REPRINT

R&C risk & compliance

FCPA CORRUPTION ISSUES FOR GOVERNMENT CONTRACTORS

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2015 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

MILLER CHEVALIER

Miller & Chevalier Chartered

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

www.riskandcompliancemagazine.com

MINI-ROUNDTABLE

FCPA CORRUPTION ISSUES FOR GOVERNMENT CONTRACTORS

PANEL EXPERTS

Jean-Michel Ferat
Managing Director
The Claro Group LLC
T: +1 (202) 800 7536
E: jmferat@theclarogroup.com

Jean-Michel Ferat is a managing director for The Claro Group. Mr Ferat has over 18 years of experience in the specialised fields of forensic accounting and fraud detection. He has taken part in some of the largest and most complex forensic accounting cases in history, including the investigation into the United Nations Oil-for-Food Program, the multi-year investigation of Holocaust-era bank accounts held in Switzerland and the investigation of market manipulation on the Karachi stock exchange in Pakistan. Mr Ferat has performed fraud and corruption investigations in over 20 countries in the context of white collar, FCPA and UK Bribery Act actions.

Marc Alain Bohn
Counsel
Miller & Chevalier Chartered
T: +1 (202) 626 5559
E: mbohn@milchev.com

Marc Alain Bohn focuses on the FCPA and other areas of international corporate compliance, including export controls and economic sanctions. He regularly advises multinational companies on compliance and enforcement matters and has broad experience conducting internal investigations and representing companies before the Department of Justice (DOJ) and Securities and Exchange Commission (SEC). Mr Bohn has worked on several large-scale FCPA investigations and is frequently engaged in due diligence exercises. He has also conducted numerous compliance-focused audits and assessments and regularly assists companies in developing risk-tailored compliance policies and procedures.

Michael B. Schwartz
Principal
KPMG
T: +1 (713) 319 2258
E: mschwartz@kpmg.com

Michael Schwartz is a principal in KPMG LLP's Forensic Advisory Services practice in Houston, Texas. He assists corporate and public sector clients in preventing, detecting and investigating fraud, waste, abuse and other misconduct. Mr Schwartz is the forensic coordinating partner nationally for the public sector and a national leader for anti-bribery and corruption and FCPA-related forensic services. Prior to his 12-year tenure at KPMG, Mr Schwartz had over 20 years of trial and other legal experience as an Assistant United States Attorney, in law firms and corporate legal departments. He is a frequent speaker nationally on fraud, misconduct, FCPA and compliance-related topics.

Gary DiBianco
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
T: +1 (202) 371 7858
E: gary.dibianco@skadden.com

Gary DiBianco represents corporations and their officers, directors and employees in criminal and civil investigations, regulatory matters and complex cross-border proceedings. He has extensive experience defending government inquiries and conducting internal investigations in anti-corruption, fraud, securities and related matters. Mr DiBianco has been involved in a number of significant matters representing US and international entities in a variety of industries and business sectors, including pharmaceuticals and life sciences, oil, gas and mining, financial services, manufacturing and professional services. His experience under the US FCPA, UK Bribery Act and related laws includes global investigations, responses to multinational governmental inquiries and due diligence in connection with corporate transactions.

RC: In what ways has the regulatory risk and compliance landscape for government contractors evolved in recent years?

Schwartz: There are public procurement rules, not just in the US, but throughout the EU and in the rest of the world – certainly in the G20 countries, but almost everywhere there is a government procurement regime. On top of that, because it is an obvious touch point between a commercial organisation and government, either direct or indirect, all of the bribery and corruption concerns that go along with any other 'government as customer' situation are present for government contractors.

Ferat: The enactment of Federal Acquisition Regulation (FAR) clause 52.203-13, 'Contractor Code of Business Conduct and Ethics' has added an increased layer of risk to US government contractors dealing with potential FCPA issues. This clause, required in most government contracts greater than $5m, suggests that to the extent that an FCPA violation becomes known to a government contractor, regardless of materiality, it would arguably be required to disclose the infraction to the government. While non-government contractors usually have the choice – albeit an often difficult one – to self-disclose Foreign Corrupt Practices Act (FCPA) infractions to the government or not, government contractors appear to have much less leeway. In addition, contractors that are subject to oversight by the Defense Contract Audit Agency (DCAA) in particular, have seen an onslaught of increased scrutiny at all stages of the contracting process including bid proposal, ongoing contract execution and project close-out. This increased scrutiny stems from the highly critical 2008 US Government Accountability Office report of the DCAA performance.

