforcement authorities and the judicial limitations on that view.

The court in *SEC v. Straub et al.* denied the defendants' motion to dismiss for lack of personal jurisdiction, finding that, if the SEC's factual assertions proved true, the court would have personal jurisdiction over the defendants. The judge noted that the defendants made false statements regarding disposition of the assets of their company – Magyar Telekom – that were being used in furtherance of the alleged bribery scheme. These false statements were then incorporated into the books and SEC filings of Magyar's parent company, Deutsche Telekom. Even though the bribery scheme occurred predominantly in a different country, the defendants engaged in conduct designed to violate U.S. securities laws. The judge specifically stressed that the defendants' concealment of the scheme from auditors and superiors – while knowing that false information would be provided to prospective U.S. investors – would be sufficient to assert personal jurisdiction.

In *SEC v. Sharef*, the court ruled that it did not have personal jurisdiction over one of the defendants – all former Siemens executives – because the defendant lacked sufficient "minimum contacts" to the U.S. Similar to Magyar, in the Siemens case, a local bribe scheme in Argentina was inaccurately incorporated into the company's books and SEC filings, and participants in the scheme filed Sarbanes-Oxley certifications that they knew were false. One defendant, Herbert Steffen, had a less significant role, and merely pressured one of the other defendants to authorize the bribes to Argentinian officials. The SEC argued that Steffen's promotion of the bribery scheme proximately caused the false filings with the SEC (a claim to which the judge responded skeptically).

The judge ruled, however, that even assuming Steffen's actions proximately caused the false filings, his actions were "far too attenuated from the resulting harm" to constitute minimum contacts. The judge cited *Straub* approvingly but distinguished the facts by emphasizing that Steffen's actions were not directed at deceiving U.S. shareholders, and that he did not authorize the bribe, direct the cover-up, or play any role in the falsified filings. The judge reasoned that minimum contacts may not arise merely from illegal conduct that ultimately has an effect on SEC filings -- or else every participant in unlawful conduct by a foreign issuer would be subject to the jurisdiction of U.S. courts.

The *Straub* and *Sharef* cases are instructive on personal jurisdiction in the FCPA context. First, they underscore how far personal jurisdiction can extend for issuers in civil enforcement actions. Both cases strongly suggest that potential wrongdoing by anyone who signs the certifications required under Section 302 of Sarbanes-Oxley could act as a "trigger" to personal jurisdiction. Second, these cases – particularly *Sharef* – reveal the SEC's internal thinking on the extent of its power to reach foreign individuals and entities. The SEC's position appears to be that any involvement in a bribery scheme that affects an issuer falls within the agency's enforcement authority. Despite losing the argument in *Sharef*, the SEC will likely continue to adhere to this position.

Conclusion

Foreign companies and individuals attempting to evaluate their level of exposure under the FCPA should proceed under the assumption that U.S. authorities will more often than not pursue an expansive jurisdictional theory in pursuit of an enforcement action. Moreover, the investigative tools available to the DOJ and SEC, coupled with the substantial litigation risk for target companies and individuals, enable authorities to place pressure on foreign companies before the issue of jurisdiction is ever raised. As the cases described above indicate, the fact development that occurs during the investigative stage typically yields an evidentiary basis for pursuing charges against a company using multiple legal theories other than (or in addition to) substantive FCPA charges.

Most foreign companies concerned about the FCPA likely face similar anti-bribery laws in their home countries, albeit with a lower level of enforcement activity. While a company should evaluate home jurisdiction conditions when calibrating the appropriate degree of action to take in order to minimize FCPA risks, the strategy should be one that proactively addresses and mitigates corruption risks rather than attempting to categorically avoid U.S. jurisdiction.

Douglas Tween is a Partner in the New York office. Jerome Tomas is a Partner in the Chicago office. Joseph Rindone is an Associate in the New York office.

Ensuring Anti-Corruption Compliance, Even in Low-Risk Countries: Surveying Singapore

By Andrew Martin, Singapore

Singapore's first Prime Minister, Lee Kuan Yew, once stated that there is a "duty to preserve a climate of confidence and discipline without which Singapore will wither away and die." Since independence in 1965, Singapore has evolved into one of the world's most highly developed and successful free economies. This success is based in no small part on a reputation for integrity, a reputation manifested in anti-corruption laws applicable to both the public and private sectors.

This commitment to integrity predates independence and is rooted in Singapore's main anti-corruption laws, the Prevention of Corruption Act ("PCA"), enacted in 1960, and the broader Penal Code. The PCA and the Penal Code cover private *and* public bribery and target both givers and recipients of bribes, which may include financial and other benefits. Neither permits facilitating payments.

