COVINGTON

COVINGTON & BURLING LLP

ADVISORY | Anti-Corruption

November 2012

AN ANALYSIS OF THE FCPA RESOURCE GUIDE

On November 14, the U.S. Department of Justice and Securities and Exchange Commission released their long-awaited *Resource Guide to the U.S. Foreign Corrupt Practices Act*. The 120-page *Guide* provides "one-stop shopping" on a broad range of FCPA compliance and enforcement issues.

For those new to FCPA practice, the *Guide* provides a treasure trove of rules and examples that will help demystify this area of the law. For those steeped in anti-corruption counseling, the *Guide* contains few surprises, but it does helpfully confirm advice that practitioners have given clients across a range of areas, much of which was based primarily on accumulated wisdom and common sense.

Because of the dearth of judicial precedent and other definitive guidance relating to the FCPA, we previously have described anti-corruption counseling as more art than science. The *Guide* has now injected more science into the mix, at least at the margins. In particular, we expect that the *Guide* will enable a much broader range of compliance professionals to take a more rigorous and uniform approach to straightforward compliance questions that arise most frequently in this area. The thornier compliance questions almost always are highly fact-bound and industry-specific, however, and they defy uniform guidance. The *Guide* provides little guidance on the tougher compliance calls, and, as a consequence, advising on those will remain less science and more art.

In this client advisory, we first analyze the most significant aspects of the *Guide*, and then identify two broader themes from the *Guide* that we believe warrant attention going forward.

SIGNIFICANT ASPECTS OF THE GUIDE

Jurisdiction

As the *Guide* explains, the "FCPA's anti-bribery provisions apply broadly to three categories of persons and entities: (1) 'issuers' and their officers, directors, employees, agents, and shareholders; (2) 'domestic concerns' and their officers, directors, employees, agents, and shareholders; and (3) certain persons and entities, other than issuers and domestic concerns, acting while in the territory of the United States." The *Guide* explains when a company is an "issuer" for purposes of the FCPA: the company is listed on a national securities exchange in the United States (either stock or American Depository Receipts); or the company's stock trades in the over-the-counter market in the United States and the company is required to file SEC reports. The test for "domestic concern" is similarly straightforward: broadly speaking, a "domestic concern" is a U.S. person or company. But the seemingly straightforward application of FCPA jurisdiction ends there.

The *Guide* proceeds to advance several controversial theories of jurisdiction, particularly in connection with foreign issuers and the requisite nexus to interstate commerce, foreign nationals, and non-issuer foreign companies. For example, the *Guide* asserts that:

- Foreign issuers, and their officers, directors, employees, agents, or stockholders, may subject themselves to jurisdiction based on nothing more than "placing a telephone call or sending an e-mail, text message, or fax from, to, or through the United States . . . [,] sending a wire transfer from or to a U.S. bank or otherwise using the U.S. banking system, or traveling across state borders or internationally to or from the United States."
- A foreign national or company may be liable if it aids or abets, conspires with, or acts as an agent of an issuer or domestic concern, *regardless of whether the foreign national or company itself takes any action in the U.S.*

These jurisdictional theories have begun to surface in enforcement actions but they remain largely untested in the courts, and they bear watching in the future. One pending case of note involves former executives of Magyar Telekom, an "issuer" under the FCPA. The former executives — Hungarian citizens residing outside of the United States — recently moved to dismiss an SEC civil complaint in which the only jurisdictional nexus alleged is that e-mail messages were routed through the U.S. or stored on U.S.-based network servers. The defendants have argued that the fortuitous and unintentional routing of e-mails cannot satisfy the requirement that the defendants "corruptly" made use of instrumentalities of interstate commerce. Additionally, they have asserted that such a thin connection with the U.S. does not establish the requisite "minimum contacts" to satisfy the basic due process requirements for the exercise of personal jurisdiction. Oral argument is set for January 2013. Regardless of the outcome of that motion, we expect that DOJ and SEC will continue to pursue enforcement actions against foreign issuers and their directors, officers, employees, and agents based on *de minimus* contacts with the United States, such as an e-mail passing through a U.S. server, when other jurisdictional hooks are unavailable.