DiBianco: Regulatory risk has increased significantly in recent years. The US Department of Justice (DOJ) reports that since 2009, it has convicted more than 50 individuals in FCPA and FCPA-related cases and resolved criminal cases against more than 50 companies with penalties and forfeitures of approximately $3bn. Twenty-five of the cases involving individuals have been brought since in 2013 and 2014, not including ongoing investigations that are not public or are pending and have not been resolved. In addition, many other countries now are joining the United States to actively investigate and bring enforcement actions in the anti-corruption arena. This includes the sharing of information by relevant enforcement authorities. When a government contractor is operating in multiple jurisdictions, cross-border investigations by

enforcement authorities in all applicable jurisdictions is a possibility.

Bohn: Although many aspects of government contracting remain fairly protected, global trade barriers to foreign competition for government procurement have gradually reduced to the point where government contractors who once serviced only domestic government markets can now serve foreign markets as well. In the FCPA context, this leads to more potential interaction with 'foreign officials' and the attendant compliance exposure that brings. While for many years the US government market was the largest draw for US and non-US companies alike, more recently, particularly in the face of domestic spending cuts, US government contractors have begun relying on non-US governments for a larger share of their business. At the same time, more and more countries have joined the fight against transnational bribery, and global cooperation among enforcement agencies is trending. As a result, government contractors who are looking to replace lost domestic business by turning to non-US markets will face a heightened enforcement environment, both under the FCPA and the anti-corruption laws in the other countries in which they operate.

RC: How would you describe monitoring and enforcement activity aimed at cracking down on corporate corruption?

Are more resources being devoted to FCPA related investigations?

Ferat: The FCPA was enacted in 1977 but remained largely out of focus by regulators until the mid-2000s. The 2005 investigation into the United Nations Oil-for-Food program, a significant catalyst in ramping up the US government's interest in foreign corruption cases, reported thousands of instances of companies paying kickbacks to the Iraqi regime, a large number of which fell within US jurisdiction. In 2010, the DOJ was quoted as saying "As our track record over the last year makes clear, we are in a new era of FCPA enforcement; and we are here to stay". Indeed, the time period between 2010 and today saw over 200 enforcement actions by US DOJ and the Securities and Exchange Commission (SEC) against both corporations and individuals alike, and significant fines included the $398m levied against Total and $152m levied against Weatherford. The consequence of this continued enforcement zeal has been the significant costs borne by companies for both reactive investigations as well as the implementation of proactive compliance measures. As an extreme example, the total outside consultant cost of the Walmart internal investigation has exceeded $450m in two years. While arguably an anomaly, it is generally accepted that medium and large sized companies requiring reactive investigations going back a number of years will

likely be on the hook for tens of millions of dollars in investigative costs.

Bohn: It is clear that there are more government resources being focused on uncovering and prosecuting corporate corruption today than in years past, but that is not all. It is the way those resources are now being marshalled and leveraged that should draw the attention of government contractors, from the Dodd-Frank whistleblower program, which is producing more than 3000 tips year in and year out, many of which are FCPA-related, to an unprecedented level of collaboration and coordination between the US government and enforcement agencies in other countries. Such multi-jurisdictional investigations are now a fixture of the global anti-corruption enforcement effort. This is a development which has greatly magnified the resources at the DOJ and SEC's disposal. One should not mistake the recent drop in resolved FCPA enforcement actions for a drop in investigative activity. On the contrary, efforts to track the level of FCPA-related investigative activity by the DOJ and SEC indicate that the number of new investigations being initiated by the agencies each year remains at near record highs.

