EMERGING ISSUES IN FCPA ENFORCEMENT
March 9, 2018

Working Effectively with Forensic Accountants

Moderator:
James Tillen, Vice Chair International Department, Miller & Chevalier

Speakers:
Jean-Michel Ferat, Senior Managing Director, Ankura Consulting Group, LLC
Frances Mcleod, Founding Partner, Forensic Risk Alliance
Tamika Tremaglio, Principal, Deloitte
Collaborating with accountants

Relationship between lawyers and accountants can be critical to the success of independent investigations.

By Carl H. Loewenson Jr. and David L. Stulb
SPECIAL TO THE NATIONAL LAW JOURNAL

"ACCOUNTING CONCEPTS are a foreign language to some lawyers in almost all cases, and to almost all lawyers in some cases." United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961). It is no surprise that as investigations of corporate fraud continue to dominate the news, attorneys seek to work alongside forensic accounting "interpreters" during independent investigations to gain a better understanding of this foreign language of accounting. The working relationship between accountants and attorneys can be critical to the success of any investigation. The current regulatory environment has also placed even more emphasis on providing corporate clients and other stakeholders an expeditious, independent and thorough investigation.

What is becoming a staple of every investigation is addressing other stakeholders of the investigation, including the company's outside counsel, the external auditors, federal prosecutors, state attorneys general (and not just New York Attorney General Eliot Spitzer), the Securities and Exchange Commission (SEC), self-regulatory organizations such as the New York Stock Exchange and National Association of Securities Dealers, creditors, rating agencies and plaintiffs' lawyers. Parallel proceedings are becoming more prevalent and place a premium on the need to coordinate a well-executed response on behalf of the company from the investigative team of lawyers and accountants.

This article will discuss the increasing importance of developing a team approach to attorney and forensic-accountant collaborations during an independent investigation and will identify some keys to a successful joint effort. The article also will examine the mounting scrutiny investigators face regarding their independence, scope of work and timing.

Before engaging a forensic accountant to assist in an investigation, a company should give careful consideration to the independence of the accounting firm. It used to be that a law firm could use the company's usual auditors—perhaps with the forensic team walled off from the audit team—to assist in the internal investigation. No longer. Not only would such dual use of the accounting firm not conform to current best practices in our post-Enron world, it would most likely violate federal law.

The consensus lesson from Enron likewise makes it unwise to have the company's primary outside law firm—particularly one that was involved in any of the matters under investigation—conduct the internal inquiry.

Sec. 201 (a) of the Sarbanes-Oxley Act of 2002 expressly prohibits any registered public accounting firm that performs an audit for a company from providing "contemporaneously with the audit, any non-audit service, including...legal services and expert services unrelated to the audit" for that same company. An audit firm may provide other nonaudit services, such as forensic accounting, provided that the client company's audit committee approves in advance. However, in order to maintain the integrity and objectivity of the investigation and to comply with Sarbanes-Oxley, an accounting firm that performed an audit for the company should not participate in an investigation of wrongdoing at that same company.

Forensic accountants

Once independence has been confirmed and the decision to engage a forensic accountant has been made, counsel must take necessary precautions to protect the privileges applicable to communications between counsel and the accountants. Communications with an accountant "made in confidence for the purpose of obtaining legal advice from the lawyer" are privileged. United
States v. Kovel, 296 F.2d at 922. Given that litigation of some sort—against the SEC, the United States, a state or three, class action plaintiffs or derivative plaintiffs—is a near certainty during and after a forensic accounting investigation, the documents prepared by the accountants should be considered protected attorney work product, prepared in anticipation of litigation.

In order to best preserve any existing attorney-client privilege or work-product immunity, outside counsel rather than the company should engage the forensic accountants. Any document prepared by the forensic accountants in connection with the investigation should carry the header, "Privileged and Confidential Document Prepared at the Request of Counsel," in order to maintain confidentiality and any applicable privilege.

From the beginning of the collaboration, it is imperative that the accountants and the attorneys work together as a team through each phase of the investigation. As soon as practically possible, the team should determine the scope of the problem that is the focus of the investigation. Regular team meetings discussing developments in the investigation are a staple of an effective investigation. Integrated e-mail distribution lists facilitate rapid communication of developing evidence and theories to all relevant members of the combined legal-accounting team and keep everyone up to date between regularly scheduled face-to-face meetings.

Once the nature of the problem has been identified, the team should develop an action plan that clearly defines the scope and goals of the investigation and delegates responsibility. For example, the forensic accountants may be assigned responsibility for analyzing financial statements, financial documents, accounts and accounting statements; determining pecuniary loss or gain; testing the efficacy of compliance programs; and conducting a comprehensive review of electronic files. The attorneys, on the other hand, will be responsible for legal analysis, determination of individual culpability and for serving as the key point of contact with the authorities. The action plan is a fluid document subject to change as the investigation proceeds and more information is uncovered.

One recurring theme in internal investigations is that the nature of the investigation evolves as it proceeds. It is the rare investigation that does not present major surprises along the way. The investigating team has to balance the need for focus and efficiency with the need for acute peripheral vision and resulting flexibility. The engagement letter between the investigating lawyers and their client—usually the company, or the audit committee or a special committee of the board—can and should list the primary areas of inquiry, but also should make clear that the investigation will go wherever the evidence leads. Otherwise, an investigation of restricted scope will garner little credibility with the many audiences who view the product of the investigation.

Document collection and review is a critical and often time-consuming part of any internal investigation. The forensic accountant typically plays an integral part in this process by interacting with the company's information technology professionals to gain a full understanding of the company's computer network, including servers, remote access capabilities, retention policies and storage capacities.

The preparation of a memorandum by the accountants detailing the nature of the search and the protocols used in the search is an invaluable tool if, and when, a government investigation begins, because the memorandum provides a road map of the search scope. It is also a wise defensive move to keep meticulous records of the document search and retention, given the prevalence of investigations of the investigation, the government's aggressive prosecution of obstruction of justice and the broadly worded obstruction prohibition (18 U.S.C. 1519) added by Sarbanes-Oxley.

**Employee interviews**

Employee interviews serve as one of the most effective information-gathering devices in the internal investigation and usually form the core of the investigation. The information gathered from the document review is used to prepare for employee interviews. Counsel and accountants should determine which employees need to be interviewed and whether to begin by interviewing lower-level employees and then work through to senior managers or vice versa.

Often it is appropriate to start with the employees who were most centrally involved in the conduct under investigation: e.g., the chief financial officer, the controller and the accounts receivable supervisor who made key adjustments to revenue at the end of seven successive quarters, with the intention of returning to these same individuals near the end of the investigation. The collaborative effort should continue with the preparation of an outline for each employee to be interviewed, covering the items identified in the action plan and developed
during document review.

The accountants should take the lead in preparing outlines for employees who are closely involved with the company's accounting processes, while the lawyers can focus on remaining employees and the directors and top officers. The interview outlines drafted by the accountants should be edited by the lawyers, and vice versa. At least one accountant and one lawyer should be present for every interview, with the lawyer taking the lead on questioning, except when the accounting issues are arcane. The accountants should also review and edit the interview memoranda summarizing the interview. The lawyers generally, but not always, draft such memoranda.

In addition to conducting formal interviews, accountants can work closely with company accounting personnel to develop an understanding of the accounting procedures at the company. It is not unusual for forensic accountants to establish and maintain a constant presence at the company's offices during an investigation to learn the nature of the operations firsthand. Often counsel for the investigation, counsel for the outside auditors and counsel for the company's accountants can develop guidelines that will permit open communication among the company's accountants, the forensic accountants and members of the audit team, but stop short of a formal interview of a company accountant or outside auditor.

Written reports

If the client decides that it would like a written report summarizing the findings of the investigation, the lawyers and accountants will again need to work closely together to draft the report in a timely, concise and coherent manner. The team should prepare an outline of the report in the early stages of the investigation in order to give further structure and definition to the investigation. The report should contain a description of the circumstances giving rise to the investigation and the scope of the investigation, the identities of the persons interviewed, the sources of documents, an executive summary, a discussion of the background facts if necessary, an analysis of the accounting controls and corporate governance, a summary of individual conduct and culpability and remedial measures and recommendations. From the start, the accountants should take the lead in drafting specific sections that focus on accounting issues.

Investigative reports typically must cover a wide range of issues and evidence. They must be prepared on a breakneck schedule. Given these exigencies, it usually makes sense to assign various chapters of the report to separate authors. It often works well to have one lawyer and one accountant bear joint responsibility for drafting a particular chapter of the report. If a particular chapter or part of a chapter delves deeply into accounting data or literature, then the accountant should take the laboring oar. Counsel and the accountants should both play a part in any communication with the client, stakeholders and governmental agencies. Regular updates regarding the status of the investigation, the names of employees to be interviewed and who have been interviewed, preliminary findings and other matters relating to the scope of the investigation can be effectively communicated by the joint lawyer-accountant team.

While the lawyer should serve as the primary contact with the government, the lead forensic accountant should be a regular participant in meetings with the government, especially to address any accounting issues that may arise during meetings.

Preserving the privilege

The company will face enormous pressure to disclose the substance of the investigation to third parties, particularly government agencies. Protecting and perhaps waiving the attorney-client privilege and work-product immunity are critical issues that can arise in any accounting investigation. The Department of Justice and SEC each have formal policies that strongly encourage companies to cooperate with governmental investigations, including the waiving of privilege by providing investigatory reports and even interview notes to authorities. The Department of Justice says that it will consider a company's "willingness to cooperate in investigation of its agents, including if necessary, the waiver of the corporate attorney-client and work product protection," when deciding whether to bring criminal charges. See www.usdoj.gov/dag/cfft/corporate_guidelines.htm.

Coordination of the efforts of the investigative team is critical to the overall success of the investigation. One cannot overestimate the importance of the attorneys and forensic accountants working closely together on interviews, strategy and findings. It is through this collaboration that the mysteries of the foreign language of accounting can be interpreted and understood.
Conducting FCPA Internal Investigations: A Practical Guide for Forensic Accountants and Investigators

By Mark Winston, Vijay Sampath, and Jamal Ahmad

1. Introduction

Major corporations have recently witnessed a flurry of Foreign Corrupt Practices Act (FCPA or “the Act”) investigations. A review of the numerous decisions reached by the Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) shows the imposition of stringent penalties for violations of this statute. When an internal investigation is commenced by a corporation (by management or audit committee or board of directors) when it has reason to believe that a potential FCPA violation has occurred or to defend itself against allegations of foreign bribery, either in-house or outside counsel are appointed to conduct an internal investigation. Forensic accountants and investigators play an important role in assisting counsel in this undertaking.

FCPA internal investigations are complex – both legally and factually – and challenging. This is primarily due to the wide reach of the FCPA given the myriad of international issues and considerations that it raises in terms of diverse legal frameworks, business practices, political environments, etc. Consulting firms with a global presence and offering multidisciplinary services such as forensic accounting, business intelligence, and forensic technology are well suited for performing such investigations.

This article provides a roadmap that will facilitate forensic accountants and investigators to design procedures to assist in conducting FCPA internal investigations. Section 2.I briefly addresses the provisions of the FCPA. Section 2.II provides examples of indicators of risk areas that will help in uncovering activities or transactions with FCPA implications. Section 2.III describes specific forensic accounting procedures that will be useful in planning and conducting the investigation.

2. Discussion

I. Provisions of the FCPA

In 1977, Congress enacted the FCPA as part of the Securities Exchange Act of 1934 in an attempt to put an end to the bribery of foreign government and quasi-government officials by U.S. corporations and to restore confidence in the integrity of the American business system. The Act contains two types of substantive provisions: (1) anti-bribery, and (2) accounting provisions. The FCPA provides criminal and civil penalties for violations of the anti-bribery and/or accounting provisions by companies and individuals. Violations of the anti-bribery provisions are enforced by the DOJ whereas the SEC generally enforces the accounting provisions.

---

1 Examples of notable recent FCPA investigations conducted by the DOJ and/or SEC include Halliburton, Bristol-Myers, Amerada Hess, ChevronTexaco, ExxonMobil, Marathon, DaimlerChrysler, Titan Corporation, Monsanto and ABB, an affiliate of KPMG.
2 15 U.S.C. §§ 78m (b), 78dd-1, -2, 3 and 78ff.
(i) **Anti-bribery Provisions**

The FCPA prohibits U.S. companies, their subsidiaries, as well as their officers, directors, employees, and agents from using the U.S. mail system or any other instrumentality of interstate commerce (i.e., bank check) to make payments or offer anything of value to foreign government officials for the purpose of obtaining or retaining business for or with, or directing business to, any person.\(^3\) The anti-bribery provisions apply to "issuers,"\(^4\) "domestic concerns"\(^5\) regardless of where and how the prohibited act is performed.\(^6\)

Since 1998, foreign nationals and corporations are also subject to the FCPA to the extent they perform a prohibited act anywhere in the world in furtherance of a bribe while in the United States or its territories. The Act also prohibits payments, authorizations, promises or offers to any other person if there is knowledge that any portion of the payment is to be passed along to a foreign official or foreign political party, official or candidate for a prohibited purpose.\(^7\)

Thus, FCPA internal investigations involve a search for actual or objective intent—a key element in determining whether payments were made for purposes of obtaining or retaining business.

(ii) **Accounting Provisions**

Put simply, the accounting provisions\(^8\) require U.S. issuers and all of their majority-owned U.S. and non-U.S. subsidiaries to (a) make and keep books and records which provide, in reasonable detail, an accurate and fair reflection of the underlying transactions and disposition of assets, and (b) devise and maintain an adequate system of internal accounting controls.\(^9\) To comply with the books and records provision, issuers must maintain their books in accordance with Generally Accepted Accounting Principles ("GAAP").\(^10\)

In addition, the Act requires that a company make a good faith effort to ensure that any company (including joint ventures) in which the U.S. company or one of its subsidiaries holds fifty (50) percent or less of the voting power comply with the FCPA accounting provisions.\(^11\) No criminal liability is inflicted for inadvertent errors however it is imposed only when a person knowingly circumvents or knowingly fails to implement a system of internal controls or knowingly falsifies a book, record, or account.\(^12\)

---

\(^3\) Id. at §78 dd-1(a).
\(^4\) An issuer is any corporation that has issued securities registered on an U.S. exchange. §78(c)(8).
\(^5\) A domestic concern is a citizen, national or resident of the United States, or a corporation with its principal place of business in the United States. §78dd-2(h)(1).
\(^6\) The 1998 amendments to the Act extend jurisdiction to issuers and domestic concerns for such acts committed outside the United States irrespective of the use of the mail or interstate instrumentalities.
\(^7\) Knowledge is defined very broadly and is present when one has actual knowledge or has substantial certainty that a payment is certain or likely to occur. Since 1998, knowledge can be established through proof of conscious disregard of an event or being willfully blind of the results. §§78dd-1(f) (2), -2(h) (3, -3(f) (3).
\(^8\) §78m (b)(2).
\(^9\) Although not specifically defined by the Act, best practices generally define an adequate system of internal controls as one accepted by the Committee of Sponsoring Organizations ("COSO") of the Treadway Commission.
\(^11\) §78m (b)(6).
\(^12\) §78m (b)(5)
(iii) **Safe Harbors - Permissible Payments and Affirmative Defenses**

The FCPA permits "facilitating" or "grease" payments to foreign officials for routine government actions.\(^\text{13}\) Specifically, payments to "expedite or to secure the performance of a routine governmental action" are permitted as long as the payments are not used to encourage a foreign official to award new business to or continue business with a particular party. Examples include: obtaining permits, licenses, or documents that are needed to do business in a foreign country; processing governmental papers, such as visas and work orders; scheduling inspections; providing police protection; and mail pick-up or delivery.

Furthermore, the Act provides two affirmative defenses: (1) the payments are legal in the country in which they are made, and (2) the payments are considered "reasonable and bonafide expenditures." The first defense permits "payment, gift, offer or promise of anything of value" to a foreign official, a political party, or a candidate's country, provided that such offerings are in accordance with the written laws of that country. In order to prevail under the second defense, the expenditure must be "directly related" to either to the promotion, demonstration, or explanation of products and services, or to the execution or performance of a contract with a foreign government or agency.\(^\text{14}\)

**II. Indicators of FCPA Risks**

FCPA internal investigations are fact-specific in nature; at times, they could become exercises in finding “needle(s) in the haystack.” In order to unearth activities or transactions that present risks from a FCPA perspective, focus should be placed on relevant risk indicators.

In addition, risk assessments should be conducted and forensic accounting and investigation techniques should be designed to largely focus on these indicators. The DOJ also provides examples of such indicators, which it terms as “red flags.”\(^\text{15}\) Examples include:

- Whether due diligence/background checks were performed in selecting agents;\(^\text{16}\)
- Apparent lack of qualifications or resources on part of the agent to perform the services offered;
- Whether the agent has been recommended by an official of the potential governmental customer;
- History of corruption in countries the company does business that Transparency International\(^\text{17}\) has determined to be highly susceptible to corruption;
- Decentralized operations;

\(^\text{13}\) §78dd-1(b), (f)(3)(A); -2(h)(4)(A); -3(f)(4)(A).
\(^\text{14}\) §78dd-1(c)(2)(A)-B; -2(c)(2)(A)-(B); -3(c)(2)(A)-(B).
\(^\text{15}\) See, DOJ Website for Publication “Foreign Corrupt Practices Act Antibribery Provisions”.
\(^\text{16}\) Also included within the agent designation would be consultants, distributors, expediters, representatives, joint venture partners and other third parties paid to assist the company in government dealings.
\(^\text{17}\) Transparency International ("TI") is a Berlin based organization with local chapters established worldwide aimed with the goal of fighting corruption. TI brings together relevant players from government, civil society, business and the media to promote transparency in elections, in public administration, in procurement and in business. As part of its mission, TI publishes annually a list known as the TI Corruptions Perceptions Index which ranks the world’s most corrupt nations based on the opinions of business people and country analysts that it surveys. If an FCPA investigation involves transactions in multiple countries, a country’s rank on the TI Index would help in prioritizing the transactions to be investigated.
• Unusual payment patterns (e.g., round currency payments made on weekends and holidays) or financial arrangements (e.g., payments for office overhead);
• “Above market” commissions paid in the ordinary course of business and lack of proper authorization of such commissions;
• Diverse commission rates paid to distributors for the same product;
• Unusually high management fees, gifts and entertainment expenses;
• Requests for payments inconsistent with the terms or purposes of underlying agreements;
• Indirect payment requests by agents; including payments (a) to other third parties, (b) to off-shore or unnumbered bank accounts, (c) to bank accounts not in the business partner’s name, (d) for invoices that do not reflect actual services performed by the business partner;
• Checks made out to "cash" or to “bearer”;
• Presence of off-the-book accounts (e.g., inter-company accounts not recorded at affiliate level);
• Lack of standard invoices; and,
• Lack of transparency in expenses or accounting records.

III. Forensic Accounting Procedures

FCPA internal investigations are similar to other forensic investigations in many respects, including characteristics, usage of tools, requirement of skills, and performance of procedures. The scope is different in that FCPA investigations are centered on finding bribe payments to foreign officials.

An FCPA investigation largely involves an in-depth review of disbursements made by an entity or others acting on its behalf. Accordingly, one of the preliminary and important tasks to perform is to develop a work program that identifies the areas within the entity likely to be susceptible to FCPA risk (i.e., accounts from which bribe payments might be made or recorded) as well as detailing the steps to be undertaken during the engagement. The steps or procedures usually fall under the following categories: forensic accounting, business intelligence, and forensic technology. It would be worth noting that these procedures are intrinsically linked, and, therefore, may be approached in a different order and/or simultaneously. Notwithstanding the unvarying significance of all the three types of procedures, business intelligence and forensic technology techniques are beyond the purview of this article.

The two critical forensic accounting techniques involve (i) an analysis of those documents and accounting information that may be relevant and (ii) interviews of employees who may be in a position to provide information regarding the matters at issue. The purpose of these components would be to reconstruct a transaction or series of transactions. Potential FCPA violations generally occur in contracting, sales or procurement processes. Therefore, special emphasis should be placed on analyzing customers, vendors, agents, cash and bank, payroll, and general ledger accounts. Also, it would be crucial to check the appropriateness of how any improper activity may have been reflected in the financial statements.

1. Customers

Identify all transactions and associated contracts with foreign government entities in effect at any time in the period. With respect to each contract:
• Review all correspondence in relation to the tender, award, performance, variations in terms or payment for each contract to ensure that contracts were awarded on a fair basis and not as the result of bid rigging. Compare actual performance to the contract terms, the government’s normal tendering procedures and normal commercial practice in order to identify any potential irregularities. Seek explanations for any irregularities found.
• Analyze the money flowing to/from the government entity according to the contract/correspondence and reconcile them to the purchase/sales ledgers, cash book and bank statement. Review supporting documentation to determine the reason for the payments and seek explanations for any irregularities.
• Draw up a list of the decision makers in each government entity and agents acting for them in relation to the contract and their companies.

2. Vendors

Based upon inquiries and business intelligence findings isolate from the vendor list, vendors that are government officials or have other relationships to government-controlled entities, political parties or similar relationships. Seek to confirm that vendors actually exist and that they performed services or received goods in exchange for the payments. Examine payment histories for such vendors for any irregularities. Also, determine whether due diligence was conducted on them, and, if so, the extent of the review. Trace the payments through to the payment ledger, cash book, purchase ledger, inventory records, and bank statements. Other procedures will include, to the extent possible:

• Identification of round currency disbursements
• Duplicate payments
• Duplicate vendors (same address)
• Vendors with P.O. Box addresses
• Sporadic payments (e.g., significant payment every few months)

Conduct additional investigation following discovery of unusual payments or vendor characteristics. Seek explanations for any irregularities and/or lack of information.

Similarly, review all licenses and permits obtained from vendors to ensure that they are legitimate, necessary and in compliance with the Act. Determine if a payment of a fee was required for the license or permit and if one was required, ensure that payment was made directly to the government entity and not the official. If no payment was recorded, determine the reason for same. Finally, confirm that no item of value was given to any government official to obtain the license/permit. If an item of value was given ensure that it was nominal and otherwise permissible by the Act.