The *Guide* is more restrained in its discussion of jurisdiction over foreign nationals and non-issuer foreign companies under 15 U.S.C. § 78dd-3, which is based on acts committed in the territory of the United States. This may signal a backing away from the aggressive position that DOJ took in the Shot Show case, where it asserted — unsuccessfully — that simply mailing a package into the United States was sufficient to establish jurisdiction over a UK national. Going forward, we expect that prosecutors increasingly will rely instead on theories of agency, conspiracy, and aiding and abetting to assert jurisdiction over foreign nationals and non-issuer foreign companies even when such persons or entities have not taken any action in the United States in furtherance of a corrupt payment to a foreign official.

Definitions of "Foreign Official" and "Instrumentality"

The *Guide* reiterates the multi-factor, fact-specific test advocated by DOJ and SEC and adopted by federal courts in recent cases to determine whether employees of state-owned or state-controlled entities are "foreign officials" under the FCPA. The *Guide* acknowledges that an entity with minority government ownership or control seldom will constitute an instrumentality of a foreign government. It stops short of establishing a bright-line rule, however, and gives an example of circumstances in which an entity would be considered a government instrumentality even though the government owns a minority share, *i.e.*, where despite the government's minority ownership stake, it had special veto rights as a shareholder and a degree of operational control.

Not surprisingly, the *Guide*'s discussion of "instrumentality" and "foreign official" reflects the DOJ and SEC's litigation position in recent cases. That position currently is being challenged in the 11th Circuit, the first time the government's interpretation of "foreign official" will be tested in an appellate court. This issue has received much attention from commentators and certainly will remain relevant in the context of enforcement actions. As a practical matter, however, because the FCPA's accounting provisions and other U.S. and foreign statutes also reach private commercial

bribery, the definition of foreign official is receding in importance for purposes of designing and implementing corporate compliance programs.

Intent Requirement for Corporate Liability

Industry groups have pressed for clarification that corporate criminal liability requires "willful" conduct by an individual. The *Guide* rejects this position, asserting that "[p]roof of willfulness is not required to establish corporate criminal or civil liability, though proof of corrupt intent is." As a consequence, corporate enforcement actions will continue to center on whether payments were made with corrupt intent, *i.e.*, with intent to "wrongfully influence" the recipient.

As those who counsel clients in this area know, the corrupt intent element often is the only thing that separates a permissible commercial payment from an impermissible bribe. Those hoping for further guidance in this important area will be disappointed, as the *Guide* devotes less than a page to the meaning of "corruptly," and fails to meaningfully expound on the issue of corrupt intent. The *Guide* says only that "[t]he corrupt intent requirement protects companies that engage in the ordinary and legitimate promotion of their businesses while targeting conduct that seeks to improperly induce officials into misusing their positions." The *Guide* thus reassures readers that it would be "difficult to envision" a scenario in which cups of coffee, taxi fare, or promotional items of nominal value would evidence corrupt intent. These are easy calls, and neither they nor the hypotheticals provided in the *Guide* address the more difficult questions that companies regularly face. As a practical matter, the standard for corrupt intent will continue to be "you know it when you see it," and common sense will remain the touchstone for those who counsel in this area.