DiBianco: Enforcement activity continues to ramp up both in the United States and abroad. While actual settled enforcement actions by the US against companies has held relatively steady over the last couple of years, there are a significant number of investigations in the pipeline that have been publicly reported. Enforcement actions against individuals have increased substantially. Moreover, US enforcement authorities have announced publicly that they are devoting additional resources to enforcement activities and also changing the manner in which cases are investigated. For example, more cases now involve use of law enforcement resources, including FBI agents. Moreover, enforcement authorities have publicly said that they now are handling corruption cases much like they approached street crime investigations in the 1980s, through the use of confidential informants, wire taps and body wires. An example of this approach can be seen in the recently publicised prosecutions of former officers of Petro Tiger.

Schwartz: The guidance has converged, whether it is guidance from the DOJ or SEC in the US, adequate procedures guidance from the UK Ministry of Justice, or information published by the UN, the Organization for Economic Cooperation and Development (OECD), the International Chamber of Commerce, the World Bank, or any number of other organisations. The guidance is clear that there should be attention focused on monitoring all sorts of elements of your bribery and corruption compliance program. This includes ensuring that training occurs for the right people on the right schedule. It includes monitoring gift and

entertainment policies for clients – if, for example, pre-approval is required, it means actually going in and testing whether pre-approvals were both sought and obtained. Whether that monitoring is done by a compliance organisation, an outside consultant or by internal audit, the key is that the monitoring occurs so that non-compliance can be detected and remediated before there is a problem. So, the regulator's expectation is that you pay attention to your program and make sure it is properly functioning and implemented. We did a survey on behalf of a specific client in a particular industry that wanted to benchmark the resources they were devoting to bribery and corruption compliance with a peer-group of organisations within the same industry and with a similar global footprint. It was interesting because I am not sure we actually found a correlation between revenue and the amount of budget for a compliance program. But they all had one thing in common: they absolutely wanted to avoid, and were spending money proactively on avoiding, misconduct because they knew that the cost of an investigation would be remarkably high. At the corporate level it is less about investigative resources and more about monitoring and proactive compliance resources, with the ability to follow up on certain kinds of allegations.

RC: To what extent do FCPA issues take on heightened importance for government contractors? Are any particular types of government contract more susceptible to FCPA risk?

> **"Being a government contractor means that you are also subject to a governmental audit at some level, which is another touch point that organisations in other industry do not necessarily have to worry about."**
>
> *Michael B. Schwartz, KPMG*

Bohn: DOJ investigations that result in criminal convictions expose US government contractors to debarment – that is, they run the risk of losing their eligibility to compete for US government contracts. This means that when negotiating settlements with the DOJ in particular, government contractors have a tremendous incentive to agree to the implementation of corrective actions and remedial measures that will serve the dual purpose of demonstrating present responsibility and persuading

debarment officials that debarment is not necessary. Many other countries and international organisations have similar debarment policies. So, when viewed in the debarment context, FCPA issues are of critical importance to all government contractors. For example, Canada's Department of Public Works and Government Services is reportedly contemplating the imposition of a 10 year ban on Hewlett-Packard entering into any contracts with the Canadian government following a guilty plea by the company's Russian subsidiary on FCPA-related charges in April 2014. It is also worth mentioning that there are FCPA risks associated with the US government's foreign military sales program. This program provides various forms of security assistance to foreign countries and international organisations, ranging from the sale of defence articles and services, to humanitarian and disaster assistance, to international military training and nation building efforts to name just a few. Participation in these programs can pose particular compliance risks, especially for contractors who previously have focused principally on domestic government procurement opportunities and have not prepared themselves to deal with the risk of FCPA violations by educating themselves on their anti-corruption obligations and implementing compliance programs.

Schwartz: By definition, government contractors are dealing with the government as a customer, so there is no question about those touch points being more typically direct as opposed to indirect. But government contractors may be part of a consortium and may lack the ability to control all the touch points. They may be a minority partner or a joint venture partner, and even if they have a sound compliance program, the venture they are part of may not for one reason or another. Then there are typical issues such as goods being exported or imported, and the usual government touch points associated with that, such as licences and permits. Government contractors engage in lobbying activity as much as most industries do. Being a government contractor means that you are also subject to a governmental audit at some level, which is another touch point that organisations in other industry do not necessarily have to worry about. In terms of particular kinds of government contracts, they are all high risk in the sense that they are dealing with government, but historically the military and defence contractors have been a focal point. If we look at the distant past of the FCPA, there were any number of defence contractors that were part of the original round of FCPA enforcement in the late 1970s and early 1980s. That repeated itself in the UK three or four years ago with another government contractor that was UK based but whose shares traded in the US. There was the infamous US government sting several years ago that involved firearms and the armaments business, which again has many government customers. Any type of government contractor or contractor is at risk when you ask the

question whether there might be some circumstance that could create some incentive for somebody to do something improper to obtain or retain business by paying a bribe.

