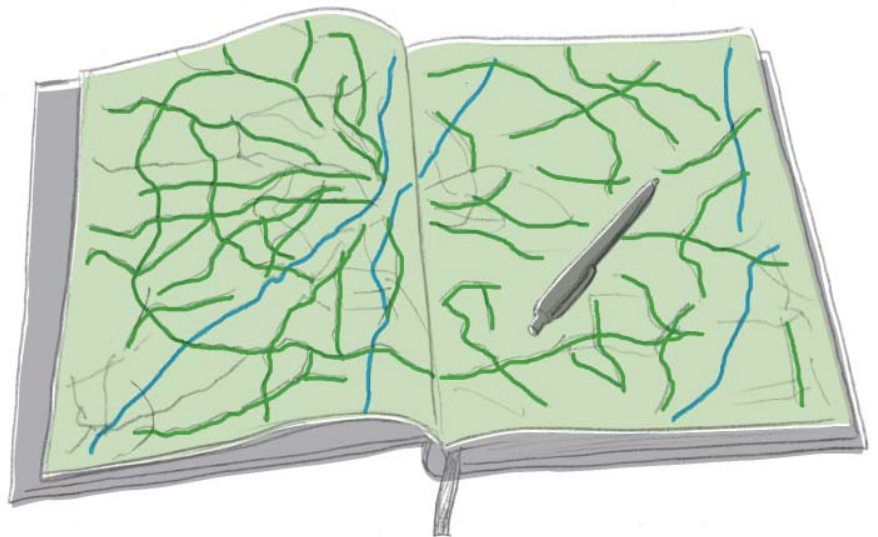


Navigating the Perils of FCPA Investigations in Emerging Markets

By William P. Olsen, Richard Kirt West, Nancy R. Grunberg and Danette R. Edwards
January 2009



Introduction

During the past several years, the Foreign Corrupt Practices Act of 1977 (“FCPA” or the “Act”)ⁱ has enjoyed an unprecedented renaissance as the U.S. Securities and Exchange Commission (“SEC”) and the U.S. Department of Justice (“DOJ”) have increasingly turned to the Act to penalize domestic and overseas companies, as well as individuals, suspected of bribing foreign officials to secure business. Congress initially passed the FCPA in 1977 in the wake of the Watergate scandal and after discovering that more than 400 corporations had made questionable or illegal payments to foreign officials to gain business or smooth business processes. The FCPA aims to prevent bribery of foreign officials and encourage the establishment of certain accounting controls and practices. The Act applies to companies whose securities are registered with the SEC, and certain of the Act’s provisions extend duties and liabilities to registered companies based on the conduct of their partly-owned subsidiaries. This article is concerned with *both* the bribery and accounting provisions of the Act and the special compliance and enforcement challenges that each present in certain regions of the world.

Last year was a watershed period for FCPA enforcement: DOJ instituted sixteen FCPA prosecutions in 2007, as compared to four only five years before.ⁱⁱ A special FCPA taskforce within the Federal Bureau of Investigation (“FBI”) was established last year. In announcing the taskforce, the FBI’s Assistant Director, Chip Burrus, proclaimed that the agency’s “highest criminal priority is to curb public corruption, whether here or overseas...”ⁱⁱⁱ The SEC has filed more than thirty FCPA actions within the past two years.^{iv} In 2008, the rate of filing of FCPA enforcement actions has so far outpaced that of 2007. All signs indicate that this trend will continue. In the future, enforcement may even be fueled by a limited class of private litigants as outlined in a recent proposal to amend the Act.^v >



ⁱ 15 U.S.C. §78m(b)(2) - 78m(b)(7), 78dd-1, 78dd-2, 78dd-3, 78ff(c).

ⁱⁱ See March 2008 DOJ fact sheet available at: http://www.usdoj.gov/opa/pr/2008/March/08_ag_246.html.

ⁱⁱⁱ See 2007 FBI press release available at: <http://www.fbi.gov/page2/feb07/fcpa020507.htm>.