3. Agents, Intermediaries and Consultants

With respect to agents, examine the nature of the company-agent relationships taking into account factors that may present risks of bribe payments as explained in Section III of this article. Additional factors to consider would include:

18 The vendor designation includes suppliers, distributors, facilitators, and third parties providing similar services.
• Whether there are written, signed contracts, sub-contracts or agreements with any government entity or instrumentality or with any company in which a foreign government official has an interest (as principal, owner or employee) thus requiring compliance with the FCPA;
• Whether the agent agreements prohibit assignment;
• Whether the agency agreements are in compliance with local laws and reviewed and approved by company counsel;
• Whether any agents are specifically responsible for government contracts, and whether any of those agents are former government officials or are related to government officials;
• Level of detail provided in agent invoices, whether commissions/discounts/rebates are properly calculated and whether the invoices agree with the terms of the agency agreement;
• Whether commissions for government contracts are higher compared to those paid for other contracts;
• The nature of the agent’s reputation in the business community; and
• Follow-up on all red flags noted during the due diligence conducted of agents such as:
  ▪ The agent’s refusal to expressly certify compliance with the FCPA;
  ▪ The agent’s insistence that his/her identity not be disclosed;
  ▪ The agent has family or business ties to a government official.

Where money has been paid to or received from agents or there have been other types of commission transactions or payments analyze those transactions and reconcile them to the purchase/sales ledgers, cash book and bank statements. Place particular emphasis on lump sum amounts paid and amounts charged for travel and entertainment that appear to be excessive. Review the supporting documentation to determine the reason for the payments. Seek explanations for any irregularities and/or lack of information.

4. Cash Book/Bank Statements/Petty Cash/Expense Reports

Identify all bank accounts operated by the company. For each bank account, document the account number, bank address, date of opening of account, signatories/power of attorney.

Review the cash book/bank statements/petty cash/expense reports to identify:

• All marketing/travel/entertainment/sundry/gifts/political contributions or lobbying expenses and donations that are not adequately explained and supported;
• All payments to agents not already reviewed (if any);
• All payments to decision makers in the government entities (if any);

Review the supporting documentation to determine the reasonableness, adequacy and reason for the payments, and whether proper approvals were obtained. Reconcile these to the cash book and bank statements. Similarly, review all gifts made to government officials to ensure that they are permitted by local law and thus covered by the safe harbor provisions of the Act.19

---

19 The DOJ has provided some guidance in FCPA Rev. Proc. Release no. 81-1 as to what constitutes valid gifts but the reader is cautioned that the guidelines are limited to that specific case.
5. Payroll

Review the current salary of all employees to confirm that the recipients all have a position and telephone extension in the company. If practicable, review payroll and related documentation to identify any employees who may have opted out of benefits (e.g., medical plans, savings, etc.) Also compare the names to the list of the decision makers in each government entity and their agents to see if the surnames are the same.

Review all bonuses or other employment related payments to employees to ensure that they are reasonable in nature. Review the details of any employee who left during the period.

An often overlooked area in FCPA investigations is whether proper amounts of income tax are withheld from payroll payments. Generally the absence of income tax withholdings or the failure to withhold appropriate amounts needs to be investigated to ascertain that nothing of value has been offered to individuals in violation of the Act. As such, review payroll records for income tax deductions and remittance of the same with the appropriate authorities.

6. General Ledger

Review general ledger to confirm that no receipts or payments have been booked directly that relate to government officials, government-controlled entities, political parties, tax and/or corporate safe-havens or other similar relationships. Where any such transactions have been booked to the general ledger, subject them to the analyses set out above.

3. Conclusion

After reviewing relevant documents and interviewing personnel, linking the evidence together and summarizing findings is akin to putting together a jigsaw puzzle. For example, if results from business intelligence procedures show connections of a particular vendor to foreign officials, sales information obtained from the sales department, contract and due diligence information from legal, accounting and payment information from accounting, and information gleaned from witness testimony would have to be pieced together to ascertain the facts and circumstances surrounding the transaction(s) in question.

A memorandum memorializing the underlying facts and circumstances would be extremely beneficial to the management or the board or the audit committee in determining an appropriate course of action. As part of the memorandum, it would be helpful if any identified internal control weaknesses are reported and recommendations are proposed to correct affected aspects of the operations. As always, follow necessary cues from counsel in drafting such a memorandum.

In sum, today’s global economy requires U.S. companies to do business in foreign countries and in doing so, they often times enlist the services of joint venture partners or other agents, consultants or principals. As a result of these relationships, companies listed in the United States should be aware of the extensive requirements of the FCPA. The core of FCPA internal investigations is to determine whether payments were made to foreign officials to obtain or retain business. Ultimately, apart from criminal and civil liabilities that may result, companies are encouraged to take prescriptive measures such as establishing robust FCPA compliance programs in order to minimize similar occurrences in the future.
About the Authors

Mark Winston, JD is a Managing Director, Vijay Sampath, CPA, CA is a Senior Director, and Jamal Ahmad, JD, CPA is a Director in the Financial Advisory & Litigation Consulting practice (FALCON) at Aon Consulting Inc. They have extensive experience in investigating Foreign Corrupt Practices Act violations. They can be reached in New York at (212) 441-1864, (212) 441-2038 and (212) 441-1694 respectively.
Culture is often thought of as a soft issue because companies struggle to measure its effectiveness. But culture and compliance are linked.

In an FCPA context, for example, compliance failures frequently flow from the erosion of ethical behavior and robust corporate governance.

So why isn’t culture reviewed with the same principles and rigor that are used to test other aspects of compliance programs?

Some companies believe one-time employee survey asking about cultural perceptions is sufficient. These surveys are typically done when new leadership is appointed, or immediately after an issue has arisen. And they only provide one data point at one point in time.

So how do we measure culture? The methodology should utilize multiple tools over various points in time.

For example:

*Employee Surveys*: Anonymous surveys are an effective way to measure company culture. Done correctly, companies can gain important insight into employee perspective, beliefs, and even practices when it comes to behavior driven by culture. However, questions need to be phrased in a way that they'll produce the most accurate responses. Leading questions tend to influence the reader to choose the "right" answer, rather than an honest answer, therefore creating bias.

Surveys -- conducted periodically or after changes or enhancements to compliance programs -- can ask the same questions rephrased differently. This allows companies to
compare results for consistency around the topic and continuous monitoring and testing of culture.

**In-Person Feedback:** Employee focus groups can add a valuable data point of culture measurement. Employees to provide their perspective, beliefs, and concerns around ethical behavior. In this setting, anonymity is unavailable. So the environment for groups of peers needs to help them feel comfortable so they'll provide honest answers. Groups that consist of different role levels and competencies will provide a broader view on beliefs and perceptions.

For focus groups, relatively short notice periods to participants helps avoid prepared feedback, especially in more hierarchical or societies the pressure to give the “right” answers can compromise the data gathered. Developing topics for discussion that elicit these types of assurances is crucial to receive honest responses.

**Assessing Your Leaders:** Replacing leaders within a company that has undergone an FCPA enforcement action is often seen as a remediation effort. But what assurances are there that new leaders will convey the right messaging and change the compliance culture?

Companies seeking to remediate compliance issues should develop an assessment tool to better understand leadership’s values with respect to compliance and ethics. In addition, the assessment tool should weigh the desired values and styles and compare and measure them versus commercial interests, including profitability, time and resource constraints and business development. This assessment should be outsourced to an independent expert who specializes in behavior and leadership values analysis.

**Find out what others think of you:** Clients and key business partners such as banks avoid companies known for unethical behavior. Although this might be a problem of guilt by association, most organizations are anxious to protect their own reputations. That's why it's important to gauge public perception about your ethical culture and how you work with clients. Ways to measure this include simple media searches, client surveys, and even focus groups, depending on your type of organization.

_____  

Frances McLeod, pictured above, is a founding partner of FRA and head of its U.S. offices. FRA provides multi-jurisdictional expertise in financial and electronic forensics to help companies manage risks. She holds a Master’s degree from Wadham College, Oxford and speaks English, German, French, and Mandarin Chinese.

Article originally appeared on The FCPA Blog (http://www.fcpablog.com/).  
See website for complete article licensing information.
Frances McLeod on data transfer compliance: It's time to become GDPR aware

By Frances McLeod | Tuesday, August 22, 2017 at 8:02AM

Companies are increasingly frustrated by privacy protection laws that vary from country to country. But the European Union’s new General Data Protection Regulation (GDPR), which becomes law on May 25, 2018, eliminates much of the confusion with a uniform code for all EU nations.

But with more severe restrictions and greater penalties for violations, the GDPR creates its own brand of frustration.

The eDiscovery required to get the information needed to respond to investigations is going to take on a great deal more complexity; fines for violating privacy regulations could run as high as four percent of an organization’s annual worldwide turnover or up to €20 million ($23.5 million).

While the United States has driven enforcement of anti-corruption and bribery laws since the 1998 expansion of the anti-bribery provisions of the Foreign Corrupt Practices Act, regulations on data privacy are far more restrictive overseas, increasing the challenges of transferring data for defending against allegations of corruption.

At least in part, history is at fault.

EU nations that have survived totalitarian regimes -- Germany, Spain, Eastern European nations -- are prone to be especially protective of individual privacy rights. The GDPR responds to those concerns, requiring organizations worldwide that store or process EU data -- both data stored in the EU as well as “belonging” to EU nationals -- to diligently protect personal information and prove how they do so, including how data is used, how it is stored and who has access.

Nations outside the EU are tightening data protection laws as well: There are a further 21 laws in other European countries or jurisdictions, and many others have enacted or are considering data protection legislation, such as Malaysia, Mexico, India, Peru, South Africa and even Qatar.
While there is no single solution to protect a company against violation of data privacy regulations around the world, international companies operating in a regulated environment should have a defined policy for responding to a regulatory subpoena.

As specialists on trans-jurisdictional data privacy and data transfer, we recommend:

- **Develop and implement a clear data strategy.**

- **Data map before collecting data.** Decide on the data to be considered, identify the jurisdiction where it resides, and determine the applicable privacy regulations in that jurisdiction and what clearances are required and from what agency.

- **Keep, process and review data in its jurisdiction of origin.**

- **Think strategically about what data you bring in and how you bring it in.** Consider how this might be viewed by an EU judge in future years -- both enforcement appetites around GDPR and the U.S.-EU Privacy Shield are as yet completely untested.

- **Be conservative.** The regulations are complex and can result in additional unintended consequences. For example, once data is transferred into the United States, it is generally discoverable for litigation purposes, in civil matters as well as by US government agencies.

- **Comply with the data policy of the jurisdiction and minimize what you transfer.** Ensure you are preserving the rights of those whose data you are using, that they give informed consent -- i.e., that they are informed of what and why you're collecting and agree to such collection, are given the right to exclude personal data and or assured that such data will be culled prior to production, and assured that the use of any data produced to regulators will be restricted to a specified purpose.

- **In each jurisdiction engage counsel with data protection expertise.**

- **Use predictive coding software to avoid sharing personal data inadvertently -- comfort can be obtained by the use of machine learning rather than human review to exclude personal data.**

Brexit in the UK and the current inclination to relax privacy protections in the United States in the name of national security add uncertainty to the use and transfer of personal data.
from the EU and other jurisdictions with data privacy regulations in responding to anti-corruption investigations.

Still, organizations operating internationally should become GDPR aware and, ultimately compliant, to assure themselves the best line of defense and avoid the increasingly real risk of penalties associated with personal privacy law violations.

Frances McLeod is a founding partner of Forensic Risk Alliance (FRA). The firm supports a variety of compliance monitors, advises on trans-jurisdictional data privacy and data transfer issues, and has electronic discovery expertise that augments their forensic accounting and data analytics skills.
THE EUROPEAN, MIDDLE EASTERN AND AFRICAN INVESTIGATIONS REVIEW 2017

Published by Global Investigations Review in association with

AlixPartners
Boies Schiller Flexner
Clifford Chance
Debevoise & Plimpton LLP
Dechert LLP
ELIG, Attorneys–at–Law
Forensic Risk Alliance
Kobre & Kim
Kulkov, Kolotilov & Partners
Niederer Kraft & Frey Ltd
Paul Hastings
Sofunde, Osakwe, Ogundipe & Belgore
White & Case LLP
Willkie Farr & Gallagher (UK) LLP
WilmerHale

© Law Business Research 2017
The Geopolitics of Data Transfer: What Do Companies Need to Consider in a Post-Trump, Brexit and GDPR World?

Weng Yee Ng and Jimmy Ko
Forensic Risk Alliance

Introduction
The last few years have seen some significant developments in data privacy regulation in Europe, the Middle East and Africa (EMEA). These have included: the repeal of Safe Harbor and the introduction of the Privacy Shield, the approval of the General Data Protection Regulation (GDPR) by the European Parliament, the passing of generally applicable data protection law by the Qatari government, and the appointment of South Africa’s first members of the Information Regulator to monitor and enforce provisions of the Protection of Personal Information Act (POPIA). It is fair to say that, with the advancement of and reliance on technology to conduct cross-border business, there will be no relaxation in data protection laws.

To add further uncertainty and complexity to the current regulatory environment, recent disruptive geopolitical developments, such as Brexit and the election of Donald Trump to the US Presidency, will inevitably further highlight conflicts of law and add complexity to the issue of data transfers, especially in the context of investigations and disputes – and, by extension, e-discovery. Because regulatory investigations and related processes frequently span several years, strategic decisions made today around data transfers will have important ramifications down the line. Will the UK establish adequate data protection for a post-Brexit Union? Will President Trump ride roughshod over EU surveillance concerns?

The existence, and the robustness, of established data protection laws globally varies significantly from one jurisdiction to another. In this article, we will provide an overview of key data privacy regulations covered by the Judicial Redress Act, which along with the Attorney General’s list became law in February 2017.

Expanded territorial reach
The new regulation is no longer limited to data controllers and processors within the EU. Instead, those whose processing activities are following closely any changes in the US that might have an effect on Europeans’ data protection rights. ‘For example, one could imagine a scenario where the Attorney General, Jeff Sessions, could decide at a later date to revoke some countries’ – or the EU’s – designations under the Judicial Redress Act: a decision that would wreak immediate havoc on the Shield.

The GDPR, which was approved by the European Parliament in April 2016, with an enforcement date of 25 May 2018 preserves the core principles and the Adequacy Criteria of the Directive,1 which prohibited the transfer of personal data to non-EU countries that do not have an ‘adequate’ level of privacy protection. To bridge the gap of jurisdiction to another. In this article, we will provide an overview of key data privacy regulations covered by the Judicial Redress Act, which along with the Attorney General’s list became law in February 2017.

In 1995, the European Commission (EC) issued a Directive,1 which prohibits the transfer of personal data to non-EU countries that do not have an ‘adequate’ level of privacy protection. To bridge the differences in approach to data privacy and to provide a mechanism to enable the free transfer of data between Europe and the US, the US-EU Safe Harbour Framework (Safe Harbour) was developed, and had been in place for the past 15 years. Since then, with the increasing internationalisation of business and related data flows across borders, the EC recognised the lack of consistent safeguards around data privacy between member states and therefore proposed introducing true consistency via the GDPR. About a year after the EC began to draft the GDPR in 2012, Edward Snowden leaked information about the extent of the NSA’s mass surveillance and data collection practices, and almost concurrently an investigation into Facebook’s European privacy practices was launched by the Irish data protection watchdog. In such an environment it was almost inevitable that the European Court of Justice review the ‘adequacy’ criteria of data protection in the US. The results of that review led to the Safe Harbour Framework being invalidated in October 2015,2 leaving corporates in a state of uncertainty around data protection and data transfer for months while an alternative mechanism was developed. The result was the development of the EU-US and Swiss-US Privacy Shield (Shield), which, after much debate, eventually came into force in July 2016, with the intent to provide more accountability and oversight over data protection privacy. The initial reactions to earlier drafts of the Shield were sceptical. Max Schrems, the European privacy campaigner and lawyer who was instrumental in getting Safe Harbor struck down tweeted: ‘#PrivacyShield: They put ten layers of lipstick on a pig but I doubt the Court&DPAs suddenly want to cuddle with it pic.twitter.com/gfkMexCruh’.3

And while US and EU officials have since described the Shield as ‘a framework that protects privacy and creates certainty’ and provides assurances that ‘any access to personal data for law enforcement or national security is limited to what is necessary and proportionate’,4 the Shield remains untested in court and is therefore vulnerable to future legal challenges.

In addition, there are clearly questions around the viability of the Shield under the Trump administration, as the EC is currently conducting an assessment of the agreement (see 7 April 2017 issue of GHR ‘Privacy Shield in Jeopardy under Trump’). Further, a recent Trump executive order (EO) to ‘exclude persons who are not United States citizens…from the protections of the Privacy Act…’ directly opposes the spirit of the Shield, as does another key consideration: the Attorney General’s designation of specific countries that are covered by the Judicial Redress Act, which along with the Attorney General’s designation became law in February 2017.

In response to the EO and the Act, EU officials commented: ‘We will continue to monitor the implementation of both instruments and are following closely any changes in the US that might have an effect on Europeans’ data protection rights.’ For example, one could imagine a scenario where the Attorney General, Jeff Sessions, could decide at a later date to revoke some countries’ – or the EU’s – designations under the Judicial Redress Act: a decision that would wreak immediate havoc on the Shield.

The GDPR, which was approved by the European Parliament in April 2016, with an enforcement date of 25 May 2018 preserves the core principles and the Adequacy Criteria of the Directive, but additionally expanded certain areas (set out below), as well as outlining hefty fines and penalties.

Evolving privacy protection across EMEA – Is it enough?

Europe
In 1995, the European Commission (EC) issued a Directive,1 which prohibited the transfer of personal data to non-EU countries that do not have an ‘adequate’ level of privacy protection. To bridge the differences in approach to data privacy and to provide a mechanism to enable the free transfer of data between Europe and the US, the US-EU Safe Harbour Framework (Safe Harbour) was developed, and had been in place for the past 15 years. Since then, with the increasing internationalisation of business and related data flows across borders, the EC recognised the lack of consistent safeguards around data privacy between member states and therefore proposed introducing true consistency via the GDPR. About a year after the EC began to draft the GDPR in 2012, Edward Snowden leaked information about the extent of the NSA’s mass surveillance and data collection practices, and almost concurrently an investigation into Facebook’s European privacy practices was launched by the Irish data protection watchdog. In such an environment it was almost inevitable that the European Court of Justice review the ‘adequacy’ criteria of data protection in the US. The results of that review led to the Safe Harbour Framework being invalidated in October 2015,2 leaving corporates in a state of uncertainty around data protection and data transfer for months while an alternative mechanism was developed. The result was the development of the EU-US and Swiss-US Privacy Shield (Shield), which, after much debate, eventually came into force in July 2016, with the intent to provide more accountability and oversight over data protection privacy. The initial reactions to earlier drafts of the Shield were sceptical. Max Schrems, the European privacy campaigner and lawyer who was instrumental in getting Safe Harbor struck down tweeted: ‘#PrivacyShield: They put ten layers of lipstick on a pig but I doubt the Court&DPAs suddenly want to cuddle with it pic.twitter.com/gfkMexCruh’.3

And while US and EU officials have since described the Shield as ‘a framework that protects privacy and creates certainty’ and provides assurances that ‘any access to personal data for law enforcement or national security is limited to what is necessary and proportionate’,4 the Shield remains untested in court and is therefore vulnerable to future legal challenges.

In addition, there are clearly questions around the viability of the Shield under the Trump administration, as the EC is currently conducting an assessment of the agreement (see 7 April 2017 issue of GHR ‘Privacy Shield in Jeopardy under Trump’). Further, a recent Trump executive order (EO) to ‘exclude persons who are not United States citizens…from the protections of the Privacy Act…’ directly opposes the spirit of the Shield, as does another key consideration: the Attorney General’s designation of specific countries that are covered by the Judicial Redress Act, which along with the Attorney General’s list became law in February 2017.

In response to the EO and the Act, EU officials commented: ‘We will continue to monitor the implementation of both instruments and are following closely any changes in the US that might have an effect on Europeans’ data protection rights.’ For example, one could imagine a scenario where the Attorney General, Jeff Sessions, could decide at a later date to revoke some countries’ – or the EU’s – designations under the Judicial Redress Act: a decision that would wreak immediate havoc on the Shield.

The GDPR, which was approved by the European Parliament in April 2016, with an enforcement date of 25 May 2018 preserves the core principles and the Adequacy Criteria of the Directive, but additionally expanded certain areas (set out below), as well as outlining hefty fines and penalties.

Expanded territorial reach
The new regulation is no longer limited to data controllers and processors within the EU. Instead, those whose processing activities are following closely any changes in the US that might have an effect on Europeans’ data protection rights. ‘For example, one could imagine a scenario where the Attorney General, Jeff Sessions, could decide at a later date to revoke some countries’ – or the EU’s – designations under the Judicial Redress Act: a decision that would wreak immediate havoc on the Shield.

The GDPR, which was approved by the European Parliament in April 2016, with an enforcement date of 25 May 2018 preserves the core principles and the Adequacy Criteria of the Directive, but additionally expanded certain areas (set out below), as well as outlining hefty fines and penalties.

Expanded territorial reach
The new regulation is no longer limited to data controllers and processors within the EU. Instead, those whose processing activities related to the provision of goods or services to, or monitoring the behaviour of EU data subjects, will require the appointment of a representative within the EU.
**Consent**
A data subject’s consent to process their personal data is required to be as easily withdrawn as it is granted. Data subjects will be able to withdraw consent to their data being processed.

**International transfers risk awareness**
Although the GDPR removes self-assessment as a basis for transfer, the consent derogation has undergone some changes. Data subjects are required to be adequately informed of the risk of transferring data outside of the EU.