DiBianco: An FCPA violation takes on heightened importance to government contractors because a violation can lead to possible debarment in government contracting. Early detection of issues is important, as it provides the company some flexibility in deciding whether to voluntarily disclose the potential violation to regulators before the regulator may learn of it through other sources, like a whistleblower. DOJ guidance states that a voluntary disclosure can earn the company credit for cooperating and allow for an opportunity to resolve the matter in a manner that potentially may avoid debarment. In terms of the types of government contracts that are more susceptible to FCPA risk, Transparency International maintains a list of jurisdictions by perceived corruption risk. Any contracts that may involve operations or activities in perceived higher risk jurisdictions are inherently more susceptible to FCPA risk. Moreover, any contracts that involve the use of third-party representatives, consultants or agents similarly are more susceptible to FCPA risk.

Ferat: The recent increase in the volume of government contracts being performed in foreign locations, many affiliated with the military and development efforts in both Iraq and Afghanistan, poses increased risk related to FCPA compliance. Companies are often challenged when operating in these and other high-risk countries for a number of reasons, including that the solicitation and payment of bribes is commonplace, that transactions are often undertaken on a cash basis, and that companies often must rely on local sales agents, distributors, subcontractors or other third party representatives to fulfil contracts. Arguably, government contractors have a significantly heightened risk than non-government contractors for failure to abide by the FCPA. The most significant risk would be suspension or debarment from future government contracts, which, for a large government contractor, could mean hundreds of millions if not billions of dollars. Other potential risks to government contractors could include the loss of government grants, subsidies, loans, government licences, security clearances and parallel debarment from other organisations such as the World Bank.

RC: Have there been any notable FCPA violations involving government contractors in the last 12-18 months? What lessons can we draw from the outcome of these cases?

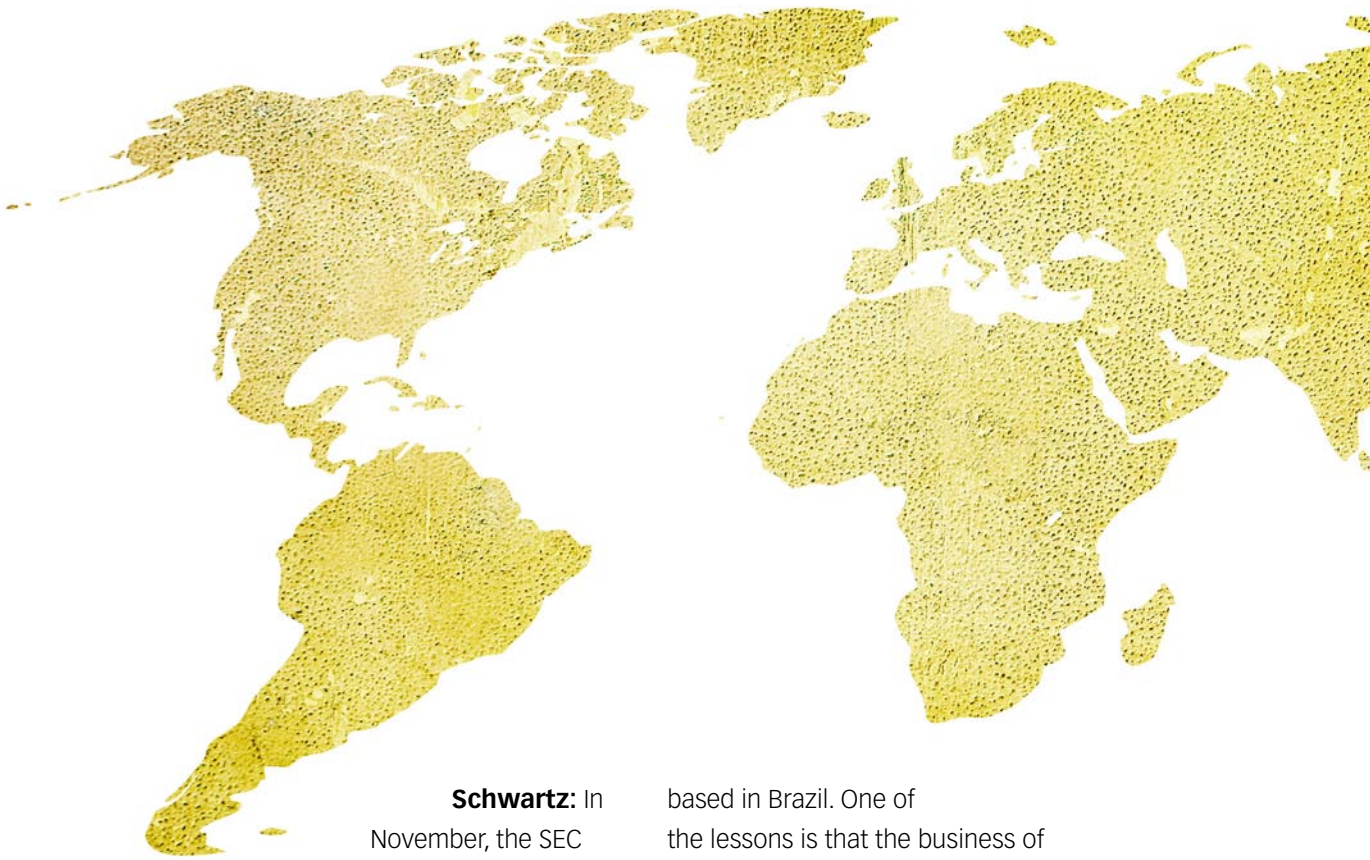
DiBianco: Two recent settlements involved conduct by third-party intermediaries in multiple jurisdictions. In December 2013, Archer Daniels

