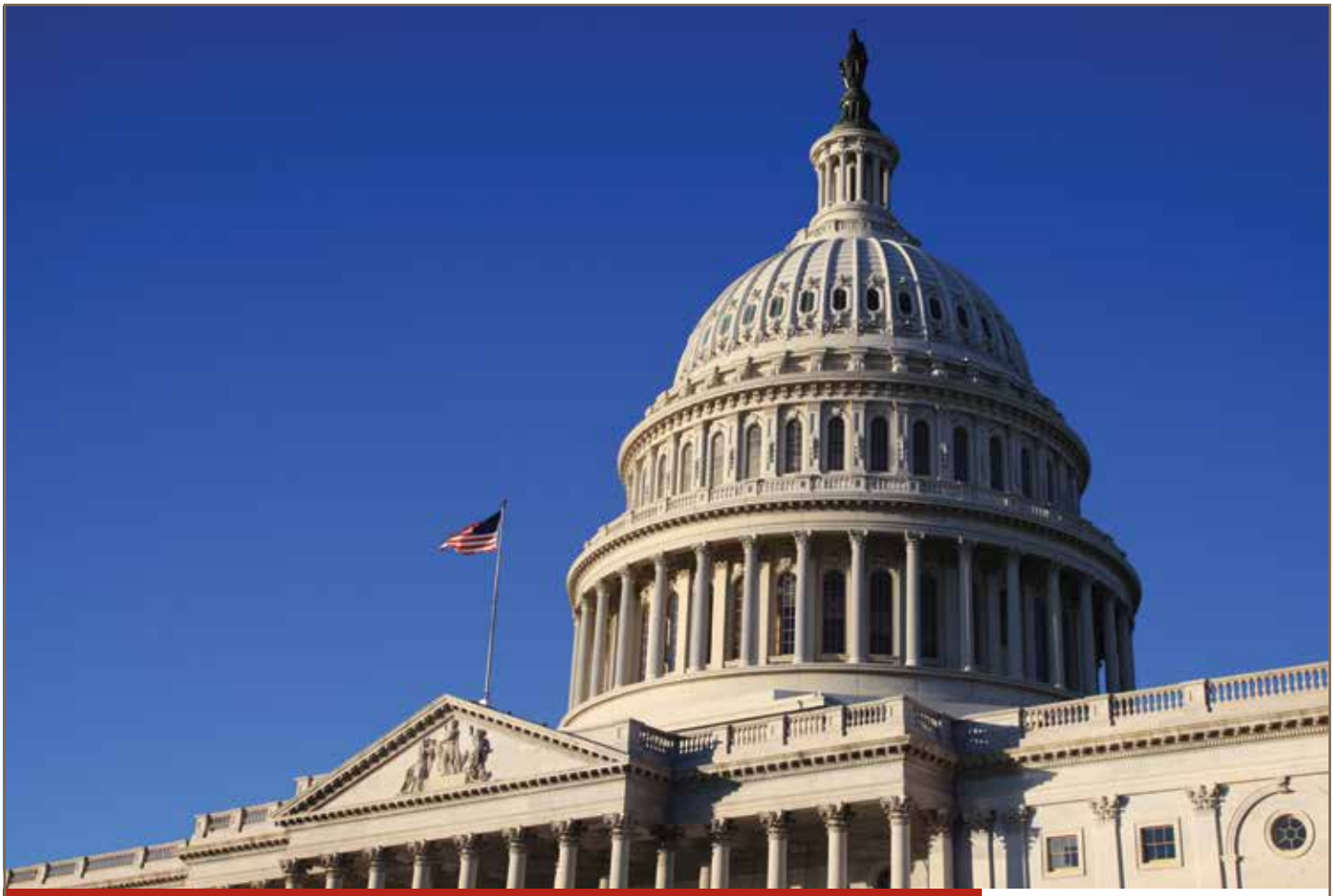


Navigating the FCPA

An Executive Summary of the DOJ and SEC's 2012 Resource Guide to the Foreign Corrupt Practices Act

BASS BERRY • SIMS PLC

Table of Contents

BASS BERRY • SIMS PLC

bassberry.com/FCPA

Introduction

BASS BERRY • SIMS PLC

The Criminal Division of the U.S. Department of Justice ("DOJ") and the Enforcement Division of the U.S. Securities and Exchange Commission ("SEC") released their Resource Guide to the U.S. Foreign Corrupt Practices Act (the "Guide") in November 2012.