**Breach notification**
Data controllers are required to report most data breaches to the new Data Protection Authority, where possible, within 72 hours of awareness, together with appropriate justification.

**Fines and penalty**
Unlike previous regulations, the GDPR introduced a tiered penalty approach for breaches, where fines for breaches are much higher than under previous regulations, ie, up to 4 per cent of annual worldwide turnover or €20 million.

Based on these changes alone, it is clear that the GDPR will introduce significant undertakings and potential risks for all parties affected, from concerned subjects, to oversight bodies and corporations with a nexus to the EU.

**What about Brexit?**
And then, there is Brexit. The Independent reported that Brexit will see ‘1,000 new laws passed unilaterally and without parliamentary scrutiny when European law is transposed into British law under the Great Repeal Bill.’ What will the new UK data privacy regulation look like? Will it be less stringent than the GDPR? How high will the fines be? All we can do is wait for a new UK-specific data privacy regulation to be introduced to find out. We can, however, begin to imagine the risks.

In a post Brexit world, companies with operations in the UK may be particularly vulnerable to the uncertainties arising from the GDPR. It would appear that the current UK government’s stance on privacy leans towards deregulation. The UK, however, will still need to abide by the GDPR in the period between May 2018 and when article 50 completes its cycle (expected to be by March 2019), regardless of the UK’s future data privacy aspirations.

To add to the complexity, there will also have to be consideration of how to handle UK–US data transfer. If the UK administration decides to opt out of the GDPR following Brexit, the US and the UK could create a unique environment for data transfers. The obligations, however, under the Regulation for UK businesses operating in Europe would remain alongside the need to demonstrate an adequate (ie, comparably robust) data privacy environment. A UK–US mechanism would be highly unlikely to satisfy such obligations. This scenario poses the very real risk for UK corporates that they end up with two conflicting data regimes within one organisation.

**Middle East**
There are currently no pan-Middle Eastern or pan-GCC (the Gulf Cooperation Council) laws governing data protection and privacy.

Israel is the only Middle Eastern country with data protection laws deemed adequate by the EC. Restrictions on transfer of data offshore are strict, and only include countries that ensure a level of protection of information, which is not lower than the level of protection provided for under Israeli law.

Many Middle Eastern countries (GCC countries in particular) have also undertaken considerable efforts to diversify their economies and increase economic integration in recent years. Saudi Arabia announced Vision 2030, which aims to increase the share of non-oil exports from 16 to 50 per cent over the next 15 years.

Other GCC countries have also undertaken similar programmes, with the intent, like the UAE to continue to attract international IT and finance companies and investment, and increase cross-border technology infrastructure. These developments imply the need to consider developing a data protection regime.

In international economic zones, such as in designated areas in the UAE and Qatar, data protection law, implementation and enforcement are relatively developed. The Dubai International Financial Centre (DIFC) and the Qatar Financial Centre (QFC), have their own dedicated data protection laws and enforcement bodies mirroring best practices from the EU. They all stipulate that personal data can only be transferred to an outside jurisdiction if an adequate level of protection for that personal data is ensured by laws and regulations that apply to the recipient, or if a special permit is approved by the regulatory bodies. DIFC also publishes a list of countries considered as being ‘adequate’ for this purpose, which notably excludes the US. No such list exist for the QFC. That being said, these laws only apply to licensed entities operating in these special zones.

Nevertheless, to date, with the exception of Israel, no Middle Eastern or African countries are considered to have adequate data protection environments from an EU perspective. However, it would appear that change is afoot: Qatar became the first GCC member state to issue a generally applicable data protection law last November. It will come into effect this May, and the potential fine of non-compliance is 5 million Qatari riyals. While the law currently provides specific guidance on the transfer of personal data to other jurisdictions, we can expect that there will be further regulations issued to assist the current law’s implementation.

In addition, there are general constitutional rights and sector-specific laws (notably in telecommunications, banking and medical information) related to data privacy in these countries. Depending on the circumstances, these laws may apply and should be considered when conducting international investigations or responding to litigation.

Given the geopolitical realities of the region, it is unlikely that any EU type regime will be enacted in the Middle East in the near future. However, recent technological developments across the region suggest that authorities are quickly becoming aware of the challenges of international data privacy, which may have implications for the Middle East. In Saudi Arabia, there is a new freedom of information and protection of private data law under review by the Advisory ‘Shura’ Council. In Bahrain, a draft data protection law is being reviewed before the Parliament. Rapid regional economic transformation will also ensure that data privacy continues to be an important topic in the future.

**Africa**
Many African economies are becoming vibrant hubs of economic progress, but the pace in the data privacy development area has been considerably slower.

In June 2014, the African Union (AU) adopted the Convention on Cybersecurity and Personal Data Protection, which many identified as a transformative moment for data protection in the region.
However, to this day, no country has undertaken its ratification, and the convention requires 15 countries to ratify it in order to enter into effect.

Morocco and Mauritius, both with robust data protection laws and active enforcement bodies, remain the notable exceptions in the continent, while the rest of the countries remain in their formative stages. Most countries include general constitution rights and sector specific laws (notably in telecommunications) related to data privacy in many African countries, but roughly half of the 54 African countries on the continent still have no comprehensive data protection regulation and are not publicly working on adopting one. African countries with data protection laws have reported very few enforcement actions, and while most of the existing data protection laws hinge on the principle of adequacy, the same laws do not specify which countries are considered to be ‘adequate’.

In Kenya, a data protection bill was expected to be presented in Parliament by the end of May 2014, but the bill has still not yet passed at the time of this article’s writing. South Africa’s Protection of Personal Information (POPI) Act was signed into law on November 2013, but it is still not effective as a full commencement date has not yet been established.

Interestingly, the POPI Act might be one of the most stringent examples of data privacy initiatives. It prohibits the transfer of personal information outside of South Africa, subject to certain exceptions. For example, where consent is provided and where the recipient is subject to a law or binding agreements that are able to demonstrate effectively data processing principles similar to the conditions for processing personal information under the POPI Act. POPI Act is also unique as it considers criminal penalties and imprisonment when convicted of a breach.

Some key considerations
In EMEA, the approach to data protection varies significantly across the board, and we have seen how both developed economies and emerging markets suffer from regulatory disparity. Essentially, global convergence on the issue of data privacy remains unlikely. Some would argue that the EU is pushing for the GDPR to be the ‘gold standard’ of data privacy for other countries to follow, while others would question costs associated with complying with these standards as well as suggest an imbalance between protecting individuals’ rights to the detriment of national security.

In Europe there are several factors dominating the political and data discourse, chief among them are Brexit and the new responsibilities related to the GDPR. In addition, considering the importance of the US to the global economy in general, and to EMEA in particular given the strength and value of trading relationships with the US, the uncertainty of the Shield must form an important part of the debate, not least because the Trump administration, if anything, makes it even more uncertain. Specifically in the US, the combination of a very old Privacy Act (it was drafted in 1974, since which time Europe has rewritten its privacy rules three times) and Trump’s wide executive order, which could see government agencies insisting on access to European citizens’ personal data, having met a very low threshold of proof – a mere ‘risk to public safety’ would be enough, and some agencies are likely to view that very broadly. In this context, risking reliance on the Shield seems unwise.

All of these factors create uncertainty for companies operating across borders, and leave investors, management and stakeholders susceptible to uneasy regulatory transitions, high costs and exposure to the risk of heavy fines. For industry practitioners, and companies involved in investigations or expecting regulatory probes or even cross-border litigation, there is no single solution, but there are certain measures that can be undertaken in preparation to mitigate risks.

Data mapping
A clear data strategy is vital to any investigation where data may reside in several jurisdictions. Crucial considerations include: knowing what data is being considered, the jurisdiction where the data resides, applicable data privacy regulations and what clearance is required, and the origin of the data collection, let alone transfer.

Depending on the nature and severity of the investigation, companies will be most successful if they take a conservative approach to data transfers, as privacy failures may (and most likely will) lead to sizeable liabilities. In addition, beyond the considerations listed above and the mechanisms potentially used for data transfer, from a strategic and practical perspective, it is worth acknowledging that once data is transferred into the US it becomes ‘discoverable’ and little regard will be given to data protection rights that it may have attached in its country of origin.

Collection and preservation
Prior to carrying out a data collection or data preservation exercise, ensure that the appropriate risk management tools have been engaged, and steps have been taken to ensure compliance with data privacy regulations in the jurisdiction the data is being hosted in. We counsel, in general, collection and preservation of data in its jurisdiction of origin.

Training and escalation
All personnel involved in investigations and data transfers should be provided with up-to-date training regarding data transfer protocols and jurisdictional data privacy regulations. They should also be trained to properly document the considerations and safeguards, throughout the investigation, for any data transfer. Escalation protocols should also be in place to ensure demonstrable consideration and consultation in relation to data transfer, especially for jurisdictions with data privacy regulations that are more challenging to address. Identifying and engaging the appropriate counsel in each jurisdiction, as well as having data identification, processing and transfer experts with extensive cross-border experience in the EU and elsewhere to assist internal stakeholders, is a necessity.

Data transfer strategy
Develop, in consultation with your advisers, a data transfer strategy that takes into consideration the nature of the data, its origin, data privacy and other data-related constraints (banking secrecy, commercial and state secrecy, etc), and security. Err on the side of caution and weigh the risks of using untested or controversial data transfer mechanisms. After all, it is not possible to close the stable door after the data horse has bolted.

Expert advice
Finally, it is imperative to consult and involve expert data privacy and transfer experts from the outset in any cross-jurisdictional investigation, to help navigate the potential conflicts of law we have addressed in this article. From the data identification and location exercise, to the treatment of data in a manner compliant with applicable data privacy laws, to the mechanism employed, if appropriate, for data transfer, advice and execution by the right experts will be critical to success.
Notes
1 Data Protection Directive 95/46/EC.
2 Court Justice of the European Union ‘The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid’ Press Release No. 117/15.
3 Max Schrems (@maxschrems) 29 February 2016.
6 The Data Protection Act 1998, Schedule 1, Part II.
9 DIFC Law No. 1 of 2007 (Amended by Data Protection Law Amendment Law DIFC Law No. 5 of 2012), section 11, 12.
10 Qatar Financial Centre Legislation, Data Protection Rules, section 3.1, 3.2.
11 www.dlapiperdataprotection.com/?t=law&c=SA.
12 www.dlapiperdataprotection.com/?t=law&c=BH.
16 Protection of Personal Information Act of 2013, Chapter 9, section 72.
17 Protection of Personal Information Act of 2013, Chapter 11, section 107.
Weng Yee Ng is a director at FRA. She holds more than 14 years of experience in external and internal audit and forensic accounting. Her main experience includes: compliance reviews; internal investigations; litigation (both civil and criminal) support for multinational companies; risk assessments; evaluation of compliance programmes; procurement fraud matters; third-party due diligence; Foreign Corrupt Practices Act (FCPA) monitorships for both the DOJ and SEC; and disgorgement and penalty calculations. Weng Yee is currently working on a risk assessment and evaluation of compliance programme for an aviation company; internal investigations into whistleblower alerts for a CAC 40 automotive original equipment manufacturer (OEM); a proactive anti-bribery and corruption review for an international bank; and a compliance monitorship for a medical devices company. Having spent over six years working in-country in Malaysia, Weng Yee possesses a first-hand understanding of the business nuances and financial and reporting practices encountered in Malaysia and elsewhere in Southeast Asia. Prior to FRA, Weng Yee was involved in statutory audits, advising on Initial Public Offering (IPO) and debt restructuring exercises, and performing SOX compliance audits for companies in, among others, the financial services, chemicals, construction, real estate, retail, pharmaceutical, education, electronics, extraction, oil and gas, and consumer goods sectors. Bilingual in English and Malay, Weng Yee is also fluent in Cantonese and Mandarin Chinese, and is familiar with Bahasa Indonesia and Spanish. She has conducted work in the US, Chile, Colombia, Costa Rica, Ireland, France, Switzerland, Hungary, Italy, South Africa, China, Indonesia, Philippines, Singapore, Thailand and Australia. Weng Yee is based in FRA’s London office.

Jimmy Ko is a senior associate at FRA. He has over five years’ experience representing global clients in complex multi-jurisdictional fraud, bribery and sanctions investigations and reviews. His main experience includes: Foreign Corrupt Practices Act (FCPA) investigations; monitorship and compliance reviews; internal control testing; fraud risk assessments; and internal investigations. At FRA, Jimmy managed an eight-month internal investigation of a Fortune 500 engineering company. He led a five-member team through onsite reviews in multiple locations in China and worked closely with senior executives including client head of investigation. As part of the monitorship team of a top-five oil and gas service company, Jimmy assessed the adequacy of its compliance programme through onsite reviews in the US, China, India, Malaysia and Colombia, and the company overhauled its third-party due diligence and manual payment process as a result. Moreover, Jimmy assisted a global manufacturing company in the development of a global ABC compliance programme and related training materials for compliance officers in over 60 countries. Prior to joining FRA, Jimmy worked at Ernst & Young in their fraud investigation and dispute services practice, where he specialised in financial sector engagements. Jimmy holds an MBA (distinction) from INSEAD, and is a certified public accountant, a certified fraud examiner and a certified management accountant, where he was awarded a certificate of distinguished performance (top 1 per cent of candidates). He also holds a BS in Commerce from the McIntire School of Commerce, University of Virginia. Jimmy is fluent in English, Mandarin Chinese and Cantonese, and is based in FRA’s Washington, DC office.
MIND THE CONTROLS GAP
How fostering joined-up thinking between the finance, compliance and internal audit functions can help organisations identify regulatory risks more efficiently

There is enormous pressure on finance, compliance, and internal audit functions to assist with the management of risk to an organisation. But are these functions truly joined-up? Are they communicating effectively so as to address blind spots that may lead to unacceptable compliance and regulatory risk exposure? From a compliance perspective, finance functions have traditionally focused on compliance with accounting and reporting standards, and tax legislation. Nowadays, their attention must span more widely.

Financial information systems
The finance function, along with the IT function, will typically have the most intimate knowledge of a company’s financial information systems, including their limitations. Each organisation’s system will be different. Compliance functions should be leveraging the knowledge of their finance team to gain a comprehensive understanding of the system. This should include, for example, which systems do/do not interface, locations where manual controls are more heavily relied upon, and/or locations that operate on standalone systems and therefore lack transparency.

Furthermore, while the financial information system setup, and the controls in place within or alongside it, might operate effectively for financial reporting, there may still be gaps from a compliance perspective. In a recent example, we identified for a multinational client in some very high corruption risk locations the accounts payable sub-ledger was effectively not ‘switched on’. While transactions could still be processed, recorded and accounted for correctly, this created a significant blind spot from a compliance perspective. In this case, the company also operated a global compliance monitoring system to perform name-matching of vendors and transactions, but this interfaced with accounts payable. More collaboration between finance and compliance could have helped identify this issue earlier.

Monitoring and testing
Regulators and enforcement authorities in the UK are building momentum in their efforts to tackle corporate economic crime with a trend towards ‘failure to prevent’ models. In such an environment, monitoring and testing is important. As companies consider the wider scope of testing that is likely to be required – fraud, anti-bribery and corruption, anti-money laundering and sanctions compliance – a good starting point is to look at existing controls more broadly and identify what is in place that has cross-functional benefit.

Some of the financial controls that ensure proper accounting and financial reporting will also have anti-fraud and compliance benefits. Companies can achieve testing efficiencies by identifying, with input from finance, internal audit and compliance, which of their controls also serve as ‘compliance controls’. Consequently, controls testing can be designed in a way that enables multiple testing objectives to be met.

Training
Training needs to deliver information pertaining to certain risks, rules and regulations, but this crucially needs to then be translated into what it means to employees. The finance department should not only receive the standard anti-bribery and corruption training but also be trained on how they – as individuals responsible for core processes, financial controls and financial information systems – can play a part in preventing and detecting bribery (for example, through red-flag training and accurate posting to account codes).

On the internal audit side there are benefits to be achieved in compliance telling the internal audit team the type of testing the compliance team conducts. The way compliance looks at transactions is often very different from the audit perspective. One main difference is the focus of compliance on understanding the business rationale for a transaction or contract, or the identity of the ultimate beneficiary. Encouraging internal audit to see transactions and arrangements with more of a compliance mindset is a way to leverage the coverage of internal audit across the company.

Finance, compliance and internal audit each have their own roles but the interplay between them is receiving more attention. A more joined-up approach will serve organisations well in achieving efficiencies across these functions and helping to bridge the controls gap.

By Emma Hodges, director, Forensic Risk Alliance

Forensic Risk Alliance, Audrey House, 16-20 Ely Place, London EC1N 6SN
Tel: +44 (0) 20 7269 7827
E-mail: ehodges@forensicrisk.com Web: www.forensicrisk.com
The arrival of the General Data Protection Regulation (GDPR) is imminent. On 25 May the regulation governing data privacy for citizens of the EU's 28 member countries becomes enforceable as law. For data collection and transfer – e-discovery initiatives related to cross-border litigation and investigation, for example – it imposes severe restrictions on the handling of the personal data of European nationals. Non-compliance could result in fines and penalties – up to 4 per cent of annual worldwide turnover or €20m.

The GDPR broadly requires organisations to respect privacy; keep EU citizens’ personal data in the country where it is collected; process and store it in that country; and maintain a comprehensive and accurate audit trail. This places the emphasis on proper data governance, as the challenge is knowing where data is and its movements. In many organisations, especially those using cloud services, it is difficult to know where the networks storing their data are actually located.

In e-discovery there is a requirement to preserve (and eventually process) relevant data, typically in response to a subpoena, Section 2 notice or other court or enforcement agency-issued demand for information. Until now, responding to a subpoena has been a co-operative effort across departments in a corporation and, for multinationals, across regions. Under the GDPR organisations will have to reconsider how they share information and the requirement to protect and, in some cases, anonymise or pseudonymise data. There is also a lack of clarity about exposure when processing one custodian’s data, and redacting data when sensitive data on another individual is encountered.

Like most new regulations, additional guidance and specificity will develop over time but the Sedona Conference, a non-profit institute whose membership includes data privacy authorities from around the world, has discussed some of the more ambiguous components of the regulation that require thought:

- **Guidelines for compliance**: The regulation specifies what organisations must do, but not how to do it.
- **Compliance audit**: The GDPR does not specify what an audit will entail or who is to conduct the audit.
- **Fines**: Maximum monetary penalties are specified but there is no designation of an agency to enforce these, nor does it explain how they will be enforced.
- **Preservation and processing**: What used to be considered data preservation can now be interpreted as “processing”.

**Processors or controllers**: There is some indication that e-discovery vendors will no longer be simply data processors, but will likely be deemed data controllers, with substantially different responsibilities.

**Here’s the plan**

More specificity is clearly due, but for now the GDPR is generating plenty of questions. What is known is that certification alone will not protect an organisation. A plan for compliance starts with:

- identifying the members and departments of an organisation who should be involved in GDPR efforts and ensuring they are aware of the new law;
- conducting risk-based data-mapping to identify where data is located jurisdictionally so it can be audited and documented;
- ensuring proper procedures are in place to detect, report and investigate any personal data breaches;
- creating or updating procedures related to requests about personal data;
- checking procedures exist to ensure they cover all rights individuals have (including audit summary, access, anonymising and deletion); and
- consulting counsel and international EU data transfer consultants, as necessary, when developing protocols and undertaking data-mapping.

**Avoid problems**

Uncertainty around enforcement, and lack of guidance around regulations governing cross-border litigation and investigations – especially now the EU has harmonised the highest of standards by enacting the GDPR – leaves investors, management and stakeholders susceptible to challenging regulatory transitions, high costs and potentially heavy fines.

To prevent data privacy compliance issues, best practice is to engage experts – legal counsel, and data privacy and transfer experts – to assist at the outset of any cross-jurisdictional litigation or investigation.
Christmas Comes Early - The FCPA Pilot Program Made Permanent

By Jenny McVey, Associate Director, Forensic Risk Alliance

ABSTRACT: When we first introduced the FCPA Pilot Program in the June 2016 issue, we noted the uncertainties of outcomes for companies who voluntarily self-disclose potential violations. On November 29, 2017, Deputy Attorney General Rod Rosenstein announced that the US Department of Justice (DOJ) had made the FCPA Pilot Program permanent. This article will review some of the key highlights outlined by the DOJ and some considerations for compliance professionals.

The heat is on life science companies. Since 2013, there have been 25 Foreign Corruption Practices Act (“FCPA”) matters involving life science companies, 13 of which occurred in the last two years. Although life science companies have not been immune to FCPA investigations in the past, the statement of Acting Chief of the U.S. Department of Justice ("DOJ") Fraud Section, Sandra Moser in August was loud and clear - the DOJ would be increasing its enforcement efforts of healthcare related companies.

We reviewed the outcomes of the FCPA Pilot Program ("Pilot Program") in the September 2017 issue of the Update, examining the benefits of self-disclosure under the program. Now, a year since its inception, the DOJ has announced that the Pilot Program will now be permanent.

Additionally, in response to the wide criticism from practitioners that more clarity about how the program works was needed, the DOJ enhanced the FCPA Corporate Enforcement Policy ("Policy") to provide more detail about its decision making in cases. This additional detail is welcomed and certainly will help companies facing the decision of whether or not to self-disclose potential misconduct. This article will examine some key updates the DOJ provided and some considerations for compliance professionals.

Background

On April 5, 2016, the DOJ launched the one-year Pilot Program to reward and incentivize companies to self-report violations of the FCPA. By voluntarily self-reporting potential violations, remediating gaps in compliance programs in a timely fashion, and cooperating with the government’s investigation of suspected violations, companies could benefit from reduced financial penalties, potential declination of prosecution or even consideration of not a monitor.

Although the DOJ has encouraged voluntary self-disclosure and cooperation in FCPA matters for many years, the Pilot Program was launched with the intent to provide more guidance and clarity around the benefits a company may receive by self-disclosing misconduct and cooperating with investigations.