Midland (ADM) resolved allegations of improper payments in connection with conduct of an indirect subsidiary in the Ukraine and a joint venture partner in Venezuela. The ADM entities paid a combined total of approximately $54m to the DOJ and the SEC to resolve the allegations. The resolution involved a plea agreement with the Ukraine entity, a non-prosecution agreement with ADM, and a civil complaint. The DOJ press release noted the voluntary and timely disclosure of the conduct and ADM's extensive cooperation. Similarly, in April 2014, Hewlett-Packard Company resolved allegations of improper payments in Russia, Poland and Mexico and three of its subsidiaries agreed to pay a combined total just over $108m to the DOJ and the SEC. The HP resolution involved a guilty plea by the HP Russia subsidiary, a deferred prosecution agreement for the HP Polish subsidiary, a non-prosecution agreement for the HP Mexican subsidiary, and an SEC cease and desist order against HP. There were no criminal charges against the parent entity. Both of these resolutions demonstrate the high risk posed by third parties and the flexibility and creativity that can go into structuring long-running, multi-country investigations.

Ferat: Recent FCPA enforcement actions or resolutions against US government contractors include IBM, Alcoa, H-P, Weatherford and ADM, among others. Perhaps more important than the specific fact patterns of these cases, two significant revelations have changed the landscape dramatically for government contractors. The first is the Eleventh Circuit's opinion in *U.S. v. Esquenazi* in which the courts took great care in defining a 'foreign official', and, more particularly, an 'instrumentality' of a foreign government. The courts laid out a number of considerations as to what defines an instrumentality and causes more entities and individuals to be potentially deemed 'foreign officials'. The second, and more significant, is the government's recent trend toward seeking plea deals. Until recently, the government has been content to secure non-prosecution agreements and deferred prosecution agreements from offending parties. On top of

> **"An FCPA violation takes on heightened importance to government contractors because a violation can lead to possible debarment in government contracting."**
>
> *Gary DiBianco, Skadden, Arps, Slate, Meagher & Flom LLP*

reputational and other collateral harm resulting from a guilty plea, government contractors will take particular note of one effect of a guilty plea – possible debarment from government procurement programs.