Unlike many countries that adopt comprehensive anti-corruption laws only to summarily ignore them in practice, Singapore created the effective Corrupt Practices Investigation Bureau ("CPIB") in 1952 to identify suspected misconduct at home and began paying high salaries to public servants, all with the clear intent of combatting corruption. Singapore's consistently high ranking in Transparency International's annual Corruption Perceptions Index,

where the country compares favorably with all of its South and Southeast Asian neighbors, reflects the success of these measures. Even those corruption cases that have been publicly investigated by Singapore authorities, and which have garnered headlines over the last year or two, are notable more for salacious allegations of sexual misconduct than for any large sums paid as bribes, as one sees in more typical corruption investigations.

As compliance practitioners know, however, it is not only a company's home country that matters in terms of anti-corruption compliance. Equally important, in terms of compliance with the PCA and the world's most-enforced anti-corruption law, the U.S. Foreign Corrupt Practices Act ("FCPA"), or the more-recent U.K. Bribery Act, are the foreign countries in which one does business.

Singapore's impressive economic prosperity and laudable transparency may ironically expose its companies to increased risks of liability under applicable anti-corruption laws, as many use the country as a regional hub for Asia, a region perceived to have a high corruption risk. Many companies employ a Singapore holding company structure for Asian subsidiaries and run their regional sales and marketing teams from Singapore, raising the risk that misconduct by those subsidiaries or regional teams could taint their Singapore business.

These risks have not always carried the weight they should in Singapore and Asia generally. While the CPIB aggressively prosecutes corruption at home, there are far fewer instances of enforcement actions arising out of Singapore companies or individuals acting abroad. Too many Asian companies, including some in Singapore, therefore dismiss anti-corruption laws as irrelevant, and laws like the FCPA are often viewed by Asian companies as applying solely to U.S. persons. Yet, there are aspects of these laws that can and do affect Asian companies in several contexts. Moreover, when account is taken of local legislation, there is an increasingly complex web of anti-bribery laws that companies doing business in Singapore and greater Asia need to be mindful of whether they are acquiring businesses or just running day-to-day operations.

The pressure of regulation at home for multinationals and financial investors such as private equity funds, coupled with the expectations of shareholders and investors, affects how companies assess acquisition opportunities and invest in Singapore and Asia generally. The investigation or due diligence process is increasingly demanding, with buyers asking their lawyers and forensic accountants to look much more closely at potential bribery and other compliance issues that may affect the target. There is fear of inheriting liabilities that crystallize post-acquisition or the continuation of conduct that will trigger new liabilities for the buyer's group. In the worst case, acquirers and investors worry about buying into a business model based on misconduct that is simply unsustainable given the compliance framework that they have to observe.

The greater awareness among companies of compliance risk is changing the way cross-border deals are done. First, whereas the traditional due diligence exercise involves a desktop review of documents, compliance and anti-corruption due diligence entails a more nuanced approach. Buyers' advisors must appreciate the risk profile of the target business and their client's home regime in order to ask more focused questions that will identify "red flags" for the deal.

Rarely will the diligence exercise reveal a smoking gun on the face of the material provided by the seller. Therefore, in addition to the desktop review, it is important to raise questions through management interviews, usually conducted by senior lawyers who can tease out the issues and get a sense of the compliance culture within the target organization. For example, does the target have codes of conduct and other procedures in place such as gift-

giving and entertainment policies to guide its staff? Does it investigate and verify the credentials of third-party agents and consultants engaged to do business on its behalf especially if overseas? Does it conduct employee training and how has it dealt with incidents of misconduct in the past?

Secondly, depending on the severity of any issues uncovered in the diligence process, buyers are expecting more from sellers in the sales contract. They will try to leave as much compliance risk as possible with the sellers. This may take the form of sweeping indemnities or warranties and, if specific remediable issues are uncovered in due diligence, an insistence that the seller put things right before closing or carve out any tainted assets from the deal, assuming that is possible.

Thirdly, in addition to changes in diligence and deal terms, investors are looking to put procedures in place that reduce their future exposure. How problems are addressed, in particular through training and the roll-out of new standards and processes in the newly-acquired target, can help build credibility with enforcement authorities should they ever come calling.

The changing practices are not confined to the acquisition context. Increasingly, Singapore-based distributors, agents, and consultants – indeed any service providers – are facing demands from their international trading partners to provide more information on who they are, including their ultimate beneficial ownership, and on any government connections, backed up by promises to refrain from corrupt practices that may violate applicable anti-bribery laws.