Parent-Subsidiary Liability

Industry groups sought confirmation that parent company liability under the anti-bribery provisions extends only to cases where the parent authorized, directed, or actually controlled its subsidiary's bad acts. Instead, the *Guide* asserts that a parent also may be held liable "under traditional agency principles," even if the parent was not directly involved in the bad acts. Under the theory set forth in the *Guide*, "a subsidiary's actions and knowledge are imputed to its parent" if an agency relationship exists. While the *Guide* indicates that "the fundamental characteristic of agency is control," it offers no substantive guidance on the nature or degree of "control" DOJ and SEC will look for before pursuing an agency theory of liability in the context of a parent and its subsidiary. Instead, the *Guide* says only that "the parent's knowledge and direction of the subsidiary's actions, both generally and in the context of the specific transaction," must be considered, and "[a]lthough the formal relationship between the parent and subsidiary is important in this analysis, so are the practical realities of how the parent and subsidiary actually interact."

The *Guide*'s reliance on indefinite notions of "control" furthers DOJ and SEC's interest in prosecutorial discretion, including the agencies' discretion to impose criminal liability on parent companies for the acts of their subsidiaries. The FCPA, however, plainly draws a distinction between parent companies and their foreign subsidiaries; absent knowledge or direct involvement in the corrupt scheme, parent companies traditionally have been subject only to civil sanctions under the accounting provisions for bribes paid by foreign subsidiaries. Pushed to its limit, the agency theory of liability potentially offers a back-door avenue — couched in elusive notions of "control" — for imposing criminal liability on parent companies for conduct that traditionally has been enforced through civil remedies.

Whether DOJ uses agency liability in this fashion remains to be seen. We believe it would be an exceptional case in which a parent could properly be held criminally responsible for the acts of its foreign subsidiary under an agency theory, absent any authorization, direction, or actual control by

the parent over the specific improper conduct at issue. To rely on such a theory for criminal liability would be especially troublesome, given that – if invoked – the theory likely would emerge through settled enforcement actions against parent companies, where it will be insulated from the rigor of judicial scrutiny.

Successor Liability

The *Guide* sensibly confirms that an acquisition does not retroactively create FCPA liability based on the conduct of a company not previously subject to the statute. Moreover, according to the *Guide*, an enforcement action based on successor liability is unlikely unless there are "egregious and sustained violations," or where the acquirer is involved in or fails to stop the misconduct post-acquisition. This approach recognizes that, as a matter of public policy, "society benefits when companies with strong compliance programs acquire and improve companies with weak ones." The *Guide* emphasizes, however, that regulators expect companies to take steps to ensure that an acquired company promptly comes into compliance with the FCPA and other U.S. laws. It sets forth a compliance road map that includes promptly rolling out the acquiring company's code of conduct and compliance procedures to the newly acquired entity, conducting training, and performing an anti-corruption audit of the new business. Pre-acquisition due diligence and post-acquisition integration form one of the ten hallmarks of an effective compliance program identified in the *Guide* (discussed more fully below), highlighting the importance of these compliance measures in the eyes of regulators.

One recurring question among practitioners has been whether there is a grace period following an acquisition during which a parent will not be held liable for conduct by its newly acquired entity. The answer appears to be a highly qualified "Yes, if . . . ." Regulators understand that, as a practical matter, it may not be possible to halt all improper business practices at a newly acquired entity the day after closing. This is a matter of discretion, however, and to earn their grace, regulators will expect the acquiring company to conduct risk-based pre-acquisition due diligence, and to develop and execute on a post-acquisition integration plan that promptly extends the acquiring company's compliance program to the acquired entity.

At the same time, regulators appear to be backing away from the extraordinary and highly burdensome requirements imposed upon Halliburton in Opinion Release 08-02. That opinion release involved a transaction that afforded little opportunity for pre-transaction due diligence, and Halliburton agreed to retain external counsel and forensic consultants to conduct thorough anti-corruption due diligence. The company agreed to report back to DOJ on its high risk, medium risk, and low risk due diligence within 90 days, 120 days, and 180 days, respectively, and to fully remediate within one year of the acquisition any problems discovered. Halliburton's due diligence process would include examination of the target's records, including financial and accounting records and e-mail review, as well as interviews of the target's employees. The *Guide* seeks to place that opinion in context. It notes that the Halliburton matter "involved special circumstances" and that "because it was an opinion release . . . it necessarily imposed demanding standards and prescriptive timeframes in return for specific assurances from DOJ." According to the *Guide*, securing comparable assurances via the opinion release procedure "will likely contain more stringent requirements than may be necessary in all circumstances."