Schwartz: In November, the SEC imposed financial penalties against two individuals who worked for a US-based defence contractor and who paid for worldwide travel for government officials in Saudi Arabia. Over the past several years, the US DOJ entered into a deferred prosecution agreement with BAE Systems, based in the UK and according to published reports, is currently investigating Embraer, based in Brazil. One of the lessons is that the business of many government contractors is global. Government contractors may find themselves being investigated in multiple countries for similar conduct, and be

subject to serial investigations or prosecutions in different countries for the same conduct.

Bohn: Because the FCPA is focused on the bribery of public officials for the purpose of obtaining or retaining business, it should not be surprising that the majority of FCPA enforcement actions involve improper efforts to secure contracts from foreign governments, including government-owned or controlled entities. Since mid-2013, the DOJ and SEC have brought 17 enforcement actions against nine companies over alleged misconduct in their efforts to secure government contracts, imposing more than $880m worth of fines, disgorgement and pre-judgment interest. In each of these cases, the agencies claimed that compliance was an afterthought for the companies involved — that these companies had either failed to put in place adequate compliance policies from the outset or failed to effectively implement paper programs. These cases make clear that no company should be soliciting government contracts abroad without first implementing a comprehensive compliance program to guard against corruption risk.

RC: What is your advice to government contractors on effectively managing FCPA risk in the course of conducting business around the world?

Schwartz: Conducting business around the world leads to an immediate realisation that it's not just the FCPA or the UK Bribery Act – there are 41 other countries that have adopted legislation based on the OECD Convention that criminalises the bribery of foreign government officials. While enforcement activity is not present in all those countries, it

certainly leads to an immediate discussion about not just complying with the UK Bribery Act or the FCPA, but having to worry about complying with local law and understanding that a violation in one country may trigger two or three or even four other government investigations in other countries, depending on the facts. What that leads to is understanding what adequate procedures are, taking into account all of the guidance, and spending considerable time on prevention and detection so a company doesn't find itself in a situation of responding to an allegation of bribery and corruption. This gets back to monitoring and training, hiring the right people and tone at the top, internal audit or other parts of the organisation playing a role in monitoring and testing that policies and procedures are in fact being followed. It also means understanding your indirect touch points, such as using agents, distributors or other third parties to interact with government on your behalf, and understanding the obligation to conduct due diligence and know who those people are, and monitoring what they are doing so they don't get you into trouble from a bribery and corruption standpoint.

Bohn: The key to effective management of FCPA risk by government contractors is for these companies to triage their compliance efforts and focus on those activities, partners, customers and countries that present the highest risk. While there is no 'one-size-fits-all' program when it comes to compliance, contractors should seek to implement a well-constructed program that helps to prevent, detect and remediate misconduct. Beyond this, methods of effectively managing risk may include, among other things, consistent compliance messaging from the top of the organisation, the implementation of 'checks and balances' to enable the monitoring of critical transactions and establish control over financial resources, tailored compliance training for both employees and key third parties and the undertaking of risk-based compliance audits.

> **"Third-party contractors and external consultants are a continuing challenge for any business interfacing with foreign officials and government controlled entities."**
>
> *Jean-Michel Ferat, The Claro Group LLC*

Ferat: The advice is simple: design a robust compliance program that is appropriate for the size and risk profile of your organisation and make sure that the program is operating effectively by

updating it and testing it on an ongoing basis. Some guidance on designing an effective compliance program is available from several sources including the US Sentencing Guidelines 'Seven Elements of an Effective Compliance Program', the OECD's 'Good Practice Guidance on Internal Controls, Ethics, and Compliance' and perhaps most importantly the US DOJ and SEC through their joint issued 'Guidance' document released in 2012. A read of all of these sources suggests that a successful program is rooted in five main areas: firstly, establishing tone at the top, secondly, performing risk assessments on an annual basis, thirdly, establishing sufficient and effective standards and internal controls, fourthly, undertaking organisation-wide training and communication, and finally, performing effective audit, monitoring and response.