Companies and their partners in Singapore must bear in mind that, even when laws may not be directly applicable, they can face liability for the actions of third-party intermediaries. In order to avoid confusion over whether or not a given law would apply to a particular party or parties – and thus to avoid asking one's business team or business partners to “play lawyer” – we recommend phrasing anti-corruption contract provisions in terms of the specific behaviors expected and prohibited and not in terms of violating this or that law. Of course it will not hurt to include as well an omnibus “compliance with laws” provision in addition to the more-specific “no improper payments” and other compliance provisions.

This enhanced diligence process and contractual protection combine to serve a second important function for buyers and trading partners: leaving a paper trail for their home regulators. Indeed, a significant element of the compliance process involves the ability to demonstrate to the authorities, should it become necessary, that compliance issues are taken seriously. There is little chance of leniency if there is nothing to point to in terms of diligence, deal documentation, or remedial action post-acquisition.

For the moment, most local Singapore companies have only felt these changes when they are on the receiving end of demands from their foreign counterparties. However, knowing one's acquisition targets and service-providers and securing proper contractual protection in these transactions represent good practices in any country, especially in the high-risk, high-reward markets that comprise the primary region where Singapore companies function.

Corporate Compliance Practice Group

Washington, DC

Lina A. Braude
Tel: +1 202 452 7078
lina.braude@bakermckenzie.com

Nicholas F. Coward
Tel: +1 202 452 7021
nicholas.coward@bakermckenzie.com

John P. Cunningham
Tel: +1 202 835 6148
john.cunningham@bakermckenzie.com

Richard N. Dean
Tel: +1 202 452 7009
richard.dean@bakermckenzie.com

Reagan R. Demas
Tel: +1 202 835 1886
reagan.demas@bakermckenzie.com

Edward E. Dyson
Tel: +1 202 452 7004
edward.dyson@bakermckenzie.com

Janet K. Kim
Tel: +1 202 835 1653
janet.k.kim@bakermckenzie.com

Paul J. McNulty
Tel: +1 202 835 1670
paul.mcnulty@bakermckenzie.com

Joan E. Meyer
Tel: +1 202 835 6119
joan.meyer@bakermckenzie.com

Jonathan C. Poling
Tel: +1 202 835 6170
jonathan.poling@bakermckenzie.com

John P. Rowley III
Tel: +1 202 835 6151
john.rowley@bakermckenzie.com

Brian L. Whisler
Tel: +1 202 452 7019
brian.whisler@bakermckenzie.com

Chicago

Robert J. Gareis
Tel: +1 312 861 2892
robert.gareis@bakermckenzie.com

Robert W. Kent
Tel: +1 312 861 8077
robert.kent@bakermckenzie.com

Jerome Tomas
Tel: + 1 312 861 8616
jerome.tomas@bakermckenzie.com

Peter P. Tomczak
Tel: + 1 312 861 8030
peter.tomczak@bakermckenzie.com

San Francisco

John F. McKenzie
Tel: +1 415 576 3033
john.mckenzie@bakermckenzie.com

Robert W. Tarun
Tel: +1 415 591 3220
robert.tarun@bakermckenzie.com

Houston

Lawrence D. Finder
Tel: +1 713 427 5030
lawrence.finder@bakermckenzie.com

New York

Marc Litt
Tel: +1 212 626 4454
marc.litt@bakermckenzie.com

Douglas M. Tween
Tel: +1 212 626 4355
douglas.tween@bakermckenzie.com

Miami

William V. Roppolo
Tel: +1 305 789 8959
william.roppolo@bakermckenzie.com

Allan J. Sullivan
Tel: +1 305 789 8910
allan.sullivan@bakermckenzie.com

Our Corporate Compliance Practice Group

Baker & McKenzie's North American Compliance team offers a comprehensive approach to assessing and resolving compliance related issues -- including everything from program building and prevention to investigations and remediation. Our team advises clients on the full range of issues relating to the FCPA, such as structuring transactions and commercial relationships to comply with the FCPA, developing and implementing FCPA compliance programs, establishing and conducting FCPA training programs, conducting internal investigations, advising corporate Audit Committees, and representing corporations and individuals before the Department of Justice, the Securities and Exchange Commission, and international regulatory bodies. The firm's extensive global network allows us to deliver FCPA-related services from offices in the overseas jurisdictions where issues arise, which in turn provides valuable local expertise on laws and culture, along with significant savings to our clients. Our coordinated approach combines a formidable presence in Washington, DC, with a vast network of experienced lawyers throughout the globe.

Andrew Martin is a Partner in the Singapore office.