In addition to the obvious incentive to reduce the need for costly and often unpredictable outcomes from litigation, the DOJ wanted to:

1. reduce the unpredictability of potential fall-out once a company voluntarily discloses a potential violation,
2. promote transparency around sanctions and
3. provide a benefit for proactively coming forward to report misconduct.

1 FRA provides multi-jurisdictional expertise in financial and electronic forensics to help companies manage risks in an increasingly regulated business climate. www.forensicrisk.com
2 Can be found at www.traceinternational.org/compendium
4 See Mark Scallon, Jenny McVey & Jimmy Ko, To Disclose or Not to Disclose... That is the Question: he DOJ’s FCPA Pilot Program – Insights from Year One and Beyond, 3.9 LIFE SCIENCE COMPLIANCE UPDATE 13–18 (2017), available at: https://www.lifescicompliance.com.
However, since its inception the program has been criticized for lack of clarity and whether there were true benefits for self-disclosing.\(^6\)

### FCPA Pilot Program Made Permanent

This past November, Deputy Attorney General Rod Rosenstein announced that the DOJ decided to make the FCPA Pilot Program permanent. Therefore, it appears that our previous conclusion that the benefits Pilot Program participation outweigh the downsides was shared by the DOJ. As the table of cases illustrates, there are significant advantages for active participation in the program.

In announcing permanent status for the Pilot Program, the DOJ made significant efforts to to provide the additional details that the Pilot Program lacked. As a result, the DOJ updated the Policy to include the following:

**Fostering a culture of compliance within the organization.** The Policy offers guidance on what an effective compliance program would look like, which includes “the company’s culture of compliance, including awareness among employees about any criminal conduct.”\(^6\) Although the concept of company culture has always been a hot topic within regulatory circles, it is probably one of the most neglected areas when examining compliance programs, because of the challenge with how to measure culture. Understanding that employees can only be as ethical as the culture in which they operate, the Policy has placed a culture of compliance as the first bullet point describing key points that should be considered when implementing a compliance program.

---

5. See Mark Scallon, et al., supra at 15.
6. See id.
7. See Mark Scallon, et al., supra at 14 (“[N]ine corporate FCPA matters were resolved through 2Q 2017 under the Pilot Program, seven which received a declination of prosecution.”)
Presumption of declination...unless there are aggravating circumstances. Under the Pilot Program, declinations would be considered, if the company self-reported, proactively cooperated, and explained remediation efforts. The revised policy now states that companies that follow the same requirements can presume that they will receive a declination. However, there is a caveat. If “aggravating circumstances” are present, then the presumption of declination is removed. Aggravating circumstances include:

- Involvement of executive management in the misconduct
- Significant profit made by the company from the misconduct
- Pervasiveness of the wrong-doing within the organization, or
- Recidivism.  

De-confliction: companies may not investigate because the DOJ will. The concept of ‘de-confliction’ is not new, but was not clearly defined within the Pilot Program. The policy now provides more clarity. The DOJ may ask companies to hold off on certain areas of an internal investigation (e.g., interviews), so that they can proceed with their own investigation. The policy further clarifies that this de-confliction would be limited in scope and time, and the company under investigation would be notified when it was lifted. This clarification is a substantial help for compliance professionals by reducing the real concern that the DOJ could view a company’s internal compliance investigation as constituting an obstruction of justice.

Adds root-cause analysis to remediation efforts. The requirement of robust remediation has not changed. However, the Policy now requires companies to undertake a root cause analysis as part of their efforts. This requirement puts the onus on the company to make sure that they identify the underlying cause of the misconduct in order to appropriately remediate. Often, remediation efforts, such as updating governance documents, implementing more employee training, or firing wrong-doers is just 'checking the box' and may not be fully effective. Identifying the root-cause of the misconduct can further direct companies as to where gaps may exist and to put the proper controls in place.

Snapchat, Cover Me, Wickr, Confide, Bleep and other self-destructing message apps are prohibited. The policy made it clear – if companies want a chance to receive full credit, they must prohibit “employees from using software that generates, but does not appropriately retain, business records or communications.” The purpose of this provision is to allow for retention of business records, and prohibit deletion or destruction of business records. As technology use continues to challenge compliance professionals, this requirement provides companies with a directed task on how to position social media within their organization. However, the life science industry, or at least the life science compliance community, is likely to welcome this requirement.

The Life Science Environment and the FCPA

Anti-bribery and corruption laws present a particular challenge in life science companies throughout the world. In many countries, the complexity around whether or not state-owned businesses and physicians are considered government officials is daunting. Additionally, in some countries such as China, the government permits hospitals to sell therapies directly to patients, thus making those institutions into government-run de facto distributors. Furthermore, although some ‘high risk’ countries (e.g., China) are making efforts to mitigate corruption, there is still a need for life science companies to take a hard look at their current programs to ensure they are taking the necessary compliance decisions and steps to help avoid violations.

The potential risk and negative effects of violating the FCPA (and other anticorruption laws such as the U.K. Bribery Act) is not lost on companies. In fact, we are starting to see companies with international operations including FCPA enforcement as a risk factor within their Securities and Exchange Commission (“SEC”) registrations.

For example, Fibrogen, Inc. and Shineco, Inc. specifically included China along with their risk warnings. Fibrogen, Inc., a pharmaceutical company based out of California, disclose their risk of operating in China stating:

As we expand our operations in China and other jurisdictions internationally, we will need to increase the scope of our compliance programs to address the risks relating to the potential for violations of the FCPA and other anti-bribery and anti-corruption laws. Our compliance programs will need to include policies addressing not only the FCPA, but also the provisions of a variety of anti-bribery laws.
an anticorruption laws in multiple foreign jurisdictions, including China, provisions relating to books and records that apply to us as a public company, and include effective training for our personnel throughout our organization.16

Shineco, Inc., a manufacturer of plant-based medicines based out of Beijing also included a disclosure within their SEC Registration, stating the challenges that come with the life science industry operating in high risk countries:

We have operations, agreements with third parties, and make sales in China, which may experience corruption. Our activities in China create the risk of unauthorized payments or offers of payments by one of the employees, consultants or distributors of our company, because these parties are not always subject to our control.

Although we believe to date we have complied in all material respects with the provisions of the FCPA and Chinese anti-corruption law, our existing safeguards and any future improvements may prove to be less than effective, and the employees, consultants or distributors of our Company may engage in conduct for which we might be held responsible.”17

It should be noted that although China is not the only high-risk country for corruption risks. In fact, all of the so-called BRIC countries (Brazil, Russia, India and China) fall into the high-risk category. However, because of the volume of SEC registrants seeking to do business with the world’s largest economy, China related warning have appeared more often. However, regardless of country, the life science industry is taking the DOJ’s promise to focus on healthcare very seriously.

**Conclusion**

What can life science companies do to potentially avoid having to weigh the benefits of self-disclosure in the first place? Some key areas to consider are due diligence processes – are they robust enough? Are they being conducted in a timely manner? How robust are your monitoring programs? Can you effectively document findings and remediation efforts? Is your fair market value analysis sound?

**Assess your compliance culture with the same rigor as your compliance program.** As stated above, the DOJ specifically references a compliance culture as part of a compliance program remediation. Employees can only be as good as the values of the organization and the behaviors its leaders exemplify. Although efforts such as updating policies and re-training employees are essential for remediation, if the culture of the organization is corrupted, no amount of governance documents or monitoring programs can keep wrong-doing from occurring.

Up your third-party due diligence game. Third-party compliance programs should be developed, if not already in place, updated, and assessed with the same stringency as companies have done for engaging an HCP as a consultant in the US. A key point to consider is that due diligence should be risk-based in order to apply the appropriate level of controls. Some considerations to include are background checks, audits, self-certifications, and conflict of interest checks.

Monitor, monitor, and monitor. Monitoring intermediaries over time sounds daunting, however it is integral to the overall health of a compliance program. Along the same lines as for due diligence, monitoring should also be risk-based, allowing the company to focus on particular areas rather than implementing a blanket-program that may not add value to mitigating risk. Consider including a ‘right to audit’ clause within contracts, and planning monitoring activities on a regular basis.

The updated policy and permanent status for the Pilot Program is welcomed by many practitioners and compliance functions, as it allows companies to better understand the potential outcomes and benefits, including the potential reputational and collateral damage from details of the investigations being made public if involved in an FCPA matter. It truly is Christmas come early.

16 See id.
17 See id.
FCPA Winter Review 2018

International Alert
02.14.2018

Featured in This Edition
- **Introduction**
- **Actions Against Corporations**
  - SBM Offshore N.V. and Its U.S. Subsidiary Settle with DOJ in Connection with Corrupt Payments in Brazil, Angola, Equatorial Guinea, Kazakhstan, and Iraq
  - Keppel Settles with DOJ Over Alleged Violations in Brazil
- **Actions Against Individuals**
  - Florida Businessman Pleads Guilty to FCPA-Related Charges in Connection with DOJ’s Investigation of PDVSA Energy Contracts
  - Two SBM Executives Plead Guilty to FCPA Charges
  - Four Individuals Plead Guilty, a Fifth Charged, in Rolls-Royce Bribery Scheme
  - Former Embraer Executive Pleads Guilty to Participating in Bribery Scheme Detailed in Embraer’s 2016 Deferred Prosecution Agreement
  - Senior Member of Keppel Legal Department Pleads Guilty
- **Ongoing Policy Developments and Related Litigation**
  - DOJ Announces New “FCPA Corporate Enforcement Policy” to Replace the FCPA Pilot Program
  - SEC Ratifies the Appointment of Its ALJs; Solicitor General Reverses Course to Take Consistent Position Before Supreme Court
- **International Developments**
  - HSBC Enters into First Ever Corporate Criminal Settlement in France
  - Argentina Introduces Corporate Liability and Compliance Standards in New Anti-Corruption Law
  - Peru Introduces Corporate Liability for Corruption Offenses with a Compliance Program Defense
- **Miller & Chevalier Upcoming Speaking Engagements and Recent Articles**

**Introduction**

Despite initial questions in some quarters about the incoming Trump administration’s commitment to enforcing the U.S. Foreign Corrupt Practices Act (FCPA), 2017 turned out to be a fairly typical year in terms of resolved FCPA corporate enforcement actions, as well as an unusually active year for enforcement against individuals, driven largely by Department of Justice (DOJ) convictions and charges. Following an active December and January under the outgoing Obama administration, the next several months of 2017 saw only a few FCPA dispositions. However, through the spring and summer of the year, the administration filled key FCPA-related positions at both the DOJ and Securities and Exchange Commission (SEC) that had been vacated after the change in presidential administrations and personnel from both agencies, including Attorney General Jeff Sessions and SEC Chair
Jay Clayton, expressed support for continued assertive FCPA enforcement. By the end of 2017, the number of publicly-announced FCPA dispositions had increased, with several large corporate settlements (including one just under $500 million) and various individual charges and guilty pleas unsealed during the fourth quarter of the year. On balance, there were 17 resolved corporate enforcement actions announced in 2017, a total that is consistent with the average over the last 10 years.

Throughout the year, we saw a continuation of three important FCPA enforcement trends that have become particularly evident in recent years. First, both the DOJ and SEC continued to emphasize actions against individuals responsible for illegal activities. For example, in early September 2017, one of the co-directors of the SEC’s Division of Enforcement stated that SEC is “incredibly focused” on the liability of individuals across the enforcement spectrum, including with regard to the FCPA, and she noted that individuals had been the subjects of over 70 percent of the agency’s dispositions in the last five years. Similarly, senior DOJ officials repeatedly highlighted the Department’s commitment to “prioritize prosecutions of individuals who have willfully and corruptly violated the FCPA,” in line with the 2015 guidance on “Individual Accountability for Corporate Wrongdoing,” the so-called Yates Memorandum.

Second, the DOJ continued to offer the possibility of declination from prosecution for companies that meet certain requirements. greater detail below, in late November 2017, Deputy Attorney General Rod Rosenstein announced the new “FCPA Corporate Enforcement Policy,” which was codified as an addition to the U.S. Attorneys’ Manual. The new policy effectively continues and modifies the DOJ’s earlier “Pilot Program” and offers the possibility of corporate declinations from prosecution as an incentive for self-disclosure and cooperation by companies. The policy’s presumption of a corporate declination continues to depend on three prerequisites: full and timely voluntary self-disclosure to the DOJ; full cooperation (including as to facts relevant to the culpability of individual employees); and timely and appropriate remediation (including implementation of an effective compliance and ethics program and appropriate discipline of employees). However, the policy’s presumption also tightens some requirements from the Pilot Program — for example, by imposing a new requirement that, in order to receive full credit for remediation, companies must prohibit employees from using software that “generates but does not appropriately retain business records or communications.”

Finally, in 2017, both the DOJ and SEC imposed penalties that were part of large, globally-coordinated settlements in which enforcement authorities from multiple countries imposed combined penalties of hundreds of millions of dollars for the same or similar alleged misconduct, but agreed to consider penalties paid in other jurisdictions for offsets or reductions. This trend was a major theme of 2016 and is, to a significant degree, the result of greater cooperation between the U.S. enforcement agencies and their foreign counterparties, particularly in the United Kingdom, Brazil, and the Netherlands.

All three of these trends were discernable in the FCPA enforcement activity for 2017, especially for the DOJ. The past calendar year marked the fourth consecutive year that both individual prosecutions and corporate declinations by the DOJ have increased. As described below, the large anti-corruption settlements with Telia Company AB and SBM Offshore N.V. (SBM) were among the top 10 global resolutions by settlement amount, making clear that greater cooperation among enforcement authorities is leading to substantial effects, in line with the longstanding U.S. goals of broadening enforcement to other countries and “leveling the playing field” for U.S.-based companies.

A notable milestone during the fourth quarter of 2017 was the 40th anniversary of the FCPA — enacted in November 1977 — which provides an opportunity to reflect on the law’s past and future. Looking back a decade, 2007 was an inflection point for the FCPA, ushering in an era of more aggressive corporate and individual enforcement. Given the three trends set forth above — namely, U.S. agencies’ commitments to individual prosecutions, more formal corporate declinations driven by companies undertaking reporting and compliance obligations, and greater global cooperation — 2016 and 2017 may mark another inflection point, particularly if the U.S. and foreign enforcement authorities continue moving in the same direction as they have been in recent years.

Corporate Enforcement Trends in 2017
In 2017, the DOJ resolved 10 corporate enforcement actions — including guilty pleas, Deferred Prosecution Agreements (DPAs), and a Non-Prosecutions Agreement (NPA) — for a total just under the Department’s average of 12 enforcement actions a year since 2007. For its part, the SEC ended the year with seven corporate enforcement actions, which was below the agency’s average of approximately 12 enforcement actions a year over the same period.

Following an active January 2017 and over seven months with only one corporate disposition, the last four months of the year saw a slight uptick in corporate enforcement actions by the DOJ and SEC. Specifically, the agencies entered into settlements with Telia and Alere, Inc. in September 2017, as discussed in our FCPA Autumn Review 2017, as well as two large, multijurisdictional settlements with SBM and Keppel Offshore & Marine Ltd. (Keppel) in the fourth quarter of the year.

On November 29, SBM, a Netherlands-based manufacturer of offshore oil drilling equipment, as discussed in greater detail below, according to the DPA, from 1996 until at least 2012, SBM paid more than $180 million in commissions to intermediaries, knowing that a portion of these payments would be used to bribe government officials in Angola, Brazil, Equatorial Guinea, Iraq, and Kazakhstan in an effort to obtain or retain business. In calculating SBM’s criminal fine in the U.S., the DOJ reportedly took into account the $240 million the company had paid to Dutch authorities in 2014 to resolve similar charges. Nevertheless, the company’s combined worldwide penalties total more than $475 million, which does not include the $342 million in cash penalties and discounts on future work that SBM has agreed to pay the Brazilian state-owned energy firm Petróleo Brasileiro S.A (Petrobras), an amount that will affect the company’s bottom line even if it does not count as a criminal penalty. Of additional interest is the DOJ’s note in its announcement of the settlement that the company “brought the conduct to the attention of the Criminal Division’s Fraud Section and Dutch authorities,” but “did not provide a complete disclosure for approximately one year.”
On December 22, Singapore-based shipyard operation company Keppel agreed to a $105.6 million criminal fine as part of DPA with the DOJ to settle one count of conspiracy to violate the anti-bribery provisions of the FCPA, while its U.S. subsidiary, Keppel Offshore & Marine USA Inc. (Keppel USA), pled guilty to a similar FCPA-related conspiracy charge. As discussed below, the charges against both Keppel and its U.S. subsidiary arose out of an alleged decade-long scheme to pay millions of dollars in bribes to officials in Brazil, including at Petrobras. The fine owed in the United States is only a quarter of the total global settlement, with another $105.6 million owed to authorities in Singapore — where the company is based — and $211 million owed to authorities in Brazil — where the misconduct took place — for a total of $422 million in criminal penalties.

Viewing the large 2017 settlements in the context of broader FCPA enforcement, only Telia’s $483 million in combined penalties ranks among the top 10 FCPA corporate dispositions. However, Telia, SBM, and Keppel are also noteworthy as examples of the recent trend of large global corruption settlements, in which the settlement amounts imposed by the DOJ and SEC were offset in recognition of penalties imposed by foreign enforcement authorities.

For example, the DOJ and SEC assessed Telia more than $965 million in penalties, but then discounted that amount by up to $482.5 million to recognize and offset penalties imposed by the Dutch Public Prosecutor’s Office and Swedish Prosecution Authority. Similarly, in calculating its $238 million penalty imposed on SBM, the DOJ reportedly took into account SBM’s payment of $240 million in penalties paid to the Netherlands in 2014, as well as future payments and work discounts owed in Brazil. Finally, U.S. enforcement authorities required Keppel to pay only $105.5 million of the $422 million imposed under the
company’s settlement agreements with the DOJ and SEC, a dollar for dollar reduction accounting for the exact amount of the penalties the company agreed to pay under parallel settlements in Brazil and Singapore.

In light of this trend, consideration of total global settlements may now be necessary to adequately assess anti-corruption enforcement trends and the concomitant risks to multinational companies. Therefore, the chart below shows the top 10 global settlements in which the FCPA was a factor:

We first discussed the increase in large multijurisdictional settlements in our FCPA Winter Review 2017, noting several settlements of this nature reached in 2016, including Odebrecht/Braskem, Rolls-Royce plc, Teva Pharmaceuticals, and VimpelCom. With regard to this larger trend, it is noteworthy that, of the 10 companies that appear among the top 10 largest global settlements involving the FCPA, only one is U.S.-based (Halliburton), while all of the others are headquartered and incorporated outside the United States. In fact, some of the companies with top 10 global settlements — for example Odebrecht (and its subsidiary Braskem), Telia, and VimpelCom — appear to do very little business within the United States.

Enforcement Against Individuals During 2017

While 2017 was an average year for corporate enforcement, it was an unusually active year for enforcement activity against individuals, largely driven by individual charges filed and convictions obtained by the DOJ. Specifically, the DOJ brought charges against 17 individuals — the agency’s highest number since 2009 — and successfully reached guilty pleas or jury convictions for 13 individuals — the agency’s highest number ever in a single year. Eight of these charges and seven of these convictions were for individuals associated with companies subject to parallel investigation and settlements by the DOJ in 2016 or 2017, namely Rolls-
Royce, Embraer, SBM, and Keppel. The SEC was less active, with only four judgments or administrative procedures and three charges initiated against individuals in 2017, a slightly below-average year for the agency. All four of the SEC’s individual resolutions were also associated with companies subject to parallel investigation by the DOJ, either itself or in conjunction with the SEC.

In the fourth quarter of 2017, the DOJ announced guilty pleas by nine individuals — five of whom had pled guilty during the quarter and four of whom had pled guilty in prior quarters, but whose pleas had not been previously announced. The agency also announced that it had filed charges against two more individuals, but that these charges had yet not been resolved.

In October 2017, the DOJ As noted below, Ardila’s is one of several recent guilty pleas by Florida-based businessmen implicated in the same corruption schemes involving the PDVSA. That same month, real estate broker Andrew Simon was arrested and charged for his role in a corruption scheme involving the Landmark 72 skyscraper in Hanoi, Vietnam, another scheme under which several other individuals have been charged or convicted.

In November 2017, the DOJ discussed in detail below. The same month, the agency announced that it had obtained guilty pleas for FCPA-related charges from four individuals associated with Rolls-Royce: former Rolls-Royce senior executive James Finley, former regional director Keith Barnett, former energy sales employee Aloysius Johannes Jozef Zuurhout, and the former head of a separate engineering and consulting firm, Andreas Kohler. As also discussed in detail below, the DOJ charged all four individuals
for their roles in the same alleged corruption scheme for which Rolls-Royce had separately entered into a DPA with U.S. authorities in December 2016. The DOJ simultaneously announced that it had brought charges against Petros Contoguris, who is the founder of a Turkish oil and gas advisory company allegedly involved in the scheme, but who has not pled guilty and is reported by the DOJ to be outside the United States.

Finally, in December 2017, the DOJ announced a guilty plea by Colin Steven, a U.K. citizen and former sales executive at the Brazil-based aircraft manufacturer Embraer S.A. The company settled charges of its own in a combined $205 million disposition with the DOJ and SEC in late 2016, as discussed in our Mr. Steven and Mr. Chow’s cases are summarized below.

Besides being an active year in terms of individual charges and convictions by the DOJ, 2017 was also the third consecutive year that the number of individuals charged and the number of individuals actually convicted has increased year over year. The numbers for 2017 could increase still further, as additional charges filed in 2017 may be unsealed in 2018. This uptick in enforcement involving individuals may be attributable, at least in part, to the DOJ's formal emphasis on individual prosecutions, as highlighted in the 2015 “Yates Memorandum” and recently reinforced by current policy statements from senior agency officials. Although the impact of the Yates Memorandum was initially unclear, enough time may now have passed to safely trace some of the patterns in individual enforcement we saw in 2017 to the policy priorities established by the Memorandum.

