Forensic Experts Discuss Key FCPA Issues And Compliance Strategies For The Real World

The Editor interviews Rocco deGrasse, Esq., Principal in KPMG’s Forensic Practice, and Jonathan Zdimal, CPA, Director in KPMG’s Forensic Practice.

Editor: How are companies responding to increased global regulatory coordination and sophistication with regard to anti-bribery and corruption ("ABC") enforcement efforts?

deGrasse: The government’s enforcement efforts certainly have become more sophisticated. The DoJ and SEC, for example, are emphasizing to companies the need for ABC compliance programs to create a control environment that contains an integrated set of “front-end” and “back-end” controls. The former category includes authorization procedures in a variety of contexts – controls that counsel often draft. “Back-end” controls are financial in nature and relate to the expenditures of company assets, including disbursements, reimbursements and sales channel support, such as rebates and discounts. The government is taking an increasingly holistic view of ABC compliance programs, and companies have responded by designing and implementing more comprehensive programs. This is a trend that we expect will continue.

The elements of compliance programs include the design and implementation of standards meant to reduce ABC risk, as well as monitoring of these standards to determine whether they are being followed in practice. In addition to its own monitoring of internal audits, the government increasingly wants to see companies engaged in a continuous monitoring of transactions and, where possible, the use of automation and data analytics to further that effort – a point I believe Jon will discuss in further detail. This monitoring is in addition to the traditional formal monitoring function performed by internal audit departments. Continuous monitoring presents companies with real challenges from an automation perspective; companies will be stepping up efforts to automate and enhance their monitoring capabilities.

Law Firms
Broad Range Of Incentives
For Businesses Are Available
In The Dominican Republic
Ricardo A. Pellerano & Rivera
Page 42


* Supporting Firm

There appears to be a trending interest involving companies seeking innovative ways to incorporate data and analytics into their compliance program initiatives – for example, to support risk assessments or compliance-monitoring-type activities. Data analytics can be a very powerful tool, offering companies a surgical, cost-effective approach, to harvest, query and analyze voluminous amounts of data in a very focused and meaningful manner – all with a view towards identifying potentially anomalous patterns, behaviors or attributes possibly indicative of non-compliance concerns. This in turn helps clients focus valuable time and resources in a more precise, risk-based manner.

In my experience, the regulators are becoming very sophisticated, in the concept that companies (and investigators alike) have access to these cutting-edge techniques to query and analyze considerable amounts of data in compliance and/or investigative settings. I do think there is a continued, but ever-evolving, expectation that companies maintain a comprehensive understanding of their systems and sources of data, including a sound understanding of the capabilities to access, query and evaluate that data in a meaningful way. In this day and age, data and analytics have to be a part of almost any conversation – particularly in the context of compliance-monitoring-type activities or in an investigative setting. In my opinion, there is a growing expectation from the regulators in that regard.

Editor: How do regulatory risks tie in with a company’s industry?

Zdimal: In general, any company operating in a foreign jurisdiction is likely to face some element of FCPA non-compliance risk, meaning its foreign operations likely require some level of government interface. Looking past the more obvious scenario of marketing and selling directly to government-based customers, FCPA-based risk can have a much broader reach, regardless of industry. Risk could undoubtedly stem from normal-course operational activities, such as sourcing, manufacturing, distribution or even cross-border logistics. Brick-and-mortar operations also face FCPA-based risk in the context of constructing and operating facilities – for example, interfacing with environmental boards, licensing and permitting associated with new construction and/or operations, site inspections, and labor considerations, among others. Many clients overlook a common situation of possible heightened risk involving paying taxes in foreign jurisdictions. The course of evaluating and paying taxes in a foreign market, there will likely be some level of interaction with the foreign taxation authorities – whether directly or through use of an intermediary.

Please email the interviewees at rdegrasse@kpmg.com or jzdimal@kpmg.com with questions about this interview.

Please turn to page 59
deGrasse, Zdimal

Continued from page 39

Editor: Which industries have been under scrutiny? Are companies learning from their experiences?

deGrasse: An incomplete list would include defense, high-risk projects, medical device and pharmaceutical industries—all have been the subject of multiple government enforcement actions and prosecutions. I believe there has also been some government scrutiny. Once the government becomes acquainted with the risk profile of a company and the nuances associated with it, the company can begin its evaluation of ABC-related risk and assist in prioritizing compliance and internal audit activities. The mistake companies often make is failing to recognize that this tool is merely the starting point for the risk assessment process. A company not in a recognized high-risk industry consequently may become complacent in creating and maintaining an ABC compliance program. What really drives a risk profile is not the industry per se but rather the government touchpoints within a company: its operations, the quality of its own personnel and its current control environment. Recent developments have shown that FCPA risk can be found in any industry, even industries traditionally deemed to be low risk, such as retail.

Editor: What additional factors affect a company’s FCPA risk profile?

deGrasse: The statute itself obviously is geographically sensitive. Government interactions are dictated not only by the company’s operational footprint but also by jurisdiction, including nuances such as the degree of U.S. governmental objectives and activities by central and local governments. A private transaction in the U.S. may be subject to FCPA in socialized economies because of the extent of business activities across international borders—in some countries, even domestic transport across provincial borders can generate high-risk government interactions.