Two inferences can be drawn from the *Guide*'s carefully worded commentary on that case. First, regulators have recognized that the burdensome requirements imposed in Release 08-02 simply are not realistic in most transactions, and cannot reasonably form a generally applicable standard of conduct. Second, companies should think carefully before asking DOJ to bless a corporate transaction, as earning a public endorsement through an opinion release almost certainly will require measures that go beyond what many practitioners would regard as necessary and reasonable.

Compliance Programs

For the first time, the *Guide* sets forth in one place U.S. regulators' authoritative view of the "Hallmarks of Effective Compliance Programs" in the anti-corruption area. The substance is familiar and reflects compliance elements articulated previously in the U.S. Sentencing Guidelines, prior settled enforcement actions, and a recent declination involving Morgan Stanley. Those elements include:

- a commitment from senior management and clearly articulated corporate policy against corruption;
- a Code of Conduct and compliance policies and procedures addressing the company's risk areas;
- autonomy and resources provided to one or more identified senior executives vested with responsibility for the oversight and management of the compliance program;
- a risk assessment in order to develop a compliance program that focuses compliance resources on areas of highest risk;
- training and continuous advice to employees, directors, officers, and, in appropriate circumstances, agents and partners;
- incentives and disciplinary measures that reinforce the importance of compliance;
- risk-based, third-party due diligence and monitoring of third-party payments and relationships;
- a mechanism for confidential reporting and a properly funded, efficient process for investigating allegations raised;
- periodic testing and review in order to continuously improve the compliance program; and
- pre-acquisition due diligence and post-acquisition integration in the context of mergers and acquisitions.

We expect that companies subject to the FCPA will use the ten elements set forth in the *Guide* as the touchstone for evaluating their anti-corruption compliance programs (much as life sciences companies historically have looked to the seven elements of an effective compliance program articulated by the HHS Office of Inspector General). Companies with established anti-corruption compliance programs also can use the ten elements as a framework for undertaking future compliance effectiveness reviews to assess how well the company's policies and controls are performing.

The *Guide* avoids endorsing a "compliance defense" urged by industry groups similar to the defense contained in the UK Bribery Act. But it notes that "DOJ and SEC also consider the adequacy of a company's compliance program when deciding what, if any, action to take," confirming that a company's compliance program can influence prosecutors' exercise of discretion in charging decisions and sentencing recommendations.

Finally, the *Guide* describes an effective compliance program as a "critical component of an issuer's internal controls." We expect the SEC in particular will continue to press SOX certifiers and outside auditors to give greater attention to the effectiveness of anti-corruption compliance programs as part of their broader assessment of a company's internal controls.

Gifts, Travel, and Entertainment

The *Guide* emphasizes that companies should focus compliance resources on their areas of greatest risk, and cautions against "[d]evoting a disproportionate amount of time policing modest entertainment and gift-giving[.]" Through several hypotheticals, the *Guide* provides concrete examples of gifts, travel, and entertainment — such as logo items and modest hospitality — that would not violate the FCPA. The *Guide* implicitly endorses controls that will be familiar to practitioners: for example, "many larger companies have automated gift-giving clearance processes and have set clear monetary thresholds for gifts along with annual limitations, with limited exceptions for gifts approved by appropriate management." The "non-exhaustive list of safeguards" set forth in the *Guide's* description of the affirmative defense for reasonable and bona fide expenditures catalogues additional compliance steps that companies should consider taking when providing travel and lodging for a foreign official.