DiBianco: A key element to ensuring that a compliance program is appropriately detecting and preventing anti-corruption issues is ongoing auditing, monitoring and risk assessments. These efforts will aid in identification of any gaps in the program and also allow the government contractor to ensure its program is addressing any new risks that may develop. The government contractor should prioritise its efforts based on the risk profiles of the jurisdictions where it conducts business and where it generates its largest volumes of revenues. In addition, a robust tone at the top is crucial to ensuring that all officers, directors, employees, agents and other third parties understand what the government contractor expects in terms of ethical conduct. At the end of the day, the key is to get everyone to embrace the concept that compliance is everyone's responsibility.

RC: What potential exposures under the FCPA do government contractors face when dealing with third-parties or engaging external consultants, for example? How can they mitigate or avoid these risks?

Ferat: Third-party contractors and external consultants are a continuing challenge for any business interfacing with foreign officials and government controlled entities. Companies have been largely unsuccessful when mounting a defence based on the premise that misdeeds were conducted by a consultant or a third-party, unbeknownst to the company. Regulators have been very consistent in asserting that a company is obligated to know how the individuals or entities working on behalf of the company are conducting business. In 2012, the DOJ noted that Merrill Lynch would not be held criminally liable for the behaviour of an employee that acted outside the scope of his authority and concealed his illicit activity from his employer. Earlier this year, the DOJ chose not to pursue Bechtel Corporation on similar grounds. In each instance, the DOJ made special mention

of the companies' control environments, deeming them sufficiently robust to reasonably deter and detect. The Merrill Lynch and Bechtel cases involved employees of a company. While we can draw some inferences from these cases, it is not clear whether the DOJ and SEC's standards would be similar for a third-party agent. What is clear is that use of a third-party agent does not alleviate a company from its duties under the FCPA. To the contrary, a third-party agent may require heightened compliance activity, especially in instances where the third-party is used because of advantageous connections to foreign officials. Accordingly, due diligence, robust record-keeping of both financial transactions and due diligence activities and communication and acknowledgement of a company's anti-corruption policies are crucial.

DiBianco: Third-parties and external consultants create great risk if not properly selected, retained and managed. The DOJ has brought a number of cases holding companies responsible for the activities of third parties and external consultants they have engaged as if they were employees or agents. In terms of mitigating risk, government contractors should thoroughly screen and train their third parties and consultants and utilise written contracts with robust compliance representations and warranties, audit rights and termination rights. It also is vitally important that the government contractor actively oversees the activities of the third parties and external consultants. This includes understanding what the third parties and external consultants are doing on the company's behalf. One mechanism to achieve visibility into the activities of third parties is to require periodic written reports from the third parties that detail what work they have performed and how they have performed it.

Schwartz: Virtually all the bribery and corruption statutes around the world will create exposure and liability whether the conduct occurs directly by a company employee or indirectly through an agent or authorised representative, or even a service provider who is doing things for the commercial benefit of the ultimate client or the company. Understanding that another organisation or its employees can create huge problems is a key first step for some companies. In this day and age, with at least a 10 year history of vigorous FCPA enforcement, I would hope most companies do understand that, but there may be some who fall back on traditional principles of agency and think that they are not responsible for the conduct of third parties – but clearly in the bribery and corruption world, companies are. That leads to how you manage those third party relationships. First, on-boarding those third parties means determining whether you really need them, and contracting with them in a way that makes it clear that you have certain expectations around their compliance, either with the company's policies or comparable policies. Some organisations even train

third parties. Some require periodic certifications. Some even exercise right to audit clauses to actually go in and examine financial transactions that are viewed as higher risk, such as gifts, entertainment, commission payments, fines or penalties, and make sure that funds are not going directly or indirectly to government officials in any illicit way.

Bohn: Government contractors routinely hire third parties for a variety of legitimate purposes, including to provide valuable expertise or to assist in commercially challenging locations, but these engagements can also expose contractors to significant liability if the third parties retained act corruptly in violation of the FCPA. In fact, over 80 percent of FCPA enforcement actions in recent years have involved the use of third party intermediaries of some type. Beyond the fines, disgorgement and additional obligations typically associated with such settlements, these FCPA violations can have additional implications for government contractors, particularly where external consultants have been engaged. Most prominent is the potential for False Claims Act liability. Many foreign military sales programs are funded under US government contracts, which exposes a contractor who falsifies records of payments to subcontractors or consultants in order to disguise bribes to civil actions for false claims by the government and by whistleblowers. To mitigate the risks associated with the use of third parties, government contractors should conduct meaningful due diligence prior to engaging third parties and then closely monitor the relationships thereafter. As part of this, one simple step a company can take to dramatically reduce its risk exposure is to limit the number of intermediaries on which it relies by requiring employees to select from a list of third parties that have been vetted and approved.

> **"To mitigate the risks associated with the use of third parties, government contractors should conduct meaningful due diligence prior to engaging third parties and then closely monitor the relationships thereafter."**
>
> *Marc Alain Bohn, Miller & Chevalier Chartered*

RC: How important is it for government contractors to update, improve and maintain their FCPA compliance program, and ensure employees are on board? What steps should they take to achieve this?

Bohn: Government regulators expect compliance programs to be dynamic and to evolve along with a company's business, applicable law and best practices in the industry in question. Because of how fast the business and legal landscapes for a company can change, what constituted an effective compliance program even five years ago would not necessarily pass muster with the DOJ and SEC today. The agencies recognise that no compliance program can anticipate and prevent all forms of misconduct, but where weaknesses in a company's program are identified, they expect a company to enhance its internal policies to address those deficiencies. Accordingly, the DOJ and SEC may interpret the failure of a company to adapt its internal policies to meet emerging risks as a sign of an ineffective 'paper' compliance program, which the agencies might argue violates the FCPA's internal controls provision. One way in which government contractors can ensure that their compliance programs are not becoming stale is by periodically conducting compliance assessments. These assessments will help to determine the effectiveness of a company's internal policies and will enable them to enhancing those policies where appropriate.

DiBianco: It is important that FCPA compliance programs are updated and improved on an ongoing basis. A compliance program should not be static and consist merely of policies and procedures. Rather, the program should be dynamic and constantly evolving to mitigate risks as they arise and which can change over time. An integral part of a dynamic and evolving program is ensuring that employees understand the expectations the company has set, which can be achieved through ongoing training and communications. The more robust the program, the better it is at early detection and prevention potentially improper conduct. Early detection is key and allows the company flexibility to decide if a voluntary disclosure is appropriate. There have been many cases where early detection and voluntary disclosure has led to declinations or less severe enforcement actions by regulators.

Ferat: FCPA compliance programs are living things that must be updated and tweaked as organisations enter new markets, gain new customers and encounter new risks. An organisation's employees and third party representatives are at the frontlines of the interface with foreign officials and those employees and agents must be on board with FCPA compliance. It is critical that organisations establish proper tone at the top and that boards and upper management communicate the importance of FCPA compliance throughout the organisation. Proper and ongoing training is critical, in particular of foreign employees who may not be as intimately familiar with the requirements of the Act and the repercussions to both the organisation and them individually if compliance is not adhered to. The cost of proactive FCPA compliance is not cheap,

however such costs typically pale in comparison to the financial and reputational cost of a government enforcement action.

Schwartz: It is critical that organisations periodically update their programs, both generally and based on any lessons learned. If, for example, a company receives a hotline call, in some ways it's a good thing that an employee has used the mechanisms the company has made available to report possible misconduct related to bribery and corruption or another topic. But, whatever the investigation shows, there may be opportunities for improvement, at the controls level, or at the policy and procedures level. The organisation should be getting the benefit of feedback and lessons learned from internal investigations, from what's happening with competitors or others in similar situations, from internal audit findings, and feed those back, not just in terms of tightening or modifying or making controls more effective, but also taking a look at their overall policies and procedures and making sure they are staying current. The reason why all of that is important is that no compliance program is foolproof and no government will expect the company to forever prevent fraud, misconduct and bribery. It is possible incidents will arise even with the best compliance program. But it's critical to be able to explain to the government the lengths that any organisation went to, to try and prevent the incident, and how its response was first-rate. There are precedents here. The government, at least in the US, declined to prosecute Morgan Stanley because it was able to document the lengths it went to in an attempt to prevent the problem in the first place, trained the individual employee who was alleged to have paid a bribe multiple times, according to the government's press release, and did everything it could. Notwithstanding that, there was still a problem, but the company was able to present the employee as a proverbial rogue employee and the government declined the case. That's plenty of incentive to try and do the right thing from a compliance standpoint. R&C