^{iv} See Linda Chatman Thomsen's March 27, 2008 remarks before the Minority Corporate Counsel 2008 CLE Expo, which is available at: <http://www.sec.gov/news/speech/2008/spch032708lct.htm>.

^v On June 4, 2008, Rep. Ed. Perlmutter (D. Colo.) introduced the “Foreign Business Bribery Prohibition Act of 2008” (H.R. 6188), which would provide for a limited private right of action under the FCPA. Potential litigation targets are limited to “foreign concerns,” so the class of potential defendants is restricted to foreign persons unaffiliated with U.S. stock exchanges. The proposed legislation is available at: <http://www.govtrack.us/congress/bill.xpd?bill=h110-6188>.

Introduction (continued)

The recent spike in FCPA enforcement is undoubtedly the result of companies moving more aggressively into “emerging markets”^{vi} where antibribery laws tend to be somewhat lax and bribes are often viewed as a normal part of the business process. Indeed, a large number of 2007 and 2008 cases have involved emerging markets.^{vii} Often, poorly trained employees in these environments assume a “when-in-Rome” attitude, not realizing that the local way of doing business may be a direct violation of U.S. laws and regulations. Many companies that fail to evaluate the full landscape of risks before entering a new market^{viii} later find themselves faced with an investigation centering on potential FCPA violations.

Managing FCPA investigations in emerging markets can be even more complex than transnational investigations in established markets, and companies need to understand these complexities in order to avoid the creation of additional liabilities. The remainder of this article presents a high-level overview of issues arising in FCPA investigations in emerging markets, along with practical tips for preventing and dealing with these issues.

vi The term “emerging markets” means countries that are restructuring their economies along market-oriented lines so as to present opportunities in trade, technology transfers, and foreign direct investment. According to the World Bank, the five biggest emerging markets are China, India, Indonesia, Brazil and Russia. Other countries that are also considered as emerging markets include Mexico, Argentina, South Africa, Poland, Turkey, and South Korea. See Chuan Li, “What are Emerging Markets?” (published by The University of Iowa Center for International Finance and Development), available at: http://www.uiowa.edu/ufdebook/faq/faq_docs/emerging_markets.shtml.

vii For instance, the past two years have seen FCPA cases involving conduct in emerging markets by the following companies: Faro Technologies, Inc. (On June 5, 2008, agreed to a non-prosecution agreement related to allegedly corrupt payments to Chinese government officials in violation of the FCPA); Westinghouse Air Brake Technologies Corp. (for conduct in India); AGA Medical Corp. (for conduct in China); Baker Hughes (for conduct in Russia and Indonesia); York International Corp. (2007 settlement for allegedly paying bribes in China, India, Turkey and elsewhere in connection with the Oil-for-Food Program); Textron, Inc. (for conduct in India); Paradigm B.V. (for conduct in China and Indonesia); Biomet, Inc. (for conduct in Poland); Medtronic, Inc. (for conduct in Poland); Smith & Nephew plc (for conduct in Poland); Stryker Corp. (for conduct in Poland); Zimmer Holding, Inc. (for conduct in Poland); Robert Philip and Si Chan Wook of Schnitzer Steel Industries, Inc. (for conduct in China); InVision Technologies, Inc. (for conduct in China); Diagnostic Products Corp. (for conduct in China); Lucent Technologies Inc. (for conduct in China).

viii The FCPA does acknowledge the complexities of conducting business in emerging markets. It includes exceptions that allow certain payments to help ease the transition into a country. These payments must be aimed at facilitating government procedures, as opposed to sidestepping them. For example, a company can generally hire an agency to facilitate the processing of employee passports and other paperwork. Similarly, many companies hire local representatives to help move equipment through customs quickly. This is normally considered legitimate, as long as the agency is not linked to government officials who oversee the process. The FCPA also allows companies to hire police protection to keep their employees safe.