It is also noteworthy that eight of the individuals charged and seven of the individuals convicted by the DOJ in 2017 are associated with companies subject to parallel investigations and convictions — namely Embraer, Rolls-Royce, SBM, and Keppel — demonstrating the DOJ’s continued goal of parallel corporate and individual actions. In addition, as discussed further below, this trend is likely to continue in light of the DOJ's new “FCPA Corporate Enforcement Policy,” under which corporate declinations are contingent on disclosure of “all relevant facts about all individuals involved in the violation of law.” Such disclosures could potentially give the DOJ access to additional information that may be used in subsequent individual prosecutions.

### 2018 Enforcement Actions to Date

There were no corporate enforcement actions under the FCPA in 2018 to date, but we did see enforcement activity against individuals, including a guilty plea by one individual and charges against another. We will briefly preview this enforcement activity here and will discuss it in greater detail in Miller & Chevalier’s forthcoming FCPA Spring 2018 Review.

- **Joo Hyun Bahn, aka Dennis Bahn:** On January 5, 2018, Joo Hyun Bahn pled guilty to two FCPA-related counts for his role in a scheme to pay an official at a Middle Eastern sovereign wealth fund to purchase the Landmark 72 skyscraper in Hanoi, Vietnam. According to the DOJ’s public release, Bahn, who was indicted in 2016, admitted to transferring $500,000 to Malcom Harris, an intermediary in New York, on the understanding that Harris would pass the money on to the Middle Eastern official. However, Harris allegedly stole the $500,000 without passing any of it along. Harris has been charged but not convicted. Two of Bahn’s co-defendants — Andrew Simon and San Woo, aka. John Woo — pled guilty to FCPA charges in 2017 stemming from their involvement in the scheme.

- **Mark Lambert:** On January 12, 2018, the DOJ unsealed an 11-count indictment — including one count of conspiracy to violate the FCPA and seven counts for substantive FCPA violations — against Mark Lambert, the former co-president of a Maryland company that provided services for the transportation of nuclear materials. According to the indictment, between 2009 and 2014, Lambert conspired to pay kickbacks to the head of a subsidiary of Rosatom, Russia’s state-owned nuclear energy corporation. Lambert’s case has been the subject of press scrutiny because of Rosatom’s indirect acquisition of Canadian mining company Uranium One, which occurred while 2016 Democratic presidential candidate Hillary Clinton was U.S. Secretary of State.

- **PDVSA Officials:** On February 12, 2018, the DOJ unsealed indictments against five former government officials known as the “management team” of PDVSA, the same Venezuelan state-owned oil company that was the center of the alleged kickback conspiracy that led to the convictions of Fernando Ardila Rueda and several other U.S.-based individuals. All five members of
the management team are Venezuelan citizens (one also holding a U.S. passport) who allegedly used their significant influence with PDVSA to solicit bribes and kickbacks from vendors in the United States. Of the five members of the management team, only two — Luis Carlos De Leon Perez and Nervis Gerardo Villalobos Cardenas — face FCPA-related charges, with the rest facing various money-laundering charges.

Declinations

In contrast to the average number of corporate enforcement actions, 2017 was a record year for corporate declinations, a term we define broadly as a decision by the DOJ or SEC to close an investigation without enforcement. Declinations are not always publicized, making exact recordkeeping somewhat difficult. Nevertheless, Miller & Chevalier has identified 16 known DOJ declinations in 2017 — including two that imposed disgorgement — which is the most on record for the agency in one year.

Over the course of 2017, the SEC issued 11 known declinations, equaling its previous high set in 2013.

This increase in declinations coincides with the DOJ’s FCPA Pilot Program, introduced in April 2016 and lasting until November 2017, which offered the possibility of a declination for companies that (1) voluntarily self-disclosed; (2) fully cooperated in any subsequent government investigation; and (3) carried out timely and appropriate remediation. Although causation is difficult to determine based on available public evidence, in a November 2017 speech, Deputy Attorney General Rosenstein credited the Pilot
Program’s incentive structure with encouraging more companies to disclose potential misconduct to the DOJ and leading the agency to offer more declinations without prosecution. We will continue to track the DOJ’s implementation and application of the new FCPA Corporate Enforcement Policy, particularly its effect on the Department’s issuance of declinations.

The declinations we have identified in 2018 to date are:

- **Cobalt International Energy, Inc.**: On January 30, 2018, the company filed a Form 8-K stating, “[o]n January 29, 2018, the United States Securities and Exchange Commission (the “SEC”) concluded its FCPA investigation relating to the Angolan operations of Cobalt International Energy, Inc. (“Cobalt”) and advised that the SEC staff does not intend to recommend any enforcement action by the SEC against Cobalt. This formally concludes the SEC investigation, which was opened in March 2017.”

- **Juniper Networks, Inc.**: In a Form 8-K filed on February 9, 2018, the company stated that “it received a letter from the U.S. Department of Justice (“DOJ”) notifying the Company that the DOJ has closed the Company’s previously disclosed investigation into possible violations by the Company of the U.S. Foreign Corrupt Practices Act (“FCPA”) without taking any action against the Company. In its letter, the DOJ acknowledged the Company’s cooperation in the investigation. As previously disclosed, the Securities and Exchange Commission is also conducting an FCPA investigation, and that matter has not yet been resolved.”

- **Core Laboratories N.V.**: On February 12, 2018, the company filed a Form 10-K stating, “[i]n a letter dated February 5, 2018, the Company was informed by the SEC, that they have concluded their investigation as to the Company’s connection with Unaoil and they do not intend to recommend an enforcement action by the Commission against the Company.” As discussed in our FCPA Autumn Review 2017, the company reported that it received a declination from the DOJ in October 2017.

In addition to the declinations listed above, we are aware of another declination issued by the SEC in 2018 to date. We cannot report any other details for this declination, including the name of the target company, because the declination has not been publicly reported. As is our standard practice, we do not report the details of non-public declinations.

**Known Investigations Initiated in 2017**

We have identified 30 investigations initiated in 2017 — slightly below the previous year’s 33 new known investigations and slightly higher than the post-2005 average of 28.8 new investigations per year. The number of known new investigations initiated by the DOJ and SEC is a reasonable proxy for the enforcement agencies’ aggressiveness in FCPA enforcement, making the 2017 statistics particularly noteworthy as an indication of no perceivable drop in FCPA investigative activity under the Trump administration. Although more speculative, the new investigations made known in 2017 may also be a useful metric to predict FCPA enforcement actions yet to come under the Trump administration, as some of the current investigations are likely to result in future dispositions. As of the date of publication, we have identified only one known investigation initiated in 2018 and will continue to monitor investigation activity throughout the quarter.
That said, while the number of known investigations initiated is a useful statistic, one cannot directly compare the numbers of resolved enforcement actions, declinations, and new investigations from year to year, as a single investigation can often result in multiple enforcement actions or declinations. Moreover, there are likely additional investigations and declinations of which we are not yet aware because the government agencies or the companies involved have chosen to not publicly disclose them. With respect to the chart above, since public companies sometimes wait months, or even years, to disclose the existence of an investigation in their securities filings — with some choosing never to do so — and since non-issuer companies often never disclose the existence of an investigation, the numbers in the chart are likely to rise, even for past years.

FCPA at 40: A Look Back and Predictions for the Future

Looking back at 2017, early speculation in some quarters regarding an FCPA enforcement slowdown under the Trump administration appears to have not come true. Rather than reflecting any significant change in enforcement priorities, 2017 was a year in which key trends from the past two years continued, offering some insight into the future of FCPA enforcement. The FCPA Corporate Enforcement Policy, announced in November 2017, may produce more formal, public declinations as it solidifies an incentive structure. The DOJ has credited the Policy with prompting more companies to self-disclose in an effort to obtain declinations, though it does not address all of the concerns that have been raised regarding past versions of such policies.

At the same time, the DOJ’s emphasis on individual prosecutions, formalized in the 2015 Yates Memorandum, appears to
continue having a tangible effect under the FCPA, resulting in four years of increases in the number of individual charges brought and convictions secured by the agency, including new year-end highs of 17 individuals charged and 13 convicted in 2017. The SEC also has publicly committed to more actions against individuals in the FCPA area. Furthermore, the growing trend of globally coordinated anti-corruption settlements continued in 2017 and encompassed the three largest corporate FCPA settlements of the year.

The last trend continues to represent what is likely the most influential shift in FCPA enforcement going forward. Long a policy goal of the United States as a response to U.S. companies’ complaints regarding potential competitive disadvantages created by FCPA enforcement, the acceleration of multijurisdictional investigations, some of which have been led by non-U.S. authorities, will continue to undergird assertive anti-corruption enforcement while presenting increasing challenges to companies under investigation.

International Developments

In November 2017, French authorities entered into a €300 million settlement with Geneva-based HSBC Private Bank (Suisse) SA (HSBC) using a Convention Judiciaire d’Intérêt Public (CJIP), or Judicial Agreement in the Public Interest. As discussed in detail below, this resolution marked the first use of a CJIP, an enforcement mechanism introduced in December 2016 as part of France’s new anti-corruption legislation (Sapin II) and frequently compared to DPAs and NPAs. The purpose behind the CJIP
was to streamline the resolution of corporate corruption cases, since the only method of resolving such cases before Sapin II was through trial. Although the charges against HSBC involved tax avoidance rather than bribery per se, the settlement illustrates French prosecutors’ enhanced ability under Sapin II to bring foreign bribery cases against corporations.

In December, Argentina’s president signed into law new anti-corruption legislation that introduced corporate liability for foreign and domestic bribery, as well as several related concepts. As discussed below, the new law allows a compliance (or “integrity”) program to serve as a key component of a defense to corporate liability, sets forth the elements of an effective compliance program, and introduces a resolution mechanism for cooperating entities akin to a DPA.

Meanwhile, in Peru, a legislative decree adopted in 2017 took effect on January 1, 2018, expanding corporate liability to a broader range of corruption offenses, as well as offenses related to money laundering and terrorist financing. The new law, discussed in detail below, introduces corporate liability for acts of employees and various third parties. It also establishes the minimum components of a compliance program (referred to as a “prevention model”), the adoption of which may serve as a defense against liability under the law.

Actions Against Corporations

SBM Offshore N.V. and Its U.S. Subsidiary Settle with DOJ in Connection with Corrupt Payments in Brazil, Angola, Equatorial Guinea, Kazakhstan, and Iraq

On November 29, 2017, the DOJ announced that it had agreed to settle FCPA-related charges in connection with the alleged bribery of foreign officials in Brazil, Angola, Equatorial Guinea, Kazakhstan, and Iraq with SBM Offshore N.V. (SBM), a Netherlands-based construction and offshore drilling company, as well as with SBM’s Houston-based subsidiary, SBM Offshore USA Inc. (SBM USA). SBM entered into a DPA in connection with a one-count criminal information charging the company with conspiracy to violate the anti-bribery provisions of the FCPA. SBM USA pleaded guilty and was sentenced on one count of conspiracy to violate the anti-bribery provisions of the FCPA. Pursuant to the DPA, SBM agreed to pay “total monetary penalties” of $238 million to the United States, including a $500,000 criminal fine and $13.2 million “paid as a forfeiture” on behalf of SBM USA.

As reported in our FCPA Winter Review 2015, SBM settled with the Dutch Public Prosecutor’s Office in 2014 for related conduct, agreeing to pay $200 million in disgorged profits and a $40 million fine — an amount the DOJ credited when calculating the 2017 penalties. According to the DPA, the U.S. also credited the amount in the announced provision taken by SBM in connection with its efforts to reach a resolution in Brazil. SBM’s total penalties for the actions underlying these resolutions, therefore, constitute more than $475 million. However, this amount does not include the $342 million in cash penalties and discounts on future work that SBM has agreed to pay the Brazilian state-owned energy firm Petróleo Brasileiro S.A. (Petrobras).

The DOJ had also investigated SBM in 2014, but declined to continue the investigation at that time, citing the findings from SBM’s internal investigation, other facts known to the DOJ at the time, and the apparent lack of jurisdiction. However, according to the 2017 DPA, the DOJ learned in 2016 that a “U.S.-based executive of one of SBM’s domestic concerns managed a significant portion of the corrupt scheme and engaged in conduct within the jurisdiction of the United States.” While unclear, this sentence could refer to either Robert Zubiate, a U.S. citizen who served as an executive at SBM USA and two other Houston-based SBM subsidiaries, or Anthony Mace, a U.K. citizen who served as an executive and board member at the same Houston-based SBM subsidiaries. According to the DPA, both Zubiate and Mace “oversaw or executed SBM’s worldwide bribery scheme” and “knowingly and willfully conspired with each other and others known and unknown,” to cause SBM to make corrupt payments to foreign officials. Both men’s guilty pleas are discussed further below.

Based on the DPA’s statement of facts, from approximately 1996 to 2012, SBM paid more than $180 million in commissions to intermediaries in Brazil, Angola, Equatorial Guinea, Kazakhstan, and Iraq, knowing that a portion of those payments would be used
to bribe foreign officials of state-owned oil companies — often to obtain confidential information that gave SBM an improper advantage in receiving contracts from those companies. According to the DPA, the company earned or expected to earn at least $2.8 billion in profits from work with these state-owned oil companies. The detailed allegations related to activities in each of the named countries are set forth below:

Brazil

According to the DPA, from approximately 1996 to 2012, SBM paid bribes to at least three officials at the Brazilian state-owned oil company Petroleo Brasileiro (Petrobras) — all through an intermediary “who provided sales and marketing services to SBM in Brazil” and owned several Brazil-based oil and gas services intermediary companies, as well as several offshore shell companies. The intermediary received “commissions” for Petrobras projects that were awarded to SBM. According to the DPA, SBM paid these commissions into a Brazilian bank account controlled by the intermediary’s company, as well as into Swiss bank accounts owned by the intermediary’s shell companies. Portions of these commissions were then wired to Petrobras officials. The DPA asserts that certain SBM executives knew about the purpose of such payments; in one instance cited by the DPA, SBM executives met with the intermediary to try to reduce the intermediary’s commission on one Petrobras project to below three percent, but the intermediary explained that the commission could not be reduced because two percent had already been promised to Petrobras officials. SBM also allegedly provided things of value to Petrobras officials, including unspecified gifts, travel, and entertainment.

Angola

From 1997 to 2012, SBM allegedly paid bribes to at least nine Angolan government officials to improperly obtain and retain business from Sociedade Nacional de Combustíveis de Angola, E.P. (Sonangol), the Angolan state-owned oil company. The DPA states that SBM made some of the payments through a Monaco-based oil and gas services intermediary founded by a former SBM executive in the form of “commissions” for projects Sonangol successfully awarded SBM. SBM deposited these commissions into a Swiss bank account controlled by the intermediary, from which funds were then wired to accounts controlled by Sonangol and Sonangol USA Co. (Sonusa) officials. According to the DPA, SBM also made direct payments to Sonangol officials, paid for Sonangol officials’ gifts, travel, and entertainment — including payments for travel to sporting events — and hired and overpaid Sonangol officials’ relatives for positions within SBM. In exchange, SBM received confidential information from Sonangol officials, including, for example, an e-mail to an SBM executive stating that Sonangol would recommend SBM as an affiliate to another oil and gas company on an offshore oil and gas development project.

Equatorial Guinea

From 2008 to 2012, SBM allegedly used the same Monaco-based oil and gas services intermediary it had used for payments to Sonangol officials to make payments to at least nine government officials from the Petroleos de Guinea Equatorial (GEPetrol), the national oil company of Equatorial Guinea, as well as to officials from Equatorial Guinea’s Ministry of Mines, Industry, and Energy (MMIE). The DPA states that SBM deposited commissions into a Swiss bank account controlled by the intermediary, a portion of which the intermediary then wired to bank accounts controlled by the Equatorial Guinean officials. SBM also provided things of value to GEPetrol and MMIE officials in the form of gifts, travel, and entertainment, including paid travel to sporting events, the provision of luxury goods like watches and sport memorabilia, and covering the costs of shipping vehicles to Equatorial Guinea.

Kazakhstan

The DPA states that from 2003 to 2009, SBM “conspired to pay bribes and attempted to pay bribes” to at least one official at KazMunayGas, Kazakhstan’s state-owned oil and gas company, as well as to an employee at the subsidiary of an Italian oil and gas company, which had received a concession from the Kazakhstan government as the operator of the Kashagan oil field development. As discussed in greater detail in the Noteworthy Aspects section below, this allegation regarding the Italian
company’s employee illustrates the ability of the U.S. authorities to apply a broad definition of the term “foreign official.” SBM paid these officials through commissions to two different intermediaries — one of which was based in Monaco, the other in Milan, and both of which the DPA characterized as providing “sales and marketing services” — in exchange for projects successfully awarded to SBM. The DPA states that both of these intermediaries passed along some portion of these commissions to officials at KazMunayGas and to “[a]t least one employee” at the subsidiary of the Italian oil and gas company. In exchange, SBM allegedly obtained confidential information that helped it obtain or retain business, including confidential information about a meeting between the Kazakh government, KazMunayGas, and the Italian oil and gas company subsidiary.

Iraq

From 2009 to 2012, SBM allegedly conspired and attempted to pay bribes to at least two officials at the former Iraqi state-owned and controlled oil company, South Oil Company (SOC) to improperly obtain or retain business. As in the other countries, SBM acted through an intermediary, the same Monaco-based sales and marketing company it has used in Kazakhstan. According to the DPA, SBM deposited “commissions” into the intermediary’s Monaco-based bank accounts with the understanding that the intermediary would transfer portions of the commissions to officials at SOC. SBM also agreed to pay the intermediary $275,000 to induce SOC into preventing a competitor’s reentry into bidding. In addition, SBM allegedly received confidential information from SOC officials — including a letter written by one of its disqualified competitors to reenter a bidding process — which helped SBM to formulate its response.

Disclosure and Remediation Issues

Although SBM voluntarily brought the conduct to the attention of the DOJ, the DPA states that the DOJ did not grant the company full voluntary disclosure credit because the company failed to fully disclose the conduct for approximately one year. SBM, however, received full credit for its cooperation with the government, as it conducted a thorough internal investigation; made factual presentations to the DOJ; made foreign-based employees available for interviews; produced documents to the U.S. from foreign countries; collected, analyzed, and organized voluminous evidence; and conducted an expedited internal investigation into conduct related to one of the intermediaries.

The DPA also notes that the company engaged in remedial measures by “terminating two employees and demoting [another]; seeking and obtaining the return of corrupt funds from agents; terminating longstanding agency relationships with corrupt and questionable third parties; stopped all payments to all of its agents in order to engage in a complete review of its then-current agents [...], hiring a full-time Chief Governance and Compliance Officer with authority to raise issues directly to the Supervisory Board or Audit Committee; engaging an independent company to design a new compliance program; creating a whistleblower hotline; training its sales and marketing personnel; and completing 3 years of monitoring under the supervision of the Dutch authorities.” The DOJ determined that a U.S.-centric independent compliance monitor was unnecessary based on the company’s remediation, “the state of its compliance program,” and SBM’s agreement to report to the DOJ and the U.S. Attorney’s Office for the Southern District of Texas at no less than 12-month intervals during a three-year term.

Based on the factors discussed above, the DOJ determined that SBM was entitled to a 25 percent reduction off the bottom of the U.S. Sentencing Guidelines range. In addition, the U.S. government noted that the penalty assessed would avoid “substantially jeopardizing the continued viability of SBM.”

Noteworthy Aspects:

- Employees of International Oil and Gas Commercial Operators Can Be Considered “Foreign Officials” in Certain Circumstances: In a previous DOJ opinion procedure release (OPR 10-03) in response to a specific inquiry, the DOJ suggested that it would consider even a U.S.-citizen consultant to be a foreign government official for FCPA purposes, if the consultant was “acting in an official capacity” for or on behalf of a foreign government, department, agency, or
instrumentality. This broad interpretation dates back to at least the SEC’s 1986 Ashland Oil case, which defined a British national who served as an unofficial advisor to the Sultan of Oman as a “foreign official” (though he did hold several unrelated official titles) and to the 1990 Young & Rubicam case, in which the U.S. District Court for the District of Connecticut concluded that a Jamaican citizen who had close political ties to Jamaican officials and who served as an executive chairman of an instrumentality of the government constituted a “foreign official.” More recently, in the 2014 Alstom case, the DOJ claimed that a dual U.S.-Egyptian citizen and employee of the U.S.-based Bechtel Corp. was a “foreign official” on the basis of his position as GM of Bechtel’s joint venture with the state-owned and controlled Egyptian Electricity Holding Company (EEHC). According to the DOJ, the joint venture worked “for or on behalf of EEHC,” within the meaning of the FCPA, which qualified the Bechtel employee, who allegedly used his position with the joint venture to secure kickbacks in exchange for parsing out contracts, as a “foreign official” under the statute.

The DOJ applied a similarly broad understanding of the scope of the FCPA’s definition of a “foreign official” to SBM’s conduct in Kazakhstan, where SBM allegedly made payments to an employee of the subsidiary of an Italian oil and gas company through a sales agent. Although the subsidiary of the Italian oil and gas company was not owned or controlled by the Kazakhstan government, the subsidiary had received a concession as the operator of an oil field in Kazakhstan, and, according to the DPA, “in this capacity, ... was acting in the official capacity on behalf of KazMunayGas in awarding contracts for exploration and development of the Kashagan oil field.” Under this reasoning, an employee of a multinational oil and gas company — including a U.S.-based company — that is acting as an operator for a concession from a foreign government authority could be considered a “foreign official” for FCPA purposes.

- **Cooperation with Foreign Authorities**: This case is another example of the increased collaboration among authorities around the world, as well as the increased enforcement by authorities outside the U.S. In its press release, the DOJ expressed its gratitude to the enforcement authorities in Brazil, the Dutch Public Prosecutor’s Office, and Switzerland’s Office of the Attorney General and Federal Office of Justice for providing substantial assistance in gathering evidence during the investigation. As in the VimpelCom settlement, summarized in our FCPA Spring Review 2016, and to the Embraer disposition summarized in our FCPA Winter Review 2017, the DOJ credited SBM’s payment of penalties to the Dutch authorities and the payment of penalties that SBM would likely pay to the Brazilian authorities.