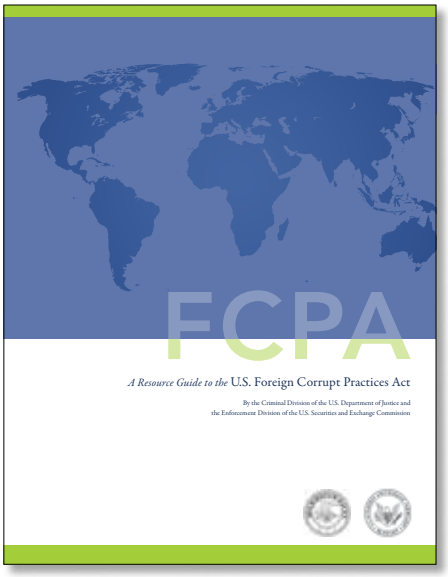
The Guide demonstrates that enforcement of the Foreign Corrupt Practices Act ("FCPA") will remain vigorous, and that enforcers' compliance expectations for private and publicly-traded companies and individuals will remain high.

The 120-page Guide provides guidance on critical issues, including:

- Hallmarks of an effective compliance program;
- Use of agents and other third parties;
- Gifts, travel, entertainment and charitable contributions;
- Parent-subsidiary liability for FCPA violations;
- Liability in the context of joint ventures, mergers and acquisitions;
- Interpretation of "anything of value," "foreign official," and "corruptly;"
- DOJ's expansive views of territorial jurisdiction under the FCPA; and
- How DOJ and SEC resolve allegations made against issuers, private companies and individuals.

Bass, Berry & Sims provides this executive summary to examine key components of the Guide and provide context, guidance and specific action items to help navigate the FCPA.

If you have any questions about the Guide or other anti-corruption efforts, contact one of the members of Bass, Berry & Sims' *Global Anti-Corruption/FCPA Compliance and Investigations team.*



Click here to view the Resource Guide to the U.S. Foreign Corrupt Practices Act.

Key Elements of Effective Compliance Programs

BASS BERRY • SIMS PLC

The Guide provides a convenient roadmap of DOJ and SEC's expectations regarding corporate compliance programs. For in-house counsel and compliance officers, the release of the Guide provides an excellent opportunity to marshal internal support for a fresh assessment of existing compliance programs.

This section provides a concise summary of seven DOJ and SEC expectations for corporate anti-corruption compliance programs generally, what these expectations mean for companies and specific actions companies can take to help address each one.

1. TONE AT THE TOP

Enforcers often stress the need for a culture of compliance, regardless of the strength of a company's program on paper. The Guide reiterates this position. However, the Guide indicates that enforcers will evaluate the culture among middle managers and line-level employees — not just the commitment from senior managers.

> **ACTION ITEM:**
> In addition to training employees on anti-corruption policies, assess employees' perceptions of the company's commitment to compliance. This kind of assessment can help leadership identify compliance weaknesses and better determine the best way to allocate anti-corruption resources.

2. RISK ASSESSMENT

In the words of the Guide, "[a]ssessment of risk is fundamental to developing a strong compliance program." DOJ and SEC expressly acknowledge that one-size-fits-all compliance programs rarely work and that compliance programs should be risk-based: "DOJ and SEC will give meaningful credit to a company that implements in good faith a comprehensive, risk-based compliance program, even if that program does not prevent an infraction in a low risk area because greater attention and resources had been devoted to a higher risk area."

> **ACTION ITEM:**
> Conduct regular, meaningful risk assessments and use them to guide the rest of the company's compliance efforts. As the Guide notes later, "Effective policies and procedures require an in-depth understanding of the company's business model, including its products and services, third-party agents, customers, government interactions, and industry and geographic risks."