Initial Concerns: Defining Fact-Gathering Activities, Staffing, and Privilege Issues

When fact-gathering in situations other than responding to a government inquiry, companies have some flexibility in how to characterize those activities at the site of the foreign operation. Depending upon the characterization (compliance monitoring vs. auditing vs. investigation), a company may encounter different levels of resistance in the foreign environment. For instance, a 2008 DOJ Advisory Opinion details the difficulties that a major U.S. company and its wholly-owned foreign subsidiary experienced when attempting to conduct due diligence on a foreign private company owner who would be considered a “foreign official” under the FCPA. The due diligence was undertaken in order to alleviate FCPA concerns related to a series of intended transactions whereby both the subsidiary and the foreign private company owner would acquire an entity responsible for managing certain public services for a foreign municipality. The foreign owner refused to make or accede any disclosures regarding his various roles or corporate interests, asserting that “in the foreign country it was neither necessary nor customary to do so.” Ultimately, the U.S. company was forced to approach various high-ranking government officials who confirmed some of its concerns. While the Opinion does not reveal the country in which this took place, it appears to have occurred in a socialist, state-run economy, where many of these fact-finding concerns arise.^{ix}

In some jurisdictions, it may be easier to obtain official approvals to conduct auditing or compliance monitoring than to perform an investigation. How a company refers to fact-gathering activities at the foreign site may rest partly on who is performing those activities (lawyers vs. non-lawyer professionals including forensic auditors, computer forensic specialists, and investigators). As with many other issues, it is advisable to obtain the advice of local counsel at the outset of the project.

The involvement of non-lawyer professionals in foreign countries raises an important issue: to what extent, if at all, would a U.S. court apply the attorney-client privilege to communications involving these professionals overseas? In all probability, the answer to this question will turn on the law of the country with the greatest nexus to the subject of the inquiry. U.S. courts have shown a willingness to apply privilege protection to communications with a non-lawyer in a foreign country where the non-lawyer is, consistent with foreign custom, essentially acting as an attorney in connection with the subject matter of the communication.^x Privilege concerns are not limited to situations involving non-lawyers. In emerging markets, communications with in-house lawyers in the course of FCPA monitoring, audits, and investigations may not qualify for privilege protection.^{xi} This issue underscores the need for consulting local counsel concerning applicable privileges in the foreign jurisdiction. It also may argue for the use of practitioners from the U.S. because of the strong protection American courts give to attorney-client communications and work product. >

ix See Department of Justice, “Foreign Corrupt Practices Act: Opinion Procedure Release,” No. 08-01, January 15, 2008.

x See *Golden Trade, S.r.L. v. Lee Apparel Co.*, 143 F.R.D. 514, 519 n.3 (S.D.N.Y. 1992) (privilege extended to communications between client and foreign patent agents concerning prosecution of foreign patents since the relevant foreign jurisdictions essentially regarded patent agents as lawyers in patent prosecution matters).

xi See, e.g., Henry Klehm, III, “Cross-Border Considerations in Internal Investigation,” PLI Order No. 14541, *312 (June 2008) (privilege does not extend to in-house lawyers in Russia, among other places). See also, e.g., Joseph Pratt, Comment, “The Parameters of the Attorney-Client Privilege for In-House Counsel at the International Level: Protecting the Company’s Confidential Information,” 20 *NW. J. Int’l L. & Bus.* 145, 162-164 (1999). The article notes that the Chinese government has historically taken a more public approach to corporate and personal information that might be considered confidential in other jurisdictions for privilege purposes. “[L]awyers in China have traditionally been required to place their allegiance to the state above loyalty to an individual client. Adding to this problem, China has only recently enacted statutes giving effect to a legal doctrine like the attorney-client privilege. Thus, the attorney-client privilege in China remains untested and may not afford much protection when competing state interests are at stake.” (Emphasis added.)