**Keppel Settles with DOJ Over Alleged Violations in Brazil**

On December 22, 2017, Keppel Offshore & Marine Ltd. (Keppel), a Singapore-based company that operates shipyards and repairs and upgrades shipping vessels, and its wholly-owned U.S. subsidiary, Keppel Offshore & Marine USA Inc. (Keppel USA), settled FCPA and related charges with the DOJ, as part of a global disposition that also included authorities in Brazil and Singapore, for a global penalty totaling $422,216,980. Keppel agreed to pay Brazil over $211 million, or 50 percent of the total penalty, and to pay Singapore over $105 million, or 25 percent of the total penalty. The United States, in turn, agreed to credit those amounts, such that it received the remaining $105 million or 25 percent of the penalty, including $4,725,000 paid as a criminal fine on behalf of Keppel USA. The DOJ issued a discussed further below.

The Statements of Fact from the DPA and the plea agreements describe conduct spanning from 2001 through 2014. In particular, the DPA sets out how executives from Keppel and Keppel USA conspired to and paid bribes to employees of Petrobras, the Brazilian state-controlled oil company, and to the Workers’ Party of Brazil, a Brazilian political party that formed part of the Brazilian federal government during the relevant time period, in connection with a number of projects located in Brazil. According to the case documents, the executives sought to conceal the payments by using a consultant who acted as Keppel’s agent from 2000 to 2016. A number of Keppel executives knew these payments were intended to benefit government officials and were connected with the projects in Brazil. The DPA and guilty plea contain numerous examples of high level executives emailing each other regarding the consultant and his companies. These cited emails overtly reference dollar-denominated payments not only to the consultant but also to “friends.” Moreover, the e-mails reflect an understanding of which officials the consultant would approach and a concern with how the payments were to be structured. Pursuant to agreements between companies

© Miller & Chevalier Chartered • millerchevalier.com • Page 15 of 25
controlled by this consultant and Keppel, payments were made into bank accounts controlled by the consultant, including some accounts located in the United States. The Statements of Fact reports that the consultant then transferred money to accounts controlled by Brazilian government officials. Through approximately $55 million in corrupt payments, Keppel and its subsidiaries earned profits of over $350 million.

**Noteworthy Aspects.**

- **Coordination with Singapore and Brazil:** The settlement was the result of a coordinated resolution with Brazil and marked the first time that the DOJ coordinated a public FCPA resolution with the authorities in Singapore. The Leniency Agreement with the Public Prosecutor’s Office in Brazil marks that office’s latest resolution in the Operation Car Wash corruption probe. In Singapore, the company accepted a conditional warning from the Corrupt Practices Investigation Bureau. The global resolution reflects continuing efforts by the DOJ to work with foreign government partners to investigate international corruption schemes and sanction the responsible corporations and individuals.

- **Cooperation and Remediation Credit:** Neither company received voluntary disclosure credit because, while they initiated communication with the Fraud Section, the DOJ already knew of the publicly-reported allegations at that time contact was made. Yet, both Keppel and Keppel USA received a 25 percent discount off of the bottom of the Sentencing Guidelines range. The DOJ press release credited the discount to the companies’ “substantial cooperation” with the investigation and to their having already taken “extensive remedial measures,” including terminating and disciplining involved employees and implementing a new compliance and internal controls system. Furthermore, neither the DPA nor the guilty plea imposed an independent compliance monitor on the companies.

**Actions Against Individuals**

**Florida Businessman Pleads Guilty to FCPA-Related Charges in Connection with DOJ’s Investigation of PDVSA Energy Contracts**

On October 11, 2017, Fernando Ardila-Rueda (Ardila), a Florida businessman, pled guilty to one count of violating and one count of conspiring to violate the FCPA. This action is part of the DOJ’s ongoing investigation into various companies’ contracts with Venezuelan state-owned energy company PDVSA, which we last discussed in our FCPA Spring Review 2017.

In its PDVSA investigation, the DOJ has alleged a conspiracy involving the owners of multiple U.S.-based energy companies who sought to obtain contracts from PDVSA for the provision of equipment and services by paying bribes to PDVSA purchasing managers. According to the indictment, Ardila served as a business partner of Jose Shiera Bastidas (Shiera), who owned several energy companies implicated in the scheme and whose guilty plea we discussed in our FCPA Spring Review 2016. Ardila conspired with Shiera and Roberto Enrique Rincon Fernandez (Rincon), another energy company owner, to facilitate their schemes. Specifically, the indictment alleges that Ardila helped Shiera and Rincon offer bribes to PDVSA officials equal to a percentage of the value of any contracts the officials steered to Shiera’s and Rincon’s companies. Ardila also wired bribe payments to the officials, provided meals and entertainment as bribes, and took steps to conceal the scheme.

Ardila is scheduled to be sentenced on February 8, 2018. Each of the charges to which he pled carries a maximum prison sentence of five years. Ardila was the 10th individual to plead guilty as part of the PDVSA investigation. Other defendants’ pleas were covered in our Spring 2016, Summer 2016, and Spring 2017 publications. The DOJ’s recent indictments against five former PDVSA officials, mentioned above, will be discussed in our FCPA Spring Review 2018.

**Two SBM Executives Plead Guilty to FCPA Charges**

On November 9, 2017, the DOJ announced a DPA with Mace and Zubiate’s former employer,
SBM, later the same month, as well as a guilty plea by SBM USA, SBM’s Houston-based subsidiary.

According to the DPA with SBM, Mace served at various times from 2008 to 2011 as a member of the Board of Directors for two of SBM’s Houston-based subsidiaries — SBM Atlantia and SBM Imodco — and as an executive for SBM Imodco. Zubiate reportedly served at various times as a member of SBM’s sales and marketing team in Latin America and as an executive at SBM USA, SBM Atlantia, and SBM Imodco until February 2016. According to the DOJ’s press release announcing the guilty pleas, Mace admitted he joined SBM’s global conspiracy to make payments to officials in Brazil, Angola, and Equatorial Guinea “by authorizing payments in furtherance of the bribery scheme and deliberately avoided learning that those payments were bribes.” Zubiate similarly admitted that from 1996 through 2012, he and other co-conspirators had used a third-party sales agent in Brazil to make payments to officials at the Brazilian state-owned oil company Petrobras, all in exchange for assistance in SBM’s U.S. subsidiaries winning bids. Maces’ sentencing was scheduled for February 2, 2018, and Zubiate’s for January 31, 2018.

Four Individuals Plead Guilty, a Fifth Charged, in Rolls-Royce Bribery Scheme

The DOJ announced that four individuals have pleaded guilty and a fifth has been charged in relation to activities that the DOJ has alleged enabled Rolls-Royce Energy Systems Inc. (RRESI) — a subsidiary of Rolls-Royce plc — to obtain an unfair advantage in securing business from foreign governments around the world. Among these was a 2009-2012 alleged bribery scheme designed to help RRESI win and maintain contracts with Asia Gas Pipeline LLP (AGP), a joint venture between Kazakh and Chinese state-owned entities that was created for the purpose of constructing a gas pipeline connecting Central Asia and China. We previously reported on this investigation in our FCPA Winter Review 2017, where we explained that Rolls-Royce had entered into deferred prosecution or leniency agreements with the U.S., U.K., and Brazil.

According to recently unsealed court documents, Petros Contoguris, CEO of a Turkish oil and gas advisory company, and Andreas Kohler, managing director at an international engineering and consulting firm, conspired with Rolls-Royce executives and employees to pay kickbacks to Kohler’s consulting firm. The kickbacks, which were disguised as legitimate commissions paid to Contoguris’s company, were in fact paid to high-ranking Kazakh officials to secure their help in securing AGP contracts for Rolls-Royce.

Of the Rolls-Royce employees, James Finley, a U.K. citizen living in Taiwan and a former senior executive in the company’s energy operation, was charged on July 21, 2017 and pled guilty on July 28, 2017 to violating and conspiring to violate the FCPA; Aloysius Johannes Jozef Zuurhout of the Netherlands, a former energy sales employee, was charged June 9, 2017 and pled guilty on June 13, 2017 to conspiring to violate the FCPA; and Keith Barnett of Texas, a former regional director in energy, was charged December 20, 2016 and pled guilty on December 28, 2016 to conspiring to violate the FCPA. In addition to the AGP conspiracy, all three admitted to participating in other foreign bribery schemes that benefitted Rolls-Royce as far back as 1999.

Andreas Kohler of Austria, whose firm received and forwarded the kickback payments, was charged June 6, 2017 and pled guilty on July 20, 2017 to conspiring to violate the FCPA. Petros Contoguris, a Greek citizen residing in Turkey, where he ran the advisory company that disguised the kickbacks, was indicted on October 12, 2017 and charged with several counts of violating the FCPA, laundering money, and conspiring to commit those offenses. He is believed to be outside the U.S. and has yet to be apprehended. Of the defendants who have pleaded guilty, all are scheduled to be sentenced in 2018.

The prosecutions were brought in the Southern District of Ohio, where RRESI held bank accounts from which the corrupt payments were made. The DOJ has touted these indictments and guilty pleas as proof of the Department’s commitment to prosecuting individuals, not just corporations, for violations of the FCPA.

Former Embraer Executive Pleads Guilty to Participating in Bribery Scheme Detailed in Embraer’s 2016 Deferred Prosecution Agreement
On December 21, 2017, a former sales executive of Brazilian aircraft manufacturer Embraer S.A. pled guilty in the Southern District of New York to charges that he engaged in a scheme to bribe Saudi officials in exchange for aircraft contracts. The scheme was part of a larger pattern of foreign bribery at Embraer that was the basis for a 2016 FCPA disposition on which we reported in our FCPA Winter Review 2017.

The Information states that Colin Steven, a U.K. citizen residing in the United Arab Emirates, admitted that he caused Embraer to make roughly $1.5 million in bribe payments from a U.S. bank account to an official for Saudi Arabia’s national oil company. In exchange, the official ensured Embraer would be awarded a contract for three new aircraft, worth approximately $93 million. According to the Information, Steven had the bribe payments funneled through a South African intermediary company that performed no legitimate services. Steven also arranged for a portion of the payments, totaling about $130,000, to be sent from the South African company to his personal bank account as a kickback. Steven admitted to orchestrating the bribery and kickback scheme, laundering the proceeds, and lying to FBI agents during their investigation. He is scheduled to be sentenced on June 21, 2018.

Steven’s guilty plea comes more than a year after Embraer resolved DOJ and SEC charges related to the Saudi Arabian scheme and similar issues in the Dominican Republic and Mozambique. Specifically, Embraer entered into a three-year DPA with DOJ while also agreeing to pay a $107 million penalty, implement various compliance program and remediation measures, and retain an independent compliance monitor for three years. To settle with the SEC, Embraer separately agreed to pay nearly $100 million in disgorgement and prejudgment interest. Brazilian authorities, in cooperation with U.S. law enforcement, have charged 11 other individuals for their alleged involvement in the Dominican Republic payments, while authorities in Saudi Arabia have charged two others in connection with Embraer’s activities there.

Senior Member of Keppel Legal Department Pleads Guilty

Nearly four months prior to the Keppel corporate settlement discussed above, Keppel senior in-house counsel Jeffrey Chow pled guilty to one count of conspiracy to violate the anti-bribery provision of the FCPA. According to the charging documents, Chow held various positions in Keppel’s legal department between 1990 and 2017, including administrative manager, general manager, and director. At his August 29, 2017 plea hearing, Chow explained that his responsibilities over his time at Keppel included drafting and preparing contracts with Keppel’s agents. He admitted to realizing that Keppel was overpaying a Brazilian consultant by millions of dollars in order for that consultant to then pay bribes to Petrobras and political party officials. Despite that knowledge, Chow drafted contracts between Keppel and the consultant that were ultimately used to pay bribes that led Keppel to be awarded projects with Petrobras and Sete Brasil. The court accepted Chow’s plea on October 24, 2017 and Chow is scheduled to be sentenced in May 2018.

Ongoing Policy Developments and Related Litigation

DOJ Announces New “FCPA Corporate Enforcement Policy” to Replace the FCPA Pilot Program

As described in a Miller & Chevalier International Alert, on November 29, 2017, the DOJ introduced a new FCPA Corporate Enforcement Policy, which expanded certain aspects of and effectively replaced the Department’s FCPA Pilot Program. The new Policy largely maintains the incentive structure of the Pilot Program, in that both policies offer the possibility of reduced penalties and other leniency for companies that (1) voluntarily self-disclose FCPA-related misconduct; (2) fully cooperate with the DOJ in any subsequent investigation; and (3) implement timely and appropriate remediation. The new Policy is incorporated into the U.S. Attorneys’ Manual as Section 9-47.120.

Although the Pilot Program appears to be an impetus for the new Policy, there are some notable differences between the two. Companies that properly satisfied the Pilot Program’s three main requirements could receive “up to a 50% reduction” off the bottom end of the applicable U.S. Sentencing Guidelines fine range, and under the program the DOJ would “consider” a
declination of prosecution. The new Policy, in contrast, offers a “presumption” of a declination and, if the DOJ nonetheless deems a criminal resolution “warranted,” the Fraud Section will generally provide a 50 percent (rather than an “up to 50” percent) reduction off the bottom end of the Sentencing Guidelines fine range and not require appointment of a monitor.

The new Policy also retains many of the Pilot Program’s detailed criteria that companies must satisfy in order to be eligible for full disclosure credit. For example, like the Pilot Program before it, the new Policy defines voluntary self-disclosure to include disclosure of relevant facts about “all individuals involved in the violation of law” [emphasis added]. Similarly, under both the old Pilot Program and the new Policy, the requirement of full cooperation in FCPA matters requires that the company make available “those company officers and employees who possess relevant information” for interview by the DOJ, at least when the agency so requests. This requirement explicitly includes officers and employees located overseas, as well as officers and employees no longer associated with the company. Based on this continuing requirement, companies may wish to ensure that they have processes in place to encourage all relevant individuals to cooperate with the DOJ in the event of a disclosure, for example, through provisions in separation agreements conditioning severance pay on such cooperation.

At the same time, the new Policy also tightens some criteria that companies must satisfy for full disclosure credit. For example, disclosing companies must make “agents” available for interviews, not only officers and employees, as was required under the Pilot Program. Similarly, in order to receive credit for timely and appropriate remediation, a company must appropriately retain all relevant business records, which under the new Policy includes a requirement that companies expressly prohibit employee use of "software that generates but does not appropriately retain business records or communications." The scope of this language is potentially quite broad; on its face, software that falls under this provision if used for business purposes is likely to include outside messaging apps that automatically delete messages after a certain period of time, such as Snapchat or Wickr; outside apps or applications that use end-to-end encryption, such as WhatsApp or Telegram; and even outside e-mail programs, such as Gmail. While the use of such software has long posed challenges in FCPA investigations, it now also threatens to disqualify companies from receiving substantial benefits under the Corporate Enforcement Policy. Until or unless this aspect of the Policy is further clarified, the Policy’s language suggests that the DOJ expects companies to at least (1) clearly instruct employees regarding what types of communication software are permissible to use in connection with business matters; and (2) effectively implement and enforce such policies.

In all, the new Policy largely strengthens the incentives previously available under the Pilot Program, continuing the DOJ’s longstanding strategy of encouraging companies to voluntarily self-disclose and cooperate with its investigations.

SEC Ratifies the Appointment of Its ALJs; Solicitor General Reverses Course to Take Consistent Position Before Supreme Court

In November 2017, the SEC ratified the appointments of its five administrative law judges (ALJs), exercising its authority as “head of a department” to appoint these ALJs as inferior officers in compliance with the Appointments Clause of the Constitution. The SEC’s action comes in the midst of ongoing litigation as to whether the ALJs’ decision-making authority for administrative actions before the SEC renders them “inferior officers” — whose appointment is subject to the Appointments Clause — or merely employees who may be hired through a more informal procedure. As stated in the Ratification Order, the agency carried out this action explicitly in order “[t]o put to rest any claim that administrative proceedings pending before, or presided over by, Commission administrative law judges violate the Appointments Clause.”

This position is a departure from the SEC’s prior stance in litigation that its hearing officers are employees and did not require appointment by the president, the courts, or the agency head. The SEC’s ALJs preside over administrative enforcement actions against individuals and entities that have allegedly violated federal securities laws. The ALJs are able to, among other things, hold hearings and issue initial decisions. Those decisions are deemed to be the actions of the SEC if further review is not sought or a request for review is denied by the SEC.
The ratification order sets out procedures for matters currently pending before the Commission, whether the ALJ has issued an initial decision or not, but does not address any potential claims by people previously sanctioned by the SEC through actions of ALJs. The order also acknowledged that the Solicitor General had, the day before, filed a brief before the Supreme Court in *Lucia v. SEC*, agreeing with the petitioner that the SEC’s ALJs are inferior officers and not employees. In the underlying decision, the U.S. Court of Appeals for the D.C. Circuit held that the ALJs were employees rather than officers and therefore maintained the constitutionality of the hearing system, as discussed in our FCPA Summer Review 2017. The brief acknowledged the circuit split on the constitutionality issue (which is discussed in our FCPA Winter Review 2017), requested that the petition for writ of certiorari be granted, and asked that amicus be appointed to defend the contrary position. In January 2018, the Supreme Court granted the petition in *Lucia.*

**International Developments**

**HSBC Enters into First Ever Corporate Criminal Settlement in France**

On November 14, 2017, HSBC Private Bank (Suisse) SA (HSBC) entered into the first ever French Convention Judiciaire d’Intérêt Public (CJIP) or Judicial Agreement in the Public Interest. The CJIP — which has frequently been compared to U.S.-style DPAs and NPAs — is a mechanism designed to allow for the settlement of corporate criminal cases created by France’s new anti-corruption legislation, Sapin II, which came into force in December 2016.

Under French law, French enforcement officials can offer a CJIP to any legal entity suspected of having committed a variety of financial crimes, including bribery and laundering the proceeds of tax fraud. A company entering into a CJIP can be fined up to 30 percent of its average annual turnover over the last three years at the time the offense was committed and can be required to implement a compliance program monitored by France’s new anti-corruption agency, the Agence Française Anticorruption.

The English version of the HSBC CJIP indicates that, in 2006 and 2007, HSBC concealed the assets of over 8,900 individuals from French tax authorities, thereby knowingly aiding and abetting violations of French tax laws. In order to resolve the matter, HSBC agreed to pay a total of €300 million in disgorgement, penalties, and damages to the French state.

The disgorgement of €86.4 million and penalties of €71.6 million together total 30 percent of the HSBC’s average annual turnover for the last three years. The French authorities indicated that they imposed the highest possibly penalty because the facts were particularly serious, the violation continued for many years, HSBC did not voluntarily disclose wrongdoing to the French authorities and provided only minimal cooperation with the French authorities during the investigation, and did not admit liability. Although the CJIP acknowledges that at the time the investigation began, French law did not provide incentives encouraging full cooperation, French authorities did not reduce the fine amount to recognize this fact. The additional €142 million constitutes damages owed to the French state.

The severity of the penalty and the speed with which this case was resolved after Sapin II’s entry into force suggests that French authorities are willing and eager to make use of the prosecutorial tools provided to them under the new law. This case may mark a turning point for the enforcement of financial crimes in France.

**Argentina Introduces Corporate Liability and Compliance Standards in New Anti-Corruption Law**

On December 1, 2017, Argentina introduced [Law 27.401](http://example.com), amending certain corruption-related provisions already in the Criminal Code and establishing corporate criminal liability for certain corruption offenses, alongside broad vicarious liability provisions and significant potential penalties. The new law, which will take effect on March 1, 2018, allows companies potentially to escape liability by self-reporting violations and returning any undue benefits if the violation occurs after an “adequate” compliance program that meets minimum requirements set forth in the law is instituted. The law also introduces a settlement mechanism that offers lower and predictable penalties for companies that cooperate with enforcement authorities.
The new law imposes liability for the following offenses:

- Bribery of or influence peddling involving public officials, whether domestic or international, in accordance with Articles 258 and 258 bis of the Argentine Criminal Code;
- The offense of “negotiations incompatible with the exercise of public functions,” in accordance with Article 265 of the Code, which imposes liability on a public official who acts upon a personal interest, whether directly or indirectly, in any contract or transaction in which the official plays a role by the virtue of his or her position;
- The offense of “concusión” (loosely translated as “extortion”), in accordance with Article 268 of the Code, which imposes liability on a public official who converts, for the official’s own benefit or that of a third party, undue funds obtained through an improper request or demand;
- Illicit enrichment of public officials and employees, in accordance with Articles 268(1) and 268(2) of the Code; and
- The offense of “aggravated balances and reports,” in accordance with Article 300 bis of the Code, which imposes liability for the misrepresentation of certain books and records and accounting information by a founder, director, administrator, liquidator, or trustee of an entity with the intent to conceal the commission of offenses defined in Articles 258 and 258 bis, namely, bribery and influence peddling.

The new law governs the conduct of domestic and foreign legal entities, including those with state ownership or control. Geographically, the law amends the Criminal Code to apply to all offenses committed in or whose effects occur in Argentina, as well as offenses committed outside of Argentina by Argentine officials acting in an official capacity. With respect to bribery of foreign officials, the law also applies outside of Argentina to Argentine citizens and to legal entities domiciled in Argentina, whether under bylaws or through the existence of any establishments or branches in the country.

A legal entity may be liable regardless of whether it committed the offense directly or if it was committed indirectly on the entity’s behalf, in its interest, or for its benefit. Indeed, an entity may be responsible if the action made in its interest or for its benefit is committed by an unauthorized third party, so long as the entity had even tacitly ratified the third party’s conduct. The only exception to vicarious liability is if the person who committed the offense acted strictly for his or her own benefit, without generating any benefit for the entity.

The limitations period under the law is six years from the commission of the offense and it expressly provides for successor liability in case of an acquisition, merger, or other corporate transformation.