BASS BERRY • SIMS PLC

3. CODE OF CONDUCT, AND COMPLIANCE POLICIES AND PROCEDURES

Unlike some previous guidance, the Guide specifically identifies risks that many companies should address with policies and procedures:

- Payments to foreign officials;
- Use of third parties;
- Gifts, travel and entertainment expenses;
- Charitable and political donations; and
- Facilitating and expediting payments.

Most companies already have these policies in place (with the possible exception of procedures for facilitating and expediting payments — a recent survey found that 64 percent of companies simply ban these outright).

> **ACTION ITEMS:**
>
> **1.** Ensure your program addresses each of the risk areas above.
>
> **2.** Translate all policies and procedures into local languages.
>
> **3.** Consider using web-based approval programs for gifts, travel and entertainment expenses. These recommendations (and the Guide in general) indicate a preference for a centralized compliance function with communications tailored for local business units.

4. TRAINING AND CONTINUING ADVICE

As the Guide notes, "[c]ompliance policies cannot work unless effectively communicated throughout a company." DOJ and SEC do not offer specific recommendations on the content of the training, except to note that companies should consider tailoring their training programs to the audience — sales personnel and accounting personnel may need different training based on the scenarios they are likely to face.

> **ACTION ITEMS:**
>
> **1.** Develop means to give specific advice when it is needed urgently. For larger companies, this typically means well-publicized ways to communicate with on-call in-house compliance or legal personnel. For smaller companies, this may mean retaining outside FCPA counsel in advance, so that they can provide timely advice when it is needed.
>
> **2.** Customize anti-corruption training to the jobs, functions and specific risks faced by specific audiences.

5. INCENTIVES AND DISCIPLINARY MEASURES

DOJ and SEC also note the need for compliance policies to be linked with meaningful consequences. In addition to disciplinary measures for non-compliance, however, DOJ and SEC explicitly note that some companies have "made adherence to compliance a significant metric for management's bonuses."

> **ACTION ITEM:**
> **Develop Positive Incentives for Ethics and Compliance Leadership.** Require employees to report suspected violations of the FCPA internally and foster a corporate culture where internal reports are expected and appreciated. For example, consider taking such reports into account when evaluating employee job performance and consider taking compliance climate metrics into account when evaluating managers and other leaders.

6. OVERSIGHT, AUTONOMY, AND RESOURCES

The Guide echoes the U.S. Sentencing Guidelines in emphasizing that companies should assign responsibility for their compliance functions to senior executives who have autonomy from management. The Guide also acknowledges that another individual can be delegated day-to-day responsibility for the compliance program.

Notably, the U.S. Sentencing Guidelines require that, for maximum credit, the individual to whom day-to-day responsibility is delegated should have "direct access to the governing authority [e.g., the Board of Directors] or an appropriate subgroup of the governing authority [e.g., the Audit Committee]."

> **ACTION ITEM:**
> Assign operational responsibility for the company's compliance program to a senior executive and give that individual "express authority to communicate personally" to the Board of Directors or Audit Committee.

7. CONTINUOUS IMPROVEMENT: PERIODIC TESTING AND REVIEW

The Guide emphasizes that no compliance program should be static. Rather, DOJ and SEC recommend that companies "regularly review and improve their compliance programs."

For companies that undertake ad hoc reviews of their compliance programs, however, the release of the Guide presents a clear opportunity to update policies and procedures in light of the guidance from DOJ and SEC.

> **ACTION ITEM:**
> Schedule routine testing and review processes (including those that are unannounced).

SUMMARY

Though the Guide does not answer every question, it brings clarity and specificity to many of the compliance expectations that guide the DOJ and SEC's FCPA enforcement decisions.

Similarly, though the action items listed above are not required or all-inclusive, if taken they can help companies prevent, detect and mitigate FCPA and other compliance problems.

Relationships with Third Parties

BASS BERRY • SIMS PLC

This section highlights the risks detailed in the Guide that can arise from third-party relationships. It also outlines steps a company can take to identify risky third parties and to spot red flags after the third-party relationship has been formed.