Initial Concerns: Defining Fact-Gathering Activities, Staffing, and Privilege Issues (continued)

There are also operational hurdles to gathering facts abroad. Immigration regulations in emerging markets may require outside counsel and nonlawyer professionals (depending upon their country of origin) to obtain business visas.^{xii} Where business visas are needed, outside counsel must understand any work restrictions imposed. For instance, some countries prohibit business travelers from conducting interviews, writing reports, and carrying out computer forensics.^{xiii} The good news for defense counsel is that similar work restrictions apply to government lawyers and other officials traveling abroad on “judicially-related official business.” Such business includes activities such as interviewing witnesses, taking depositions, or conducting investigations and inspections. Government officials must secure permission from the host country to conduct these activities; this requirement usually means that a diplomatic note must be sent to the Ministry of Foreign Affairs requesting permission. See e.g., U.S. Attorneys Manual, 3-8.730.



xii For instance, in China, a business visa (“F Visa”) will only be issued if the foreigner or “alien” to China is invited to China for, among other things, a visit, an investigation, or to perform business. Typically, an invitation letter from an established Chinese entity is required in order for the business visa application to be considered for possible approval. See <http://www.china-embassy.org/eng/hzqz/zgqz/t84247.htm>.

xiii Attorneys seeking to depose or gather information from individuals in China must be particularly prudent, as conducting even a voluntary deposition may lead to the arrest, detention, expulsion, or deportation of the American attorneys and other participants. Chinese authorities do not recognize the authority or ability of foreign persons, such as American attorneys, to take voluntary depositions of willing witnesses, even before a U.S. consular officer, notwithstanding Article 27(1) of the U.S. - China Consular Convention of 1980, 33 U.S.T. 3048, TIAS 10209. Moreover, in its declaration on accession to the Hague Evidence Convention, China states that it does not consider itself bound by Articles 16-22 of Chapter II of the Convention. Therefore, China may deem taking depositions or conducting interviews by American attorneys or other persons in China as a violation of China’s judicial sovereignty. In 1989, China permitted the taking of a limited deposition in the matter of *U.S. v. Leung Tak Lun, et al.*; CR 88-0214- WHO in a matter before the U.S. District Court for the Northern District of California. However, the U.S. was advised by China that the particular grant of authority for that deposition should not be regarded as a precedent, and we understand that efforts to obtain permission from the Chinese Ministry of Foreign Affairs to conduct depositions since then have been unsuccessful.

Obtaining and Reviewing Records

Once a company has made early decisions regarding the use of outside lawyers and non-lawyer professionals and ironed out the broad operational issues, it can concentrate on the mechanics of fact-gathering activities. To a large degree, this task means determining how to conduct an appropriate records review. This portion of an investigation can be quite challenging for many companies even when there are only domestic concerns involved, especially when it comes to the preservation and processing of electronic records. The process can be fraught with additional difficulties in emerging markets as a result of the different laws, languages, and attitudes toward recordkeeping in those jurisdictions.

Recordkeeping. As an example of the difficulty that may be encountered in emerging market countries, recordkeeping practices in Asia differ widely from those in the United States. In China, official tax receipts are known as “fa piao.” These documents are official receipts received by the purchaser of goods and services from establishments. They are used by establishments to document the sale of goods and services for tax purposes as part of China’s Value Added Taxation (VAT) system. Companies in China must maintain these documents as proof of the business expenses for which employees are reimbursed, such as meals or lodging. The “fa piao,” however, show only the amount and the company “chop” (official company stamp) of the establishment that issues them; they do not show details of the transaction, such as the nature of the goods or services provided.

This system does not provide for the transparency of transactions that is commonplace in the United States and presents a stark contrast to the American approach to recordkeeping. After Congress expanded the federal obstruction of justice laws in 2002 via the Sarbanes-Oxley Act, many companies invested substantial resources in the design (or re-design) and implementation of robust corporate records and information management programs for their U.S. offices. The December 2006 e-discovery amendments to the Federal Rules of Civil Procedure prompted many companies to redouble their records management efforts within the last year, at least with respect to U.S. operations.