The law provides a range of penalties, including fines of two to five times the undue benefit obtained or that would have been obtained; a total or partial suspension of the legal entity’s activities of up to 10 years; debarment, dissolution and liquidation of the entity’s legal status; and others. The law also grants courts discretion to consider a number of factors in determining a penalty. These factors are: failure to comply with internal rules and procedures; the number and seniority of officials, employees, and others involved; lack of oversight over the principal actors and other participants; the extent of the harm; the amount of money involved; the size, nature, and finances of the legal entity; self-reporting to the authorities; subsequent conduct; disposition to mitigate or repair the harm; and recidivism. With respect to the last factor, the law provides a presumption of recidivism if the legal entity is sanctioned for an offense within three years of a previous conviction. Notably, suspension and dissolution penalties do not apply if there is an essential need to maintain the operational continuity of the legal entity or some specific project or service, though the law does not clarify those circumstances.

Notwithstanding the gravity of potential penalties, a legal entity may be completely exempted from liability if it takes the following steps, concurrently:

- Self-reports the violation as a result of its internal detection and investigation;
- Had implemented an adequate system of control and supervision before the conduct at issue, whose breach would have required an effort by the participants in the offense; and

- Returns the undue benefit.

The second of these requirements references provisions of Law 27.401 that define the benefits and elements of an “integrity program” that companies subject to the law may adopt. As defined in the law, the program should be tailored to a company’s risk profile, including its activities, size, and financial capacity. The program must include (1) a code of ethics or conduct, or an equivalent set of integrity-oriented policies and procedures applicable to all directors, administrators, and employees; (2) specific rules and procedures to prevent unlawful conduct in the context of public tenders, the execution of public contracts, or any other interaction with the public sector; and (3) periodic training. Beyond these required elements, the program may include any of 10 additional components, such as periodic risk analysis, visible and clear support from senior leadership and management, reporting mechanisms, whistleblower protection, third-party monitoring, M&A due diligence, and more. Somewhat unique in the context of written global anti-corruption compliance standards, one of the optional elements is compliance with the regulatory requirements with regard to integrity programs of respective authorities at the national police, provincial, municipal, and community levels. Presumably, the rationale behind the optional elements is that companies would adopt them as appropriate based on their risk profile.

Although the law generally does not require companies to have an integrity program, it includes an exception for companies that contract with the Argentine federal government, which must have an integrity program in place to engage in certain types of government contracts (e.g., contracts that under local law require approval by a Minister or higher ranking government official and certain public works or concession contracts).

The law also introduces a new settlement mechanism called “Effective Collaboration Agreement,” which has some commonalities with a DPA under U.S. enforcement practice and offers certain leniency to cooperating entities. In entering into such an Agreement with the authorities, an entity commits to providing accurate, useful, and verifiable information regarding relevant facts, identities of participants, and recovery of illicit proceeds. The entity would have to also agree to pay half the minimum applicable fine, return any illicit assets or proceeds, and forfeit any goods that would presumably be confiscated in case of conviction. Optional components of an Agreement include community service, disciplinary measures against direct participants, and implementation of or improvements to an existing integrity program. If a review of the Agreement by the prosecutors or the judge, conducted within one year of its execution, confirms that the information provided by the entity under the Agreement was truthful and useful, the imposed sentence cannot exceed that in the Agreement. If the information provided is not verified, the settlement is nullified and the process continues in accordance with applicable rules.

The Argentine Congress passed the law on November 8, 2017, and it was signed into law by President Macri on December 1, 2017. The law will take full effect 90 days after its official publication, on March 1, 2018.

One of the primary motivations behind the new law is a requirement by the Organization for Economic Co-operation and Development (OECD) – which Argentina has been seeking to join – that member states impose corporate liability for foreign bribery and the OECD’s finding that Argentina was not in compliance with this requirement, despite being a signatory to the OECD Anti-Bribery Convention. While it is too early to tell how the authorities might enforce the new law, the carrot-and-stick approach appears at least partly intended to motivate companies to implement meaningful anti-corruption compliance programs.

Peru Introduces Corporate Liability for Corruption Offenses with a Compliance Program Defense

On January 1, 2018, Peruvian Law 30424 went into effect, introducing corporate liability for existing criminal offenses related to corruption, money laundering, and terrorist financing. The law was originally scheduled to take effect in July 2017, but Legislative Decree 1352, adopted on January 6, 2017, amended the original version of Law 30424, broadening the range of applicable
offenses and shifting the effective date of the entire law to January 1, 2018.

Under the new law, legal entities may be liable for domestic and international bribery of public servants or officials, expressly including officials in judicial positions (as the corresponding provisions are defined in the Criminal Code), as well as for certain offenses related to money laundering and terrorist financing defined in other legislation. In addition to direct liability, legal entities may be liable for conduct carried out in the legal entity’s name, on its behalf, or for its benefit by any of the following:

- Partners, directors, de facto or legal administrators, legal representatives, or attorneys-in-fact of the legal entity or any of its branches or subsidiaries;
- Any person who was under the authority and control of a person or entity in paragraph (a) and committed the offense by their order or authorization; or
- Any person within the scope of paragraph (b), where the commission of the offense was possible because the person or entity in paragraph (a) did not fulfill his or her duties of supervision, oversight, and control with respect to the conduct at issue.

A legal entity is exempt from corporate liability only if an individual who commits the offense does so exclusively for his or her own benefit or the benefit of a third party that is distinct from the legal entity.

Violations of the law can result in two types of penalties. The first is a fine, the amount of which is derived from either the undue benefit or the legal entity’s annual income. The second is a corporate “disqualification,” which can take one of several enumerated forms, from suspension of an entity’s social activities to debarment, nullification of various administrative or municipal licenses, or dissolution.

The law lists several mitigating circumstances that can reduce potential penalties, including cooperation with authorities, impeding the harm caused by the offense, full or partial reparation of the damages, and the adoption and implementation of a “prevention model” (akin to a compliance program) after the commission of an offense but before trial. The law grants courts substantial discretion with regard to the imposition of penalties, including the ability to suspend a penalty by requiring a legal entity to: (1) provide full compensation for the damage caused by the offense; and (2) adopt and implement a prevention model. If the legal entity does not become subject to another criminal proceeding within the suspension period, the court may nullify the imposed sanction and dismiss the case upon confirming that the legal entity satisfied the compensation and prevention model requirements.

To be considered sufficient under the law, a prevention model must be tailored to a legal entity’s nature, risks, needs, and characteristics, and must contain adequate monitoring and control measures to prevent the offenses covered by this law or significantly reduce the risk of their commission. It must also include, at a minimum, the following elements (with an exception for small enterprises):

- A person (or body) in charge of prevention, appointed by the highest administrative body of the legal entity and able to exercise this function autonomously;
- Identification, evaluation, and mitigation of risks related to the offenses covered by this law;
- Reporting procedures;
- Dissemination and periodic training; and
- Continuous evaluation and monitoring of the prevention model.

The law states that if an adequate prevention model is in place, corporate liability will not attach if an individual commits a proscribed offense by fraudulently eluding a duly implemented prevention model.
In all, the new law reflects a number of standards called for by the OECD Anti-Bribery Convention. Peru has not yet acceded to the Convention but has agreed to adhere to the Convention’s standards under an OECD Country Programme, and the new law appears designed to address certain gaps in the country’s legal framework for reducing domestic and international corruption. With corruption allegations recently reaching the highest levels of Peru’s government, the new law comes into force at an opportune time for the country’s enforcement authorities to put it into practice.

**Miller & Chevalier Upcoming Speaking Engagements and Recent Articles**

**Upcoming Speaking Engagements**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>02.15.18</td>
<td>ABA Section of International Law Anti-Corruption Committee Meeting</td>
<td>Homer E. Moyer, Jr.</td>
</tr>
<tr>
<td>02.22.18</td>
<td>ABA Section of International Law U.S. Economic Year-in-Review Event</td>
<td>Abigail E. Cotterill</td>
</tr>
<tr>
<td>02.22.18</td>
<td>WIIT Panel: Customs 101 - The Basics of Cross-Border Transactions</td>
<td>Barbara D. Linney</td>
</tr>
<tr>
<td>02.28.18</td>
<td>ABA Section of International Law U.S. Export Controls Year-in-Review Event</td>
<td>Abigail E. Cotterill</td>
</tr>
<tr>
<td>03.02.18</td>
<td>J. Reuben Clark Law Society Event</td>
<td>James G. Tillen, Marc Alain Bohn</td>
</tr>
<tr>
<td>03.09.18</td>
<td>GW Law Event: Emerging Issues in FCPA Enforcement</td>
<td>James G. Tillen</td>
</tr>
<tr>
<td>03.09.18</td>
<td>14th Annual TRACE Forum</td>
<td>Alejandra Montenegro Almonte</td>
</tr>
<tr>
<td>03.12.18</td>
<td>ACI 5th Mexico Summit on Anti-Corruption</td>
<td>Matteson Ellis</td>
</tr>
<tr>
<td>03.14.18</td>
<td>Transparency International’s Western Canada Anti-Corruption Conference</td>
<td>Kathryn Cameron Atkinson</td>
</tr>
<tr>
<td>03.21.18</td>
<td>CS Conference on Anti-Corruption</td>
<td>William P. Barry</td>
</tr>
<tr>
<td>03.22.18</td>
<td>3rd Annual GIR Live DC</td>
<td>Kathryn Cameron Atkinson</td>
</tr>
</tbody>
</table>

**Recent Articles**

<table>
<thead>
<tr>
<th>Date</th>
<th>Article</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>02.06.18</td>
<td>Sanctions Showdown Looms in U.S. and Cryptocurrency</td>
<td>Brian J. Fleming</td>
</tr>
<tr>
<td>02.01.18</td>
<td>Trade Compliance Flash: United States Names Russian Oligarchs: Promises Additional Sanctions Required by CAATSA</td>
<td>Barbara D. Linney, Collmann Griffin, Patrick M. Stewart</td>
</tr>
<tr>
<td>01.30.18</td>
<td>The ABA Hosts Boni De Moraes Soares, a Federal Prosecutor from Brazil’s Advocacia Geral Da União</td>
<td>Leah Moushey</td>
</tr>
<tr>
<td>01.16.18</td>
<td>Trade Compliance Flash: United States Issues &quot;Last Chance&quot; Waiver of Iran Sanctions and Steps Up Sanctions Against Iranian Weapons Proliferators and Human Rights Abusers</td>
<td>Brian J. Fleming, Barbara D. Linney, Collmann Griffin; also published in the January 2018 issue of WorldECR</td>
</tr>
<tr>
<td>12.20.17</td>
<td>FCPA Enforcement Picks Up in 2nd Half of 2017</td>
<td>James G. Tillen, Michael Skopets</td>
</tr>
<tr>
<td>12.19.17</td>
<td>U.S. Export Controls and Economic Sanctions Enforcement - Seven Trends to Watch in 2018</td>
<td>Timothy P. O'Toole</td>
</tr>
<tr>
<td>12.14.17</td>
<td>New DOJ Enforcement Policy Takes Aim at Messaging Apps</td>
<td>Nate Lankford, Aiysha S. Hussain</td>
</tr>
</tbody>
</table>
Our top 10 calculations for global settlements involving the FCPA reflect only the settlements of which we are aware, and may therefore be incomplete. In determining a collective penalty amount for comparative purposes, our top 10 calculations combine all actions brought against a particular company and its subsidiaries and affiliates.

The information contained in this communication is not intended as legal advice or as an opinion on specific facts. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. For more information, please contact one of the senders or your existing Miller & Chevalier lawyer contact. The invitation to contact the firm and its lawyers is not to be construed as a solicitation for legal work. Any new lawyer-client relationship will be confirmed in writing.

This, and related communications, are protected by copyright laws and treaties. You may make a single copy for personal use. You may make copies for others, but not for commercial purposes. If you give a copy to anyone else, it must be in its original, unmodified form, and must include all attributions of authorship, copyright notices, and republication notices. Except as described above, it is unlawful to copy, republish, redistribute, and/or alter this presentation without prior written consent of the copyright holder.
Hackers’ successes in 2017 were a stern warning. Despite efforts to implement system-wide defences, even the largest corporations proved vulnerable.

Hackers are now finding their way in through the tiniest of openings. Two of the biggest cyber theft headlines of the year involved Equifax, where an attack netted the personal information of 143 million people, and Deloitte, where the breach was first thought limited to a “small number of emails” but later found to include all of the firm’s administrator accounts as well as its entire internal email system, including attachments with confidential security and design materials, login information and IP addresses.

While both breaches were of substantial magnitude – and the damage to those firms’ reputations alone severe – at least Equifax and Deloitte were able to identify and quantify the data that had been hacked. But what if they could not have quantified what was compromised?

GDPR looms

Data making its way into your servers without your knowledge could put your organisation at risk – risk that is increasing given the impending GDPR restrictions and the harsh consequences for violating them.

Data can infiltrate your systems unnoticed in many ways – for insidious purposes or unwittingly. It can come in with employees: existing employees, new hires, or through a merger or acquisition. Exposure is particularly high in organisations where employees use their own devices (BYOD) – laptops, tablets, mobile phones – and access online services such as personal webmail accounts and cloud storage (iCloud, Dropbox etc). Employees can generate personal data outside the work environment which, when reintroduced into the workplace – for example, when an employee synchronises a mobile device – becomes integrated with data stored on the company server.

Consider an employee who has saved work product from a previous job and brought it into your organisation. In an IP theft lawsuit it would be compromising, costly to defend, and challenging to prove there was no collusion with the employee to steal trade secrets. Your company most likely performs background checks on employees pre-hire, but are you just as careful about ensuring unwanted data is not being brought in by new hires? Are you taking meaningful steps to prevent it or simply stating that there is a policy against it?

In an environment of increasingly strict regulation and rigid enforcement, the job of protecting your organisation against unwanted data has become tougher and the related financial risk greater. Organisations must be aware of the data they have, the type and the sensitivity of that data. As well as policies, controls should be in place to ensure employees and external parties are not bringing in data that could put the organisation at risk – and, most importantly, they must be enforced.

While most companies have implemented security procedures to ensure outside contractors do not access or infiltrate their data, they have not been as careful with people inside their organisations. They have been lax on such standard practices as locking down the use of external drives and implementing policies that prohibit copying data onto the network or accessing personal webmail accounts. Even when policies are in place it can be difficult to know whether or not employees are adhering to them without technical preventive, detective and corrective controls, and periodic review to support security and acceptable use policies.

Know your data

If there is a breach, would you know what was there? How do you respond properly to a breach, defend yourself in a lawsuit or protect your reputation if you have not taken steps to screen data coming into your organisation?

Best practices for protecting the organisation from unwanted and potentially damaging data remain as the following: training, policies for proper data construction, controls around the policies, and auditing the controls. But companies should also be committed to knowing all the data that exists in their networks, and finding out how data can enter their networks. For this, proper Information Governance and audit is key.
Controlling Forensic Accounting Costs

BY ROBERT S. STEINBERG

Lawyers are sometimes astounded at the final bill submitted by their forensic accountant. “What took so much time?” they will ask in disbelief. Of course the answer usually is, “I did just what you asked me to do.”

The problem is that lawyers are often unspecific about what they ask of a forensic expert. They will call and say something like, “I have a complex case and need someone to summarize all of the financial stuff.” Then they will send the accountant boxes of documents produced by either or both parties without specific instructions regarding what the expert is to do with them.

Reviewing and summarizing documents is time-consuming and unnecessary if most will not be introduced into evidence or used in developing evidence or used to assess what additional documents are needed. Thus, open-ended engagements without regard to the facts and needs of the particular case will result in unnecessarily high forensic accounting fees.

It is helpful to have a clear perspective of each person’s role in the litigation. Think of the main players as comprising a three-tiered structure analogous to the military. The client is the commander in chief, the one who initiates the divorce action and makes the ultimate decisions about settlement. The lawyer is the general in charge of carrying out the litigation, planning strategy, deciding what evidence is needed and how to present the case to the court. The forensic accountant is the reconnaissance officer who must find and summarize the financial evidence.

The lawyer who understands these roles will: (1) communicate more effectively to the forensic accountant exactly what evidence must be presented in the case; (2) provide specific instructions as to each item of income,
Almost every family lawyer in an alimony case will ask the work: extraordinarily detailed procedures and analysis that are sic accountant. Searching for unreported income involves should the lawyer authorize an income probe by the foren- closure documents that reflect income and expenses. Avoid not surprisingly, a spouse will often accuse a partner of gathering of evidence. While forensic accountants experienced in the divorce field may already have this material, never assume so.

Discovering and substantiating income
Not surprisingly, a spouse will often accuse a partner of under-reporting income on tax returns or in financial disclosure documents that reflect income and expenses. Avoid sending the forensic accountant off on a wild goose chase. Only if there is a factual predicate in probative evidence should the lawyer authorize an income probe by the forensic accountant. Searching for unreported income involves extraordinarily detailed procedures and analysis that are time consuming and expensive. Expansive discovery is required to obtain circumstantial evidence of income, such as net worth increases, bank deposits, and cash expenditures. The attorney should expect the other side to vigorously oppose discovery requests resulting in additional trial preparation and court time. These intrusive and expensive measures should never be commenced on mere suspicions. Undertake a thorough effort-versus-rewards analysis by discussing with the forensic accountant:

- The likelihood of finding unreported income;
- The discovery and procedures required to bring the income to light;
- The amount of income likely to be found versus the costs to find it.

Then discuss the results of this analysis with the client. Discuss how to handle other legal or factual issues concerning income before the forensic accountant begins work:

- "Income" as it is defined under alimony and child support statutes, which may or may not be the same;
- "Bonuses" in relation to arriving at current wages to be reported on the statement or disclosure of income;
- Dramatic year-to-year fluctuations in income;
- Income slowdowns or RAIDS (Recently Acquired Income Deficiency);
- Undistributed income from trusts, S corporations, and partnerships.

Marital standard of living
Almost every family lawyer in an alimony case will ask the forensic accountant for a lifestyle analysis. The lawyer may or may not understand what this means. To a forensic accountant, it will most certainly mean conducting a comprehensive analysis of the parties’ spending during some agreed upon period preceding the filing for divorce. Generally, the forensic accountant will ask both parties for bank account statements, check registers and cancelled checks, brokerage accounts with check-writing privileges, and credit card statements (both business and personal). The accountant will summarize and categorize all disbursements, making certain that all transactions for the period are captured. The forensic accountant must interview the client intensively and attend the other spouse’s deposition or at least read the transcript. This will assist in a comprehensive analysis of the monthly spouse’s expenses of the parties, whether paid by them personally or through some entity. Obviously, this is a laborious project with a high price tag. Should it always be undertaken and, if so, when?

Let me first address when. At the commencement of a case one of the first things a lawyer must address is disclosure. Some lawyers dump the entire process on the forensic accountant. This is a mistake. Involving the expert in this aspect of the case adds nothing but expense to the process. Of course, there are exceptions to every rule, such as when the case is document intensive and the accountant is asked to maintain a document database for production.

One component of disclosure is the filing of the income, expense, assets and liabilities statement. Because the statement is usually due early in the case, before substantial discovery has transpired, it often is amended later in the proceedings. Prepare the initial statement and indicate clearly that it is preliminary, prepared without the help of an accountant, and based on initially available information provided by the client. State too that it does not take into account the impact of income taxes on alimony or equitable distribution considerations. Use common sense in preparing the statement and, if necessary, customize it to the facts of the case, e.g., if the couple has more than one home, use a separate column for each home’s expenses.

As to the second question, the answer is an emphatic no. A comprehensive lifestyle analysis should not be undertaken routinely. Often in small cases, the standard of living can be deduced from examining a few monthly bills. Stipulations and requests for admission as to specific expenses are underused in resolving disputes regarding lifestyle. Use lifestyle analysis techniques where the standard of living is lavish and where payments are made from many sources, thus making an assessment of expenses difficult, or where there is significant commingling of personal and business affairs. Discuss with your forensic accountant how sophisticated the analysis should be and what summaries to prepare.

The lawyer will usually ask the forensic accountant to
prepare a schedule of assets and liabilities. The valuation date for the schedule may be the date of filing or another date determined by the court to be most equitable under the circumstances. Thus, the lawyer may argue to the court that the separation or trial date is a more appropriate valuation date for some or all of the assets and liabilities. Multiple valuations must then be prepared. Requiring multiple valuation dates for a business will greatly increase business valuation costs. Whenever possible, the parties should attempt to stipulate to the valuation date for each asset and liability.

**Be date specific**

Specifically instruct the forensic accountant as to the valuation date to be employed. Do not assume anything. Sometimes practical considerations may dictate a date at the month's end preceding or following the valuation date; or at the end of the calendar quarter. Such is often the case when financial statements and general ledgers are prepared quarterly and tax returns are filed annually. For example, if the petition was filed on January 17, 2006, financial information from December 31, 2005, could be used.

What if the petition were to be filed on February 15, 2006? Would using the December financials be appropriate for the valuation? Could the quarterly financials be used for a March 31, 2006, filing? Is there an objection that they include post-petition nonmarital earnings? The attorney and forensic accountant should explore these questions. The proper solution will be that which promotes an equitable distribution of marital assets and it will vary from case to case.

If the forensic accountant has business valuation credentials and is to value one spouse's business interests, discuss with the expert the methodology to be employed. Adjudicated precedent may dictate certain methodology or prohibit others. An example is professional goodwill. Another potential disparity from common business valuation standards is whether the discounted future cash-flow method under the income approach may be employed in valuing a business in a divorce case. Some have questioned its appropriateness because the method utilizes post-petition nonmarital earnings to value the business. Agreement on these matters will preclude unnecessary valuation work leading to testimony that unexpectedly is not permitted upon objection.

Remember that a forensic accountant is not a banker, an underwriter, a mortgage banker, a real estate appraiser, a bond expert, an antiques dealer, an actuary, or per se a business valuation expert. Unless he or she has additional credentials, seek other expert advice in valuing assets in those fields. Otherwise costs will be expended and, on challenge, the expert may not be allowed to testify as to matters beyond his or her qualifications and credentials. In addition, the court will not award those costs.