In substance, the *Guide* confirms what practitioners long have advised their clients: while specific dollar limits in this area matter, what matters more is ensuring that a system is in place to control, track, monitor, and audit expenditures for gifts, meals, entertainment, and travel. The *Guide* does not take on more complicated scenarios that companies can confront, however, such as whether a company should accede to a state-owned customer's demand to include in the contract price the cost of travel and per diems for the customer's employees; or under what circumstances sponsoring a doctor at a public hospital to attend a medical conference crosses the line. Those scenarios and many others will continue to require careful, fact-specific scrutiny that goes beyond the advice provided in the *Guide*.

Charitable Contributions

Cautioning that "[p]roper due diligence and controls are critical for charitable giving," the *Guide* lists five questions to consider when making charitable contributions in a foreign country:

- What is the purpose of the payment?
- Is the payment consistent with the company's internal guidelines on charitable giving?
- Is the payment at the request of a foreign official?
- Is a foreign official associated with the charity and, if so, can the foreign official make decisions regarding your business in that country?
- Is the payment conditioned upon receiving business or other benefits?

The *Guide* highlights Opinion Release 10-02 as a successful case study. In that 2010 opinion, which Covington obtained on behalf of a client, DOJ endorsed certain due diligence steps, contract provisions, and other compliance controls as prudent practices in this area.

The *Guide* confirms that charitable contributions should be addressed in anti-corruption compliance programs, and suggests questions that we expect will be incorporated into relevant diligence questionnaires. But it breaks no new ground in an area that seldom has been the focus of enforcement actions.

Third-Party Representatives

The *Guide* confirms that regulators expect companies to pay special attention to their third-party representatives who may interact with foreign officials on the company's behalf. It lists common red flags that compliance professionals will find familiar, and includes hypotheticals discussing vetting of distributors and local partners. The hypotheticals involve glaring red flags that cry out for follow-up, and provide little practical guidance on how to manage third-party risk. This was a missed opportunity. A substantial majority of recent enforcement actions have involved third-party intermediaries, and it is fair to say that such intermediaries present *the* principal risk for many companies.

In recognition of that risk, companies have developed a range of thoughtful and sophisticated compliance processes and controls that are designed to prevent and detect bribes paid by third-party intermediaries. For example, we are aware of companies that have leveraged technology to implement distributor compliance management systems that integrate up-front due diligence, contract management, training, certifications, ongoing monitoring, auditing, and periodic diligence updates. The *Guide* would have benefitted from a more robust description of emerging practices in this area, as it did in the sections addressing gifts and charitable contributions.

Resolutions

Chapter 7 of *the Guide* discusses the means for consensual resolution of FCPA charges, including deferred prosecution agreements ("DPAs"), non-prosecution agreements ("NPAs"), and declinations. The *Guide* explains what DPAs, NPAs, and declinations are and how they function, but offers little insight into questions such as how DOJ and SEC determine whether to employ a DPA or NPA, and whether NPAs typically will be reserved for companies that have made a voluntary disclosure.

In contrast, the *Guide*'s discussion of recent declinations provides useful and welcome transparency into DOJ and SEC's decision-making on whether to charge cases. Of particular note, the *Guide* states that DOJ has declined to prosecute matters "where some or all of the following circumstances were present: (1) a corporation voluntarily and fully disclosed the potential misconduct; (2) corporate princip[al]s voluntarily engaged in interviews with DOJ and provided truthful and complete information about their conduct; (3) a parent company conducted extensive pre-acquisition due diligence of potentially liable subsidiaries and engaged in significant remediation efforts post-acquisition; (4) a company provided information about its extensive compliance policies, procedures, and internal controls; (5) a company agreed to a civil resolution with the Securities and Exchange Commission while also demonstrating that criminal declination was appropriate; (6) only a single employee was involved in the improper payments; and (7) the improper payments involved minimal funds compared to overall business revenues." Given the *Guide*'s reference to the presence of "some or all" of the listed circumstances in cases DOJ has declined to prosecute, there remains a degree of unpredictability in DOJ's decision-making regarding declinations. But this information — which is found in an endnote at the conclusion of the *Guide* — will become required reading for companies subject to an enforcement action.