In light of the recent spate of FCPA cases charging books and records violations,^{xiv} companies would be well-advised to focus their attention on recordkeeping practices abroad.^{xv} The accounting provisions of the FCPA contain both internal controls requirements and recordkeeping requirements. Broadly speaking, the internal controls provisions require companies to establish a framework of internal controls that will ensure that transactions are appropriately authorized and that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP or other applicable laws.^{xvi} The recordkeeping provisions require companies to maintain accurate books and records “which in reasonable detail accurately and fairly reflect the transactions and disposition of the [company’s] assets.”^{xvii} >

xiv FCPA accounting provisions apply to any issuer that has a class of securities registered pursuant to 15 U.S.C.A. § 781 or that is required to file reports under 15 U.S.C. § 78o(d).

xv For general information about the design and implementation of records and information management programs, see the following publications, both of which are posted on Venable’s website: “Are You Protected? Frequently Asked Questions and Answers about Records and Information Management,” by W. Warren Hamel and Danette R. Edwards, (March 2008); available at: http://www.venable.com/publications.cfm?action=view&publication_id=1883&publication_type_id=3; “Avoiding the Next ‘Spygate’: Critical Records Management Advice for Your Company in the Wake of the Destruction of the NFL and CIA Tapes,” by Danette R. Edwards, Mealey’s Litigation Report: Discovery, Vol. 5, #7 (April 18, 2008).

xvi 15 U.S.C. § 78m(b)(2)(B).

xvii 15 U.S.C. § 78m(b)(2)(A).

Obtaining and Reviewing Records (continued)

Failure to abide by the Act's accounting provisions can expose companies and individuals to significant fines and penalties.^{xviii} Some well-publicized, recent fines in cases involving allegations of FCPA accounting violations have exceeded \$30 million and \$40 million.^{xix} The threat of these stiff penalties, coupled with the known risks of inadequate recordkeeping practices in certain emerging market countries, make overseas records management initiatives a corporate governance imperative that guarantees to smooth the process of data collection in an investigation.

Data Collection and Processing. One of the many challenges in conducting an investigation abroad is ensuring that information obtained on targeted individuals, whether the information consists of hard copy records or electronic data recovered by computer forensic techniques, actually pertains to the targeted person. For instance, in China there are often problems in translating the individual's English name into Chinese because of the many characters found in the Chinese language. People are commonly mistaken for others. In addition, the commonality of last names in China can make it exceedingly difficult to be confident that any information retrieved about an individual is in fact referring to that individual and not another individual with the same name.

In Latin American countries, the convention of having the mother's maiden name at the end of an individual's surname can potentially lead to the misidentification of individuals.

With respect to financial records, as evidenced by the "fa piao" in China, the accounting records that must be maintained in emerging markets may be very different both in content as well as format from those that are maintained in the United States and the EU. Often records are not in electronic form and may be extremely difficult to retrieve.

For these reasons, it may be desirable to have the assistance of an independent local forensic accounting firm that can provide cultural and language assistance during an investigation. The local forensic accounting firm will know what records are available and will know where such records can be found and, of course, can provide invaluable assistance in reviewing such records. Similarly, these same language skills will be critical in conducting an effective forensic search of computers and servers and analyzing records discovered during the search. >

^{xviii} In addition to civil penalties, companies can pay up to \$25 million in criminal fines for each accounting violation. These fines can be increased to a maximum of two times the amount of the benefit that the company sought to gain through its illegal conduct. The repercussions for individuals are also severe; these include a maximum \$5 million criminal fine and up to 20 years in prison. The Act's bribery provisions carry their own hefty criminal fines and penalties—\$2 million per violation for companies (which can be increased to a maximum of two times the amount of the benefit that the company sought to gain through its illegal conduct) and \$100,000 per violation for individuals and up to 5 years in prison, or both.

^{xix} In April 2007, Baker Hughes, Inc. agreed to pay \$44 million to settle the SEC's claims that it violated the Act's antibribery, books and records, and internal controls provisions when it engaged in certain activities in Indonesia, Russia, and elsewhere. On May 14, 2008, Willbros Group, Inc. agreed to pay a combined total of \$32.3 million to the DOJ and the SEC to settle FCPA charges (including anti-bribery, books and records, and internal controls charges) and related securities fraud charges.