WHY YOU SHOULD BE AWARE OF THIRD-PARTY RISKS

Although third parties often play a fundamental role in a company's business in foreign jurisdictions (e.g., identifying local opportunities, developing local relationships and advising on local customs), they also can pose significant corruption risk. The Guide reemphasizes that individuals and companies can be subject to civil and criminal penalties under the FCPA for corrupt payments to foreign officials made on their behalf by third parties — such as agents, consultants and distributors.

In addition, DOJ and SEC make it clear that they use a low threshold when assessing whether a person or company possesses the requisite knowledge to be liable for a third-party's conduct. For example, they stress that a "head-in-the-sand" approach to, or conscious disregard of, unlawful third-party payments and conduct will not insulate an individual or company from criminal liability for such actions.

COMMON THIRD-PARTY RED FLAGS

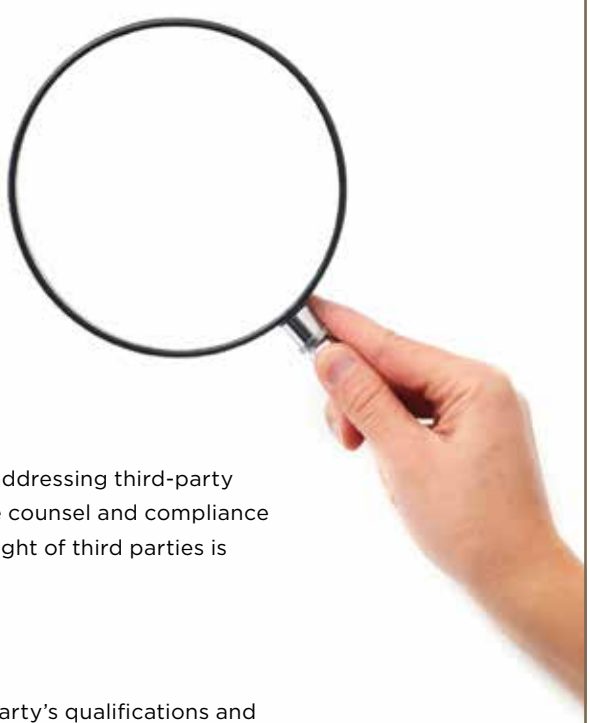
To assist companies in understanding third-party risk, DOJ and SEC identify these common red flags in the Guide:

- "excessive commissions to third-party agents or consultants;"
- "unreasonably large discounts to third-party distributors;"
- "vaguely described services" within third-party consulting agreements;
- the third party's line of business differs from that for which it has been engaged;
- "the third party is related to or closely associated with the foreign official;"
- a foreign official initiated or requested the third party's involvement;
- the third party is "a shell company incorporated in an offshore jurisdiction;" and
- "the third party requests payment to offshore bank accounts."

To reduce the risk of these red flags arising, and to identify them when they do occur, the Guide includes recommendations that a company conduct risk-based due diligence before engaging a third party and routine oversight of third parties with whom it currently does business.

BASS BERRY • SIMS PLC

DUE DILIGENCE AND MONITORING OF THIRD PARTIES



In the Guide, DOJ and SEC emphasize that one of the hallmarks of an effective anti-corruption compliance program is risk-based due diligence of third parties.

A due diligence program should be scaled according to the characteristics of the third-party engagement, including:

- the historical relationship with the third party;
- the size and nature of the transaction; and
- the industry and country involved in the transaction.

While DOJ and SEC discourage a static, one-size-fits-all approach to addressing third-party risk, the Guide does include guiding principles that can assist in-house counsel and compliance officers in assessing whether their company's due diligence and oversight of third parties is sufficiently robust.

1. LEARN THE THIRD PARTY'S BACKGROUND

A critical part of any risk-based due diligence is the review of a third party's qualifications and affiliations — particularly its business reputation and any relationships with foreign officials. This review should occur before using the third party and intensify as red flags appear.

> **ACTION ITEