International Compliance

Mitigating Risk In FCPA and Other Cross-Border Transactions

By Jacob S. Frenkel and Ira E. Hoffman

The "good news" is that President Obama has launched the "National Export Initiative," with the goal of doubling exports over the next five years by "working to remove trade barriers abroad, by helping firms – especially small businesses – overcome the hurdles to entering new export markets, by assisting with financing, and in general by pursuing a Government-wide approach to export advocacy abroad, among other steps." Exec. Order No. 13,534, 75 Fed. Reg. 12,433 (Mar. 11, 2010). In other words, the Federal Government is committed to helping grow exports at an unprecedented pace, and Maryland businesses that are innovators in such areas as technology, pharmaceuticals, homeland security and defense can look forward to significantly increased cross-border opportunities.

The "bad news" is that the Government also is intensifying enforcement of the Foreign Corrupt Practices Act ("FCPA"), 15 U.S.C. §§ 78dd-1 *et seq.*, and other statutes governing the conduct of and compliance by U.S. companies and persons, and their representatives, seeking to enter or expand business in international markets. For example, the FCPA enforcement trail in the first quarter of calendar year 2010 is littered with such international corporate giants as BAE Systems plc (but not its Maryland-based U.S. subsidiary, BAE Systems, Inc.), which paid a $400 million criminal fine for violating the FCPA (and the Arms Export Control Act and International Traffic in Arms Regulations), and Daimler AG, which, together with three non-U.S. subsidiaries, paid $185 million in criminal fines and civil penalties for FCPA violations.

In late 2008, Siemens AG set the record for off-the-charts penalties, as coordinated enforcement actions by DOJ, the Securities and Exchange Commission ("SEC") and German authorities resulted in the payment of penalties alone of $1.6 Billion. Yet, at the other end of the enforcement spectrum, but of equally high profile, was the arrest of 22 persons from 16 different companies in January 2010 as a result of a multi-year sting operation in the military and law enforcement products industries. *See, e.g.*, http://www.shulmanrogers.com/media/publication/63_ENFORCE.pdf. As of the end of the first quarter of 2010, DOJ has approximately 140 active FCPA investigations.

Despite such dramatic changes in doing business globally, U.S. lawyers instinctively focus on the efficacy and enforceability of contracts. There often is a general knowledge that certain countries are off limits, certain products are not eligible for export and certain labor practices are not acceptable. Once corporate managers identify target countries for expansion, the outreach to effect market penetration begins. Before looking beyond America's borders to new business frontiers, however, companies are best served if they first look internally at their compliance systems and governance structure, as the effectiveness of these essential corporate principles could impact significantly the ability of companies to continue doing business both domestically and internationally.

An intense and understandable focus on a company's revenue generation, particularly in non-publicly held and smaller companies, tends to result in delaying the adoption and implementation of prudent governance policies and procedures. That is, until it's too late. Executives often view compliance and governance issues as unnecessary costs, a drain on the bottom line. As a result, they are more inclined to react to problems than proactively mitigate risk. It is the executives and directors acting with foresight who view governance as an integral part of doing business on a daily basis. Regardless of perspective, the current business climate – which will not change – features an expectation that corporations be good citizens, and the template for corporate citizenship and best practices is accomplished through a governance program.

DOJ undoubtedly recognizes that the push to prosecute individuals, such as principals, agents and employees of many smaller companies in the January sting operation, is more likely to get the attention of business executives and managers than prosecutions of corporate entities. Indeed, as the Assistant Attorney General for the Criminal Division said in February 2010, "the prospect of significant prison sentences for individuals should make clear to every corporate executive, every board member, and every sales agent that we will seek to hold you personally accountable for FCPA violations." *See* http://www.justice.gov/criminal/pr/speeches/2010/02/02-25-10aag-AmericanBarAssosiation.pdf. Since then, Philadelphia-based export company Nexus Technologies Inc., a privately-held corporation, and three of its employees pleaded guilty to bribing Vietnamese officials in exchange for lucrative contracts to supply equipment and technology to Vietnamese government agencies. Nexus' President and owner, as well as two of his siblings, also pleaded guilty to offenses that included FCPA violations. Then, two days after the Nexus announcement, DOJ reported that Innospec, Inc., a publicly-held specialty chemical company and Delaware corporation, pleaded guilty to violating the FCPA and the U.S. embargo against Cuba, and agreed to pay a $14.1 million fine.

DOJ's heightened enforcement has reached such a scale that TIME Magazine recently described the FCPA as "a far-reaching bit of American legislation that cracks down on corporate bribery in all its forms and is rattling the cages of corporate chiefs the world over." K. Stier, *U.S. Cashes In on Corporate Corruption Overseas*, TIME, Apr. 7, 2010, at 1, *available at* http://www.time.com/time/business/article/0,8599,1977526,00.html. This from a statute that traces its roots to sev-

eral cases in the early 1970s involving the fraudulent concealment of illegal corporate campaign contributions in public company books and records. *Report of the Securities and Exchange Commission on Questionable and Illegal Corporate Payments and Practices*, Senate Comm. on Banking, Hous. & Urban Affairs, 94th Cong., 2d. Sess. (Comm. Print 1976).

Focusing solely on the corporate bribery component of the FCPA overlooks its most widely applied section, what securities lawyers call the "books and records" provision, 15 U.S.C. §78m(b), which requires issuers with securities registered with and required to file periodic reports with the SEC to keep books and records that accurately reflect the disposition of the corporation's assets. When a public company files financial statements with the SEC in connection with its periodic reporting obligations or the registration of securities, and those financial statements are false in some material respect, the SEC's civil enforcement actions typically include a violation of the books and records provision. Additionally, where the facts suggest that a public company has violated the FCPA's anti-bribery provisions, but there is insufficient evidence to charge the company under the bribery section, the SEC will bring civil charges for violations of the books and records provision.

The more notable component of the FCPA nevertheless is the anti-bribery provision in section 30A of the Exchange Act, which applies equally to private persons and privately held and publicly held companies and their officers, employees and agents. Specifically, the basic elements of the anti-bribery prohibition of the FCPA are:

- giving, offering or promising to give anything of value
- "corruptly"
- to an officer, employee or agent of a foreign government or international organization, or instrumentality of that government or organization, or a foreign political party
- while knowing that the gift, offer or promise to give is
- for the purpose of influencing or inducing an act or decision, "securing any improper advantage," or "inducing such foreign official to use his influence"
- "in order to assist ... in obtaining or retaining business for or with, or directing business to, any person."

See 15 U.S.C. §§ 78dd-1, 78dd-2. It is important to note that the FCPA applies to acts occurring entirely outside of the United States. As such, the statute confers jurisdiction over the unlawful conduct, eliminating the need to ascertain whether the conduct satisfies the traditional tests for subject matter jurisdiction. The FCPA imposes liability for acts of foreign agents acting on behalf of the "issuer" or "domestic concern." *Id.* § 78dd-2(a).

Moreover, the FCPA defines broadly a "foreign official" as "any officer or employee of a foreign government or any department, agency, or instrumentality [of that government, department or agency], or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization." *Id.* § 78dd-2(h)(2).

The FCPA also provides specific guidance as to what constitutes "knowledge" under the statute. *Id.* §§ 78dd-1(f)(2), 78dd-2(h)(3), 78dd-3(f)(3). The definition of "knowledge" with respect to "conduct, a circumstance or a result" includes actual awareness, recognition of circumstances that may give rise to a result, or a "high probability" of the existence the circumstances required for an offense. *Id.* The term "knowledge" further includes "deliberate ignorance" – that is, a person's conscious decision to avoid learning the truth. *See* H.R. Conf. Rep. No. 100-576, *reprinted in* 1988 U.S.C.C.A.N. at 1952-54. (Congress intended for the FCPA to cover those persons who deliberately choose to ignore evidence of possible FCPA violations -- "both prohibited actions that are taken with 'actual knowledge' of intended results as well as other actions that, while falling short of what the law terms 'positive knowledge,' nevertheless evidence a conscious disregard or deliberate ignorance of known circumstances that should reasonably alert one to the high probability of violations of the Act.")

It is not FCPA enforcement alone that has created a sea change of expectations with respect to corporate compliance. The guilty plea by BAE Systems plc included violations of the Arms Export Control Act ("AECA"), 22 U.S.C. §§ 2751-2799aa-2, and the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Parts 120-30. Other statutes and regulations well within the international enforcement umbrella include the Money Laundering Control Act of 1986, 18 U.S.C. §§ 1956-57; the Trading

with the Enemy Act ("TWEA"), 50 U.S.C. App. §§ 5, 16; the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701--06; the sanctions regulations promulgated pursuant to IEEPA by the Treasury Department's Office of Foreign Asset Controls ("OFAC"), *see* 31 C.F.R. Parts 500-598; the Export Administration Regulations ("EAR"), 15 C.F.R. Parts 730-774; the Foreign Assistance Act, 22 U.S.C. §§ 2151-2431k; the Anti-Boycott Regulations, 15 C.F.R. Part 760; and various sections of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

These statutes and regulations all include civil penalties and fines for violations and most provide criminal sanctions, too. Moreover, the IEEPA Enhancement Act of 2007, Pub. L. No. 110-96, 121 Stat. 1011 (2007), "enhanced" the penalties that companies, their executives, directors, agents, and employees may face for violating IEEPA, the TWEA, EAR, Anti-Boycott regulations and OFAC regulations. Specifically, willful violations of these IEEPA-covered statutes and regulations now may result in criminal penalties of up to $1 million for companies and individuals, as well as imprisonment for up to 20 years for individuals, per count; and civil fines may also be imposed for each violation of up to $250,000 or twice the amount of the transaction that is the basis of the violation, whichever is greater. 50 U.S.C. § 1705.

The potential consequences of FCPA violations are a criminal fine of up to $2 million per violation of the antibribery provisions for a company, and a criminal fine of up to $250,000 per violation and imprisonment for up to five years for an individual. 15 U.S.C. §§ 78dd-2(g), 78dd-3(e), and 78ff(c). Willful violations of the books and records and internal control provisions also can result in criminal fines of up to $25 million for a public company and a criminal fine up to $5 million as well as imprisonment for up to 20 years for responsible corporate officials. 15 U.S.C. § 78ff(a). There also are possible collateral sanctions, including suspension and debarment from government contracting programs for violations of any of these statutes or regulations. *See* DFARS Export-Controlled Items, 75 Fed. Reg. 18,030 (Apr. 8, 2010) (to be codified at 48 C.F.R. § 252.204-7008).

Ignorance and economics are not sources of protection for companies; governance and compliance programs are. The U.S. Sentencing Guidelines applicable to organizations set forth expressly what constitutes an effective compliance and ethics program. *See* U.S.S.G. §8B2.1 (2009) (viewed at http://www.ussc.gov/2009guid/TABCON09.htm). The Principles of Federal Prosecution of Business Organizations governing DOJ (U.S.A.M. 9-28.000, et seq.) ("Corporate Prosecution Principles"), identify one of the factors that prosecutors should consider in determining the proper treatment of a corporate target as "the existence and effectiveness of the corporation's pre-existing compliance program...." U.S.A.M. 9-28.300 (2008). The Comment to the Corporate Prosecution Principles explains what prosecutors examine in evaluating a compliance program:

> While the Department recognizes that no compliance program can ever prevent all criminal activity by a corporation's employees, the critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives. The Department has no formulaic requirements regarding corporate compliance programs. The fundamental questions any prosecutor should ask are: Is the corporation's compliance program well designed? Is the program being applied earnestly and in good faith? Does the corporation's compliance program work? In answering these questions, the prosecutor should consider the comprehensiveness of the compliance program; the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned.

Comment, U.S.A.M. 9-28.800, B. (2008). These standards do not distinguish companies based on whether they are public or non-public, large or small, or particular revenue thresholds.

What then should companies of all sizes do upon discovering a possible violation, particularly one that may subject the corporation or offi-

cers, directors, employees or agents to criminal prosecution? The short answer, although a treatise unto itself, is to conduct an independent corporate investigation. A properly conducted investigation brings the insight of regulators and prosecutors to the analysis, effectively maneuvers the corporate culture, adroitly develops evidence without the benefit of subpoena power, understands the voluntary and compulsory self-disclosure regimes in play, and commands the respect of management, the board and regulators upon presentation of findings and recommendations. The information developed about acts and omissions, evaluated in the context of lawful and ethical conduct, becomes the benchmark for determining what, if any, corrections are necessary or disclosure strategies may be advisable.

In the world of compliance, one size does not and cannot fit all. Since each company faces unique risks, compliance programs must be tailored. Implementing a compliance program in consultation with counsel is a best practice, because management and the directors can discuss the issues under the protection of the attorney-client privilege. If a company constantly is recognizing, addressing, and considering the risks that it confronts, then it should attempt on an ongoing basis to evaluate how to improve its governance systems to reduce its risk exposure. The role of counsel should be to assist a company in the development and administration of a compliance program, not policing the program.

American businesses are motivated to expand overseas, and the President's new National Export Initiative will increase that motivation. Noticeably absent from the Initiative's "Export Promotion Cabinet," however, is the Cabinet official responsible for enforcing criminally the FCPA and the other statutes and regulations affecting international transactions – the Attorney General.

On one hand, the President is encouraging reducing barriers to trade and "tak[ing] steps to improve market access overseas for our manufacturers, farmers, and service providers by actively opening new markets, reducing significant trade barriers, and robustly enforcing our trade agreements." Exec. Order No. 13,534, § 3(g). On the other hand, DOJ, the SEC, and other federal regulators with enforcement jurisdiction over cross-border transactions are watching closely to ensure that there is strict compliance with all federal laws. There is no better way to ensure compliance than to take trade overseas with an effective compliance program in tow.

Mr. Frenkel chairs the Corporate Investigations, Governance and Risk Management and White-Collar Crime practice groups at the Potomac law firm Shulman Rogers. He may be reached at jfrenkel@shulmanrogers.com. Mr. Hoffman chairs Shulman Rogers' Government Contracts and International practice groups. He may be reached at ihoffman@shulmanrogers.com.