Obtaining and Reviewing Records (continued)

Trans-Border Data Flow Issues. Pitfalls and hurdles for U.S. lawyers in gathering facts abroad are not only limited to emerging markets. For example, the European Union’s directive on data privacy (“EU Directive”) has been in place since 1995.^{xx} The EU Directive served as a model for the personal data protection laws of Argentina and Poland,^{xxi} to name a few examples, and other emerging market countries may look to it if and when they adopt or amend their own data protection laws. It creates some hurdles to the gathering and use of information, such as that contained in e-mails. In brief, the EU Directive and the laws of Argentina and Poland essentially require consent to use personal data and place limits on the transmission of personal data to third party countries.^{xxii} Even within-company transfers are not allowed if the recipient jurisdiction does not have adequate data protection laws of its own. Violations of the transfer rules are punishable through fines, penalties, lawsuits, and other sanctions. EU member states have implemented the strictures of the EU Directive through their own data

protection legislation. Some EU member states already had substantial privacy protection regimes in place well before the EU Directive took effect, and the EU Directive was a mere supplement. Additionally, some countries’ privacy laws contain criminal blocking statutes that criminalize the export of specific categories of documents and information. Also, depending upon the country, banks may be restricted from disclosing certain data pursuant to bank secrecy laws. In the future, these more stringent rules could also find a place in the privacy protection laws of emerging market countries.

Accordingly, before reviewing and/or exporting documents or data in an international FCPA investigation, counsel must be aware of the nuances in the privacy and data protection laws of the applicable countries. Finally, it is important for companies and defense counsel to realize the value of data protection laws, blocking statutes, and bank secrecy laws as bases for potential objections to evidence-gathering (and sharing) by governmental authorities in international investigations.

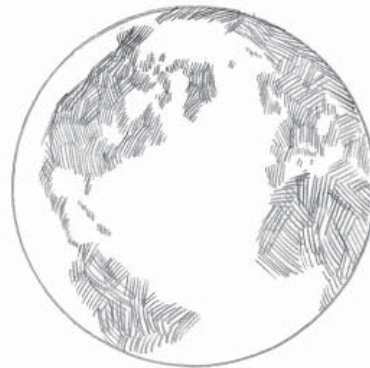
xx The EU data protection law is known as Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It is available in English on the European Commission’s website at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#directive.

xxi Argentina’s Law for the Protection of Personal Data (Law 23.56) is available in English on the Central Bank of Argentina’s website at: <http://www.bcra.gov.ar/pdfs/marco/IHabeas%20Data.PDF>. Poland’s Act on the Protection of Personal Data is available in English on the Polish Inspector General’s website at: http://www.giodo.gov.pl/data/filemanager_en/98.doc.

xxii See EU Directive 95/46/EC, Article 2. Chapter II, Article 12 of Argentina’s data protection law addresses international transfers of data. Chapter 7, Article 47 of Poland’s data protection law addresses the transfer of personal data to a third country.

Compounded Liability Risks Due to International and Domestic Parallel Proceedings

Government enforcement authorities in post-911 society appear more committed than ever to information-sharing.^{xxiii} There are a handful of mechanisms available to governmental authorities for evidence-gathering (and sharing) purposes in international investigations. Mutual Legal Assistance in Criminal Matters Treaties (“MLATs”) are a prime example. MLATs are treaties between the U.S. and other nations that govern cooperation between DOJ and other foreign prosecuting authorities. Through MLATs, other countries provide DOJ with evidence from foreign companies and individuals for use in U.S. investigations and proceedings, and vice versa. MLATs also generally allow criminal authorities to share requested information with regulatory agencies (e.g., the SEC or its foreign counterparts, such as the Hong Kong Securities and Futures Commission), and to request information for the purpose of assisting regulatory investigations.^{xxiv} MLATs generally allow witnesses to be summoned, documents and other evidence to be produced, searches to be executed, and process to be served. The U.S. has numerous MLATs in force, including ones with the following countries with emerging markets: Argentina; Brazil; Hong Kong SAR; India; Korea; Mexico; Poland; Russian Federation; South Africa; and Turkey.^{xxv}