The *Guide* also gives six examples of recent cases where DOJ and SEC declined to prosecute. A few common threads emerge from those examples: (1) all of the cases involved voluntary disclosure; (2) all involved immediate remediation and improvements to the company's compliance programs; and (3) four of the six cases involved bribes that were "small" or "relatively small." These examples provide helpful guideposts, and they may lead some companies to give more serious consideration to disclosing small-scale violations.

Voluntary Disclosure

Industry groups have pressed for a clearer articulation of the benefits of voluntary disclosure — as distinct from the better-understood benefit of cooperating with the government in an enforcement action and remediating the misconduct. The *Guide* avoids quantifying the benefits of voluntary disclosure, stating only that "DOJ and SEC place a high premium on self-reporting, along with cooperation and remedial efforts." An exhortation to self-report runs throughout the *Guide*, which DOJ and SEC clearly views as a vehicle to encourage voluntary disclosure.

In our view, the *Guide* does not fundamentally alter the calculus of voluntary disclosure, because, at bottom, the tangible benefits of self-reporting remain unclear. For example, while every example of a declination discussed in the *Guide* involved voluntary disclosure, the *Guide* does not elaborate on how regulators weigh voluntary disclosure when deciding whether to prosecute a matter, or to pursue an NPA rather than a DPA. Absent concrete guidance in this area, companies will continue to weigh the potential but uncertain benefits of disclosure, including the possibility of lesser penalties, against the cost and distraction that may result from voluntarily disclosing a matter that otherwise might not come to regulators' attention. That calculus will remain highly fact-specific. A company that thoroughly investigates bribery allegations, looks for other manifestations of the same type of conduct, takes appropriate remedial and disciplinary measures, enhances its compliance program in response to deficiencies identified, and takes other appropriate measures, might conclude that it is reasonable to forego voluntary disclosure.

For companies that do choose to self-disclose, the *Guide* offers a useful framework for benchmarking their conduct against the conduct described in the declinations and other enforcement actions discussed in the *Guide*.

Compliance Monitors

The *Guide* lists six factors that DOJ and SEC consider in deciding whether to require a compliance monitor:

- Seriousness of the offense
- Duration of the misconduct
- Pervasiveness of the misconduct, including whether the conduct cuts across geographic and/or product lines
- Nature and size of the company
- Quality of the company's compliance program at the time of the misconduct
- Subsequent remediation efforts

The *Guide* draws two links that will be helpful to compliance professionals. First, it emphasizes the link between the effectiveness of a company's compliance program and the decision on whether to impose a monitor. Acknowledging that the "[a]ppointment of a monitor is not appropriate in all circumstances," the *Guide* explains that a monitor may be appropriate, "for example, where a company does not already have an effective internal compliance program or needs to establish necessary internal controls." Second, the *Guide* states that "self-monitoring," as opposed to an external monitor, may be appropriate where "the company has made a voluntary disclosure, has been fully cooperative, and has demonstrated a genuine commitment to reform." This is consistent with recent corporate resolutions such as the Pfizer and Johnson & Johnson settlements, both of which included self-monitoring provisions.

LOOKING FORWARD: TWO THINGS TO WATCH

In addition to the specific points discussed above, the *Guide* highlights two broader points that we believe bear watching going forward.

Enforcement Actions as Quasi-Precedent

First, the *Guide* effectively places settled enforcement actions on par with judicial precedent. Though presented as a straightforward recitation of settled law, the *Guide* is in fact a comprehensive and well-organized statement of DOJ and SEC enforcement policies and intentions — a manifesto of sorts, codifying enforcement theories that have been pursued over the past decade. The *Guide* speaks authoritatively and seldom qualifies its statements by noting when they reflect DOJ and SEC's litigation positions, some of which can and will be challenged in the courts.