Unlike for publicly traded companies, no active marketplace exists from which to obtain traded prices to verify the current value of a family-owned business. The family business may be a small convenience store or a large conglomerate, but generally is the single most important marital asset and always the most difficult to value. Experts often disagree in their valuation conclusions. Thus, the family lawyer must be knowledgeable enough in these matters to conduct direct and cross-examination of the business valuation expert. (See Friedlander, p. 24, and Steinberg, Robert S., Florida Family Law, Chapter 59, "Analyzing Economic and Valuation Issues," (Matthew Bender & Company, 2000, Brenda Abrams, ed.).

No generic approach exists to deal with the family business in a divorce case. The owner spouse may have been the founder of the business or second-generation owner. He or she may own a controlling interest or a minority share; may be employed by the business and own no shares of stock; or may have acquired the business as part of his or her job. The interest may be held directly or through a holding company, trust, or family partnership. If incorporated, the entity may be a C corporation or may have elected to be treated for tax purposes as an S corporation or an LLC.

These many variations will have an impact on the valuation process and the type and extent of discovery. For example, the company may maintain excellent accounting books and records or its records may be poorly maintained with personal and corporate expenditures intermingled without proper classification. Such commingling of personal and business affairs may necessitate a full-blown audit to untangle the web. Such extensive discovery generally will not be provided voluntarily. The lawyer must file a motion asking the court to order it. Be prepared to explain with the assistance of your expert why you need such intrusive and disruptive discovery.
What the buyer will pay

In the real world, the value of a family-owned business is determined by the value of future benefits that a willing buyer could derive from its ownership. In deciding what to pay for a business, the buyer first looks at historical profits and normalizes them, eliminating extraordinary items not likely to be repeated. He or she then analyzes the risks of ownership and the likelihood that past profits will repeat in the future. Next an extensive due-diligence review will be undertaken in an attempt to understand these matters. From this risk analysis, the potential buyer will decide what rate of return is appropriate for this investment, taking into account the rate of return available from safe investments, such as Treasury bonds, differentials from public company rates of return, and specific company characteristics.

The business valuation expert conducts the same analysis, except in most cases no sale is pending. This is certainly true in a divorce case. The discovery needed to conduct this analysis is extensive and varies with the kind of business being valued and the industry within which it operates. Therefore, document requests from formbooks are useless. Ask your expert for a list of documents to be produced by the opposing side.

To effectively utilize or attack a business valuation expert, the family lawyer should note some imperatives, namely, the expert must establish an adequate factual predicate for his or her opinion. If all the expert does is scramble up some numbers and apply some formulas, the resulting opinion should be discounted. The expert must examine the records, unless presented with a hypothetical question. The expert must follow the standards promulgated by the appraisal organization to which he or she belongs and is credentialed.

The lawyer must become comfortable enough with the topic of business valuations to adequately support discovery requests and knowledgeably conduct direct and cross-examination.

Although the discovery required and methodologies employed are far too varied and case specific to generalize about expert fees, following are some basic guidelines, with the caveat that generalizations may vary from one jurisdiction to another. Be wary of an expert who offers a business valuation for $2,500. It cannot be accomplished at that fee. One might offer an indication of value akin to a hypothetical, but not a valuation. This means basically that assuming fact A and fact B, your conclusion of value would be X.

The expert first must see the books and records of the company to ascertain how difficult it will be to extract such items as reasonable compensation, personal expenses paid or charged through the business, normalizing adjustments, related-party transactions, such as rent at nonmarket prices, etc. Thus, a retainer of $5,000 to $7,500 is the norm. The valuation may cost $7,500 if the case is settled before trial and no report is required, or it may cost much more if the books and records are a mess and the case goes to trial with the required report, depositions, discovery hearings, etc.

To control costs, the expert and lawyer must communicate throughout the process and agree as to which business records are available and what kind of report is required for trial. The report may be anything from summary schedules to a full-blown business valuation of more than fifty pages. The lawyer must decide what is best for the case, based on the facts and his or her knowledge of the particular judge.

Effective direct examination

All of your work in controlling costs will go for naught if your expert's testimony is ineffective. You will have saved money in a losing cause.

Devote more time to preparing for the expert's direct examination than for cross. Direct is more difficult for both lawyer and expert. The questions and answers must be precise to avoid opening up a wider and potentially damaging cross-examination. Moreover, a good direct examination limits the opponent's cross, which is then more easily navigated by the expert.

An expert should be ready to discuss with the lawyer his or her preliminary opinion after having been educated about the case, the law that applies to the issues on which he or she is to opine, and the facts that will predicate his or her opinion. By that time, the lawyer will have become educated about the subject of the expert's opinions and the basics of his or her discipline as they apply to the issue at hand. The lawyer should review with the expert the following:

1. The substance of opinions, making sure that the expert is opining only on issues for which his or her opinion is requested.
2. The facts upon which opinions are based and whether those facts comport with the lawyer's factual understanding of the issues.
3. The pros and cons of the expert's position. If the expert were on the other side, what line of cross-examination would be or she suggest and how would he answer those questions?
4. Third-party information on which the expert relied. The lawyer must be satisfied that the expert's opinions are his or her own and not those of a third party. The lawyer also must be sure that the expert is not relying on facts supplied by the client without independent investigation. The court may exclude as speculative testimony of an expert proffered from assumed facts when not responding to a hypothetical. Thus, the lawyer must understand how the expert arrived at his or her conclusions.
5. Areas of concern that the lawyer may have with the expert's opinion. If the lawyer disagrees with the expert's opinion, he or she may try to persuade the expert as to a different viewpoint. However, be suspect of any expert who immediately caves in merely because the lawyer is unhappy with the opinion. If the expert has misinterpreted facts or law or has overlooked an argument, ask the expert to reconsider the opinion.

6. Review with the expert an overview of the direct examination. Ask the expert to suggest direct examination questions.

7. Shortly before the trial date, review questions and answers with the expert. Even if the expert is a seasoned witness, remind him or her about the basic rules of testifying.
   * The lawyer will use the expert to tell part of the story of the case.
   * The lawyer will pose questions, and the expert will answer those questions briefly.
   * The expert need not anticipate the next question.
   * The lawyer will cover thoroughly the expert's qualifications, work, and opinions.
   * The lawyer fully understands and accepts the expert's opinions and conclusions and will break the issues down to a level the judge can understand.

Following these suggestions, a lawyer should have little trouble presenting a forensic accountant's expert testimony coherently and cogently to the court. The expert will feel comfortable that the lawyer is familiar with his or her testimony and will not feel the need to become didactic or repetitive. Because the lawyer will control the presentation, the expert will more likely stay on course and not inadvertently stray into sensitive areas that could open up an unwanted and damaging cross.

**Controlling without leading**

As an expert I have worked with many trial lawyers. The best ones make my job easy. They ask specific, surgical questions that slice my testimony into nicely bundled, small packages of information. In this way, the attorney controls the expert's testimony without leading. The lawyer actually presents his or her argument through the expert. Each succeeding question builds on the prior one until a clear picture of the expert's qualifications, work, and opinions is presented. The colloquy between lawyer and expert will sound like a natural conversation that will not bore or intimidate the judge, who easily will follow the testimony.

Generally, in most jurisdictions, leading questions are not permitted on direct examination. But a question is not leading merely because it can be answered yes or no. The question is leading if it suggests only one answer. Thus, "Are you admitted to the bar of a federal court?" is not leading, but "Are you admitted to practice before the United States Tax Court, are you not?" is leading. A good question is one that is specific and focuses the witness's attention without providing the answer.

**Conclusion**

The need to expend client costs for specific forensic accounting procedures should be carefully thought through to be certain that it is necessary, taking into account the issues and complexities of the case and the likelihood of achieving worthwhile results for the client. When a forensic accountant is engaged, the lawyer as the field general should communicate clearly which evidence is required and monitor closely the expert's progress toward the goal of presenting cogent, compelling testimony without incurring unnecessarily extravagant fees. 

Robert S. Steinberg is a tax attorney who is admitted to practice in New York and Florida, the United States Tax Court, and in various other federal jurisdictions. He is also a CPA and CVA who concentrates his practice in tax controversies, divorce mediation, valuation, and forensic accounting. He speaks and publishes often on subjects pertaining to tax issues and accounting.
Books & More

Financial Experts Bibliography


Client Handouts


Pension


Tax


Valuation


Order today from the ABA

★ ABA Publication Orders: PO Box 10892, Chicago, IL 60610-0892 800-285-2221, orders@abanet.org or www.abanet.org/family/advocate/client.html.

Index to Advertisers

As a service to our readers and advertisers, we are listing the advertisers and their page numbers along with a contact and telephone number, if available.

<table>
<thead>
<tr>
<th>Advertiser</th>
<th>Phone/Contact</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Bar Endowment</td>
<td>800-621-8881</td>
<td>7</td>
</tr>
<tr>
<td>ABA Section of Family Law</td>
<td>312-285-2221</td>
<td>3, 5, 13, Cover III and IV</td>
</tr>
</tbody>
</table>
Effective Use of the Forensic CPA

By Stephen L. Ferraro, CPA/ABV/CFF, MAFF, CVA, CBEC, CEPA

During the course of your work, you may have called upon a Forensic CPA for assistance. It might have been for the assessment of commercial damages or to perform a fraud or financial investigation. You may have hired one to calculate future lost earnings related to personal injury or to prepare a business valuation for a shareholder dispute or estate matter. Perhaps you engaged a forensic CPA to determine financial motive in an arson case. As with most things in life, some attorney experiences with CPA Experts have probably been good and some...not so good. So how can you get the most out of your Forensic CPA relationships?

1. Call Early

One of the best ways to compromise the effectiveness of any expert is by delaying their involvement in the process. Some attorneys are hesitant to call in the hopes of controlling the cost of outside experts. Others only think of CPAs as expert witnesses at trial and, consequently, delay their involvement. There are also those who mistakenly think if they gather some financial information on their own it will make the process smoother. Whatever the reason, most delays in making that phone call will result in weakening the expert's value to the process.

The initial phone call does not have to result in the start of a full-scale engagement. In fact, it may only be for assurance purposes, since sometimes there is no need for further involvement on the part of the expert. On the other hand, many times the immediate involvement by the Forensic CPA is required to effectively develop the document request, follow-up interrogatories, or important deposition questions. Having expert financial assistance to develop a well-drawn document request and insightful deposition questions is the first step toward negotiation and, ultimately, a reasonable settlement. The bottom line is that it does not hurt and, in fact, can only help the situation by calling the Forensic CPA early in the process.

2. Communicate Throughout the Process

Advanced and regular communication is required to properly manage the work, and ultimately the bill, of the Forensic CPA. The attorney should be very specific in their instructions right from the start. This will serve to avoid unnecessary or duplicate work, as well as the omission of important procedures, on the part of the expert.

The attorney should discuss the overall strategy with the expert. Often an attorney may discuss what needs to be done, but omit the reason. CPAs dedicated to forensic accounting and expert witness services have a broad background and a great deal of experience in dealing with these types of financial matters. If the attorney discusses strategy with the expert, they may be able to suggest alternatives that the attorney had not even considered.

3. Determine Relevant Experience

Engaging a CPA with forensic accounting and litigation experience should be a must. Litigation support and expert testimony are very different from more traditional accounting, which typically involves tax return preparation and auditing for a client with whom they have had a cooperative relationship for many years. A Forensic CPA has to be much more creative and adaptable. They are often faced with many adversarial relationships that a more traditional CPA may be unprepared to deal with. These situations require the ability to be forthright, yet tactful. A Forensic CPA must also have a broad business
background and be perceptive to differing methodologies, techniques and record keeping options. They must be able to
delve into the situation in spite of disorganized or incomplete records.

Engaging an experienced CPA who has no expertise in forensic accounting and litigation support could result in the attorney
paying for the CPA to get the proper training or experience. Even a very talented CPA who has no previous forensic
accounting experience will have to spend some time getting up to speed in forensic techniques and methods and the
litigation environment. The basic point is that hiring a CPA inexperienced in forensic accounting and litigation could easily
produce substandard results, mishandling of the case, or unnecessarily high billings.

4. **Evaluate Supporting Forensic Credentials**

The CPA expert's credentials are an important part of the decision making process. The attorney should look for an expert
with relevant credentials governed by the American Institute of Public Accountants (AICPA), the National Association of
Certified Valuation Analysts (NACVA) and other relevant organizations. Some of the more pertinent credentials are the
following: Master Analyst in Financial Forensics (MAFF), Certified Fraud Examiner (CFE), Certified Business Appraiser (CBA),
Accredited in Business Valuation (ABV), Certified in Financial Forensics (CFF) and Certified Valuation Analyst (CVA). The CPA
expert should also be an active participant in the organizations that monitor their relevant designations and continuing
educational requirements.

5. **Assess Expected Costs vs. Potential Benefits**

During the initial telephone call the attorney should begin to evaluate the extent of involvement warranted by the Forensic
CPA. If the issue is relatively small, the attorney may be able to proceed after only a short conversation with the expert. In this
type of situation extensive work would probably be overkill and not considered cost effective. On the other hand, in more
complex situations, the attorney may want more extensive involvement on the part of the expert to help develop effective
document requests, interrogatories, deposition questions, and perhaps ultimately, expert testimony.

6. **Review Previous Expert Testimony**

Attorneys should look into previous cases to see the opinions and reports the CPA Expert has issued in the past for
deposition or trial. Counsel should also find out whether an expert has been subject to Daubert challenges and/or has had
their opinion excluded at trial. This is a critical part of the selection process.

7. **Control the Costs Where Possible**

One way to keep billings under control is to remember that attorneys should not always request a formal detailed written
report. The CPA's financial analysis can be made in financial schedules. A shorter, less formal report can serve well in many
instances for effective negotiation and settlement proceedings. In many situations the attorney could make the most effective
use of the expert's time by hiring them for a meeting or teleconference to help explain the analysis and reach a mutually
agreeable settlement. Formal detailed reports are more appropriate for cases definitely going to trial and with complicated
fact patterns. If appeal is a factor, a formal detailed report will undoubtedly become a welcomed part of the attorney's
records.

**Summary**

In summary, if used effectively, a Forensic CPA can be an invaluable resource for an attorney in litigation matters. The
relationship should begin early and there should be good ongoing communication between the expert and the attorney
regarding the work to be performed and the related strategy. The attorney should weigh the cost of the CPA Expert against
the benefit they hope to obtain and direct the expert work accordingly.
Stephen Ferraro is a partner with Ferraro, Amodio & Zarecki CPAs (FAZ), based in Saratoga Springs, NY and serving clients in Albany NY, greater NYC, and beyond. FAZ is a boutique Forensic CPA firm committed to supporting, our clients, the legal community and our team members in the successful resolution of financial disputes, fraud & financial investigations, economic damage assessments and business valuation and transition matters by delivering valuable forensic accounting expertise and related expert services at an appropriate cost. We are a recognized leader in the forensic accounting profession serving clients in Albany and the Capital Region, as well as New York City and the surrounding Metropolitan Areas. If you think you need assistance with a case or are interested in more information, please call me directly at (518) 288-2136.

Related Posts

- Ferraro Amodio & Zarecki CPAs Talk Forensic Accounting  March 29, 2017
- Calculating Lost Profits – Commercial Damages  March 15, 2017
- CLE – Legal Advice on Business Reorganizations  February 10, 2017
Typical forensic accountant roles in anti-corruption due diligence
Given the continued focus on the importance of assessing corruption risks in the context of mergers and acquisitions by the US Department of Justice and the Securities and Exchange Commission, as demonstrated through continued enforcement efforts as well as the joint November 2012 “Resource Guide to the U.S. Foreign Corrupt Practices Act” (the Guide), the question is often posed to forensic accountants:

“What is the role of forensic accountants in performing anti-corruption due diligence versus the role of attorneys?”

This question can best be answered by considering the typical phased approach to performing anti-corruption due diligence. In this context, certain phases involve both the forensic accountants and legal counsel, in addition to the company itself, and other phases might involve only the forensic accountants. The typical phases of anti-corruption due diligence include:

- Anti-corruption risk assessment
- Anti-corruption due-diligence procedures
- Enhanced procedures surrounding corruption red flags
- Development of a post-closing anti-corruption compliance program

The anti-corruption risk assessment phase is typically a joint effort among the company, its forensic accountants and its external legal counsel. Data room information and publicly available information regarding the target may have different legal and accounting ramifications. A joint effort to establish the scope of the diligence procedures is key to avoiding a “cookie cutter” approach and instead allowing the scope of the diligence to focus on areas of perceived risk.

The anti-corruption due diligence procedures phase can generally be broken down into three primary areas: interviews, transaction records testing and electronic data review. Interviews are typically a joint effort of external legal counsel and the forensic accountants. The transaction records review is the focus of the forensic accountants, especially when you consider the type of information being analyzed. Such procedures may include detailed analysis in the following areas:

- Analysis of target financial information to identify trends outliers, and potential corruption red flags. This could include analysis of third-party payments, distributor margins, expenses involving gifts and entertainment, and promotional spend. Additional analysis around sales data to isolate specific target sales locations and customers that could present corruption risk based on geography or industry may warrant consideration.
- Assessment of target's sales channels to detect higher opportunities for corrupt activity. Typically, sales through third-party sales intermediaries, such as sales representatives or agents, for example, would present a higher corruption risk than sales through a direct employee sales force. Statistics suggest that a majority of recent enforcement actions involve the use of third-party sales intermediaries.
- Assessment of target's internal controls for high-risk activities specifically related to the client's industry, known industry risks and target's key operating locations to isolate potential control gaps. Examples may include controls around the following areas: cash activities and petty cash, entertaining and gift giving, political contributions, charitable donations, payments to third parties, due diligence on third parties and sponsorship activities.
- Performance of background research on the target, the target's key management and any major third-party vendors or partners for negative media, government actions (investigations, convictions, settlements), and government connections using publicly available and proprietary databases to detect potential corruption red flags.
The source of information used in the transaction records analysis process will include not only direct accounting support such as ledgers and journal vouchers, but also contracts, litigation files, board meeting minutes, management representation letters, internal audit reports, etc., many of which may necessitate teaming with external legal counsel after their analysis of such documents.

The third phase typically involves performing enhanced procedures surrounding red flags identified in phases one and two. This phase often requires a deeper analysis of available information and further transaction testing to determine if prohibited conduct is occurring. Therefore, these enhanced procedures are typically performed by the forensic accountants. Payments to third parties, detailed analyses of gifts and entertainment, petty cash, charitable contributions, political donations and payments to third-party sales intermediaries are often tested on a detailed basis, and typically require significant access to and understanding of accounting records and processes. These procedures may include detailed steps, such as the following examples of accounting-based analyses:

- Test a broader sample of high-risk activities (e.g., payments to agents and high-risk vendors, analysis of cash activities (including petty cash), analysis of travel and entertainment reports, analysis of gift giving and entertainment involving government officials, analysis of payments to freight forwarders, analysis of contract bid activities) to analyze stated controls and to assess potential impact of the buyer’s controls on the target’s future performance.
- Perform further analysis on the target’s key management and third-party vendors and partners for negative media, government actions (investigations, convictions, settlements) and government connections, focusing on previously identified red flags.

The fourth phase typically involves developing an anti-corruption compliance program post-close. This phase is typically a joint effort among the company, its outside legal counsel and its forensic accountants to address compliance standards, procedures and training reasonably capable of reducing the prospect of corruption risk based on the information obtained through the due-diligence process.

The aforementioned Guide points to specific examples where anti-corruption due diligence and post-acquisition efforts resulted in the government’s decision not to prosecute successor companies for pre-acquisition violations. In situations where pre-acquisition due diligence is not possible, the Guide highlights the need to conduct post-close procedures to achieve the same goal: identification of corruption risks at the newly acquired entity.

Why Transaction Forensics?

- Deep anti-corruption and FCPA due diligence, investigative and compliance experience coupled with global capabilities and resources, specifically focused on potential issues with cross-border transactions
- Understanding and experience in helping financial services firms identify and measure corruption risks in various industries
- Experience assisting private equity clients with anti-corruption risk assessments and pre-acquisition anti-corruption due diligence
- Experience assisting companies in their response to industry-wide corruption initiatives
- Experience supporting clients responding to DOJ and SEC inquiries and investigations
- Experience assisting companies in pre-acquisition contractual language assessments and pre-arbitration dispute analysis
- Experience in providing post-acquisition assistance with preparation of accounting mechanism and post-closing arbitration and dispute services

Transaction Forensics is a separate service line in Ernst & Young LLP’s Fraud Investigation & Dispute Services practice. Transaction Forensics focuses on due diligence services (primarily related to anti-corruption and other forensic due diligence) and disputes and investigations that stem from contemplated and completed merger and acquisition transactions

About the authors

This paper was written by Greg Wolski and Virginia Adams. Greg is a partner and the leader of Ernst & Young LLP’s Transaction Forensics team within its Fraud Investigation & Dispute Services practice. He can be reached at gregory.wolski@ey.com or +1 312 879 3383. Virginia Adams is a Partner on Ernst & Young LLP’s Transaction Forensics team. She can be reached at virginia.adams@ey.com or +1 212 773 7475.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY’s Fraud Investigation & Dispute Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the industry sector. With our more than 2,000 fraud investigation and dispute professionals around the world, we assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide.

How EY’s Global Private Equity Center can help your business

Value creation goes beyond the private equity investment cycle to portfolio company and fund advice. Ernst & Young’s Global Private Equity Center offers a tailored approach to the unique needs of private equity funds, their transaction processes, investment stewardship and portfolio companies' performance. We focus on the market, industry and regulatory issues. If you lead a private equity business, we can help you meet your evolving requirements and those of your portfolio companies from acquisition to exit through a highly integrated global resource of 152,000 professionals across audit, tax, transactions and advisory services. Working together, we can help you meet your goals and compete more effectively.

© 2013 Ernst & Young LLP.
All Rights Reserved.

SCORE No. WW0313
1306-1091704

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ED None