In addition to MLATs, governmental authorities can obtain information through less formal, case-by-case arrangements between the regulatory bodies of different nations. In this regard, the SEC often utilizes what are known as Memoranda of Understanding, or MOUs, which provide for the sharing of evidence and cooperation in compliance and enforcement efforts. MOUs can be used to collect evidence for civil and criminal investigations. The SEC’s arrangements with other countries also include frameworks for cooperation and less specific exchanges. Another method whereby the SEC gathers evidence is issuance of domestic subpoenas for the production of data located in a foreign country. >

xxiii A recent testament to this attitude is the June 12, 2008 U.S. – E.U. law enforcement data-sharing agreement. The agreement consists of 12 guiding principles that will ultimately be incorporated into a more formal document addressing the handling and protection of personal data by governments and businesses on both sides of the Atlantic. More specifically, the principles cover topics such as transparency/notice to the person whose data is being shared and restrictions on onward transfers of shared data to third countries. The principles are intended to be applied by governments and businesses “for the prevention, detection, investigation, or prosecution of any criminal offense,” not just suspected terrorism. (Emphasis added.)

xxiv See, e.g., Article 1(2) of the MLAT between the U.S. and India (Treaty Doc. 107-3, 107th Cong., 2d Sess.). As explained in the Secretary of State’s January 9, 2002 letter of submittal, “[t]he scope of the Treaty includes the obligation to provide assistance not only with respect to the investigation, prosecution, and prevention of criminal offenses, but also with respect to proceedings related to criminal matters, which may be civil or administrative in nature.”

xxv See State Department website at: http://travel.state.gov/law/info/judicial_690.html?css=print.

Compounded Liability Risks Due to International and Domestic Parallel Proceedings (continued)

For companies, the existence of each of these data collection and sharing methods means that evidence located abroad might become available to the U.S. government (or, conversely, to a foreign government) if a government investigation is initiated outside of the U.S. Once foreign documents are accessible to one nation's governmental authorities, other governments can potentially gain access to them through MLATs, MOUs, or other similar treaties or agreements. The risk of incurring additional liabilities in multiple legal systems as a result of international information sharing policies should be taken into consideration in deciding whether to voluntarily cooperate with certain government agencies in matters implicating the FCPA or foreign bribery laws.

The risk of incurring multiple types of liabilities as a result of providing information to one governmental authority and then having that information shared with other authorities is not limited to cooperation between sovereign nations. Domestic parallel proceedings by DOJ and SEC^{xxvi} in cases involving FCPA violations are typical, with the SEC sometimes tacking on additional securities fraud claims.^{xxvii} In light of this phenomenon, defense counsel and companies must carefully weigh the decision to cooperate in a civil FCPA investigation, as it could lead to criminal liability in a domestic parallel proceeding.^{xxviii}

xxvi The mechanisms by which information is passed from the SEC to DOJ are embodied in Section 20(b) of the Securities Exchange Act of 1933 (codified at 15 U.S.C. § 77(b)) and § 21(e) of the Securities Exchange Act of 1934 (codified at 15 U.S.C. § 78u(d)). These statutes similarly provide that whenever it appears to the SEC that a violation of the relevant Act has occurred, the SEC may "transmit such evidence as may be available concerning such acts or practices to the Attorney General" who may, in his discretion, institute the necessary criminal proceedings.

xxvii See supra note 21 (regarding the Willbros Group, Inc.).

xxviii For information about the limits on the government where there are parallel civil and criminal investigations, see the following article, which is available on Venable's website: "Pay No Attention to the Man Behind the Curtain: United States v. Stringer and the Government's Obligation to Disclose", by W. Warren Hamel and Danette R. Edwards, BNA White Collar Crime Report, Vol. 3, No. 11 May 23, 2008.

Conclusion

The DOJ and the SEC have substantially increased their focus on the FCPA in the past several years and regard the FCPA as their most potent weapon in combating foreign corruption. With this increased focus on the FCPA, the overseas operations of U.S. based corporations will be facing more scrutiny. U.S. corporations that proactively investigate potential FCPA violations and self-report the findings to DOJ and the SEC are less likely to face some of the harsh penalties that can be imposed by these agencies. Understanding the unique challenges in conducting FCPA investigations in emerging market countries will help counsel provide effective representative for the client and reduce the risk to the client.