For practitioners, this approach carries with it a risk and an opportunity. The risk is that today's enforcement positions become tomorrow's unchallenged conventional wisdom, even when a particular position may not reflect the most reasonable interpretation of the statute. For example, the *Guide* states without citation that "an issuer's books and records include those of its consolidated subsidiaries and affiliates." That view is reflected in many of the SEC's more recent enforcement actions. Until 2000, however, misrecorded entries on a foreign subsidiary's books, without more, were not automatically treated by the SEC as a violation by the parent/issuer of the FCPA's books and records provision. Two enforcement actions in 2000 and 2001 changed that conventional wisdom, which today is presented as settled doctrine in the *Guide*.

At the same time, the treatment of settled enforcement actions as precedent, coupled with the transparency provided by the *Guide*, offers practitioners the opportunity to argue for preferred results by drawing analogies with the case studies provided in the *Guide*. To be sure, regulators will not be bound by their prior dispositions in other cases, and they may be able to distinguish settled cases based on facts not included in the public record. The existence of public benchmarks, however, particularly with respect to declinations, will help counsel ensure in appropriate cases that similar cases are treated similarly.

Compliance Programs: Companies Cannot "Set It and Forget It"

Second, the *Guide* marks a shift of emphasis from putting a compliance program in place — which most larger companies have done already — to conducting ongoing risk assessments, monitoring performance, auditing for effectiveness, and making appropriate modifications to the program going forward. The *Guide* notes that "[a] company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the standards of its industry." Accordingly, "a good compliance program should constantly evolve." The unmistakable message is that a company's compliance program, like its business, must be dynamic and subject to periodic review and renewal.

As part of this evolution, the *Guide* alerts companies that they will be expected to fully integrate compliance programs into their internal controls, and to ensure that anti-corruption risks are considered in the design, implementation, and monitoring of internal controls over accounting and financial reporting. As a practical matter, this means that in addition to designing and updating traditional compliance tools such as third-party due diligence procedures, companies will need to link those measures to the corresponding financial controls — such as delegations of authority, approvals over third-party invoices, travel and expense reporting and approval, expense monitoring,

the process for opening new vendors, and the like. Some companies are doing this already. Those that are not would do well to heed the recent caution from Kara Brockmeyer, head of the SEC's FCPA unit, that "bribery can't happen if the company has control over where its money is going."

If you have any questions concerning the material discussed in this client advisory, please contact any of the following senior members of our Global Anti-Corruption Practice:

Tammy Albarran	415.591.7066	talbarran@cov.com
Robert Amaee	+44.(0)20.7067.2139	ramaee@cov.com
Stephen Anthony	202.662.5105	santhony@cov.com
Bruce Baird	202.662.5122	bbaird@cov.com
Eric Carlson	86.10.5910.0503	ecarlson@cov.com
Casey Cooper	+44.(0)20.7067.2035	ccooper@cov.com
Christopher Denig	202.662.5325	cdenig@cov.com
Steven Fagell (co-chair)	202.662.5293	sfagell@cov.com
James Garland	202.662.5337	jgarland@cov.com
Haywood Gilliam	415.591.7030	hgilliam@cov.com
Barbara Hoffman	212.841.1143	bhoffman@cov.com
Robert Kelner	202.662.5503	rkelner@cov.com
Nancy Kestenbaum	212.841.1125	nkestenbaum@cov.com
David Lorello	+44.(0)20.7067.2012	dlorello@cov.com
Lynn Neils	212.841.1011	lneils@cov.com
Mona Patel Doshi	202.662.5797	mpatel@cov.com
Don Ridings (co-chair)	202.662.5357	dridings@cov.com
John Rupp (co-chair)	+44.(0)20.7067.2009	jrupp@cov.com
Anita Stork	415.591.7050	astork@cov.com
Alan Vinegrad	212.841.1022	avinegrad@cov.com