Companies also need to assess risk exposure in the sales channels, as Jon noted. Companies may need licenses to make sales, and the company’s internal controls may change depending on goods that impact public health or relate to national security. They also need to pay attention to discount and rebate payment procedures as well as to tax incentive and gift card programs that sell to government entities may face significantly heightened ABC risk in dealing with government agencies.

Another factor that determines risk is the sophistication of internal controls and accounting systems and the number of different accounting systems that exist across markets. Multiple systems create significant challenges from a design, implementation and monitoring perspective. An often-overlooked factor is the need to make conscious decisions about the quality of your team on the ground. An experienced team in a high-risk market may help significantly reduce the potential for an ABC risk jurisdiction, while an inexperienced team—or perhaps one with a record of non-compliance—surely will increase risk in a low-risk jurisdiction. Personnel certainly are only one variable in the risk assessment process, but they are an important one that companies sometimes overlook.

Transparency International indices that are designed to be but one arrow in the compliance officer’s quiver.

Editor: What common mistakes do companies make when assessing their corruption-related risk profiles?

deGrasse: We discussed a few of the common mistakes earlier in the interview. An additional error is the failure to differentiate between complacency in markets versus a lack of knowledge of or accountability to the law. Companies often maintain that satisfying external auditors and Sarbanes-Oxley (SOX) requirements demonstrate a low risk—an assumption that reflects a misperception of the nature and scope of audit work, including what is or is not in scope. Such mistakes will not hold up well with regulators, who very well understand the limits of audits and SOX-related efforts and expect more from an effective ABC compliance program.

Another mistake is to rely on the fact that the company is in a “low-risk industry,” which many believe is a disparate indicator. It’s not. We already discussed the dangers of buying a well-designed plan with an effective compliance program, i.e., one that is properly implemented and monitored, and we covered the critical need to ensure that training programs are effective—not simply a “check-the-box” exercise—and really serve to drive implementation.

On a personal level, I am always impressed by how lawyers and accountants/controls specialists differ in their vernacular and approach to compliance matters. Lawyers think of identifying risk activities and proactively addressing and mitigating those risks. They think in terms of reducing risk associated with those activities. Controls specialists focus on the processes in which the ABC risk can exist in a company and design a set of controls to remediate that risk. Both views of course are valid but reflect different perspectives based on the training and skills sets of the respective professions. I have sat in meetings where the lawyers and accountants afterwards approached me separately to ask that I translate into their vernacular what the other side was saying.

Finally, the case law is littered with companies that believed they had an ethical culture, which for most employees was trite. A recent example is what I understand as a challenge with any white collar activity is that it takes just one unethical person to damage its reputation, particularly in the social media age. Having no materiality standard that creates liability for a company improves the sphere of purpose: making this point, the DOJ has taken cases that involve very small amounts. In my former role as an assistant United States attorney in Chicago, our office certainly would have declined such cases, so our thresholds really are higher in today’s environment.

Zdimal: Building on Rocco’s point, the qualitative aspect of an otherwise immaterial financial transaction could be the reason for concern. Apart from assessing quantifiable factors, it is the qualitative aspect of a bribe that matters: the intended and potential benefits to a government official that create the concern from a materiality standpoint. The qualitative aspect of a bribe is generally what puts you in the gray area of FCPA violation—precisely why we are trying to ensure our clients don’t have to engage in something that is not necessarily the quantitative aspect.

Editor: In closing, please summarize the key takeaways of this discussion and talk about KPMG’s role in helping companies with compliance efforts.

deGrasse: The broad point is this: most companies are well aware of their ABC compliance obligations and the price of non-compliance in the U.S. market and beyond. The law is not as big a threat as the regulatory environment and the potential cost of non-compliance. The case law suggests that the U.S. government is more willing to hold individuals responsible for violations. What is less clear is how the government is going to react to FCPA violations by companies. Is this going to be a move to prosecute more companies or is it going to result in increased enforcement of existing laws?

Rocco deGrasse is an Assistant U.S. Attorney who travels worldwide to address FCPA-related issues for clients, including in the due diligence, compliance, internal audit and training arenas. His professional experience includes service as an Assistant United States Attorney in Chicago and Raleigh, North Carolina; he also was a Partner with the law firms of Winston & Strawn and Foley & Lardner, where his practice focused on complex criminal and civil litigation. Mr. deGrasse represents companies ranging from Fortune 10 to mid-market in FCPA investigations and global FCPA compliance projects. He currently serves as KPMG’s global lead partner for a complex and high-profile engagement in a country currently pending before the Department of Justice and Securities and Exchange Commission.

Jonathan Zdimal is a Certified Public Accountant with over 14 years of global forensic accounting and financial statement audit experience across a variety of industries, including diversified industrials, retail, automotive, energy, software & electronics, life sciences and pharmaceutical. Mr. Zdimal currently resides in the area of conducting global investigations into matters involving alleged corruption & bribery and financial reporting related fraud. Mr. Zdimal has provided proactive and reactive investigative advisory services to attorneys, audit committees, corporate management and internal audit functions around the world—including training, risk assessments, program assessments and on-demand investigative response services.