About the authors

Mr. Olsen is a principal in Grant Thornton LLP's Forensic Accounting and Investigative Services practice located in McLean, Virginia. He has performed numerous FCPA investigations in Asia, Eastern Europe and Latin America. He also conducted investigations involving organized crime, business corruption and management fraud and has consulted with several Global 1000 clients in developing comprehensive anti-fraud, anti-corruption and anti-money laundering programs.

Mr. West is a senior manager in Grant Thornton LLP's Forensic Accounting and Investigative Services practice in McLean, Virginia. He is the former Inspector General of the Legal Services Corporation with more than twenty years in federal law enforcement including senior positions at the Offices of Inspector General at the Department of Labor, Central Intelligence Agency and United States Postal Service.

Ms. Grunberg is a partner at Venable LLP and the co-chair of the firm's SEC/White Collar Defense practice group. She spent approximately 10 years at the U.S. Securities and Exchange Commission and was an Assistant Director in the Enforcement Division when she left to join Venable in 2002. Her practice includes defense of all varieties of SEC investigations, including FCPA cases.

Ms. Edwards is an associate in Venable's SEC/White Collar Defense practice group. Her practice includes white collar criminal defense, complex civil cases, and advising clients on corporate compliance and internal control issues, including records management policies and a range of Sarbanes-Oxley related matters. She also focuses on environmental criminal defense and internal investigations.

About the forensic accounting and investigative team

Grant Thornton's forensic accounting and investigative services team has a unique combination of Certified Public Accountant (CPA) auditors and tax professionals, Certified Fraud Examiners (CFE), Certified Anti-Money Laundering Specialists (CAMS), certified electronic data discovery technologists, and high-tech computer and research tools that give us unmatched capabilities to successfully perform the most complex forensic accounting assignments. Our credentialed specialists use established forensic investigation methods such as interviews, computer forensics, financial analysis, records research and background searches to discover the red flags that uncover evidence of fraud. We produce reliable findings and conclusions, which have been used successfully in civil, criminal and bankruptcy proceedings, corporate actions, governmental inquiries, regulatory investigations and insurance claim cases, among other matters. For more information on our services, locations or advisory professionals, visit us at www.GrantThornton.com/advisory.

Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd, one of the six global audit, tax and advisory organizations. Grant Thornton International Ltd and its member firms are not a worldwide partnership, as each member firm is a separate and distinct legal entity.

Grant Thornton Investigations Leaders

William P. Olsen – McLean, VA
National Investigations Practice Leader
T 703.847.7519 E William.Olsen@gt.com

Erik C. Lioy – Charlotte, NC
T 704.632.6915 E Erik.Lioy@gt.com

David Wedding – Charlotte, NC
T 704.632.6787 E Dave.Wedding@gt.com

Thomas L. Kabler – Chicago, IL
T 312.602.8010 E Thomas.Kabler@gt.com

Jeff Matthews – Dallas, TX
T 214.561.2420 E Jeff.Matthews@gt.com

James Schmid – Detroit, MI
T 248.233.6910 E Jim.Schmid@gt.com

Nick D'Ambrosio – Houston, TX
T 832.476.3654 E Nick.D'Ambrosio@gt.com

Shauna Woody-Coussens – Kansas City, MO
T 816.412.2550 E Shauna.Woody-Coussens@gt.com

Doug Anderson – Miami, FL
National Forensic Technology Practice Leader
T 305.381.7540 E Douglas.Anderson@gt.com

Renée Marino – Minneapolis, MN
T 612.677.5180 E Renee.Marino@gt.com

Gary Goldman – New York, NY
T 646.825.8430 E Gary.Goldman@gt.com

Bradley J. Preber – Phoenix, AZ
National Litigation Practice Leader
T 602.474.3440 E Brad.Preber@gt.com

Robert C. Albretsen – Seattle, WA
T 206.398.2404 E Bob.Albretsen@gt.com

Beginning in 2009, the Economic Advisory Services Practice of Grant Thornton LLP is proud to offer our new **Focus on Forensics** newsletter providing valuable insights to corporate decision-makers and their legal counsel. To subscribe, visit us at www.GrantThornton.com/subscribe.



© Grant Thornton LLP
All rights reserved
U.S. member firm of Grant Thornton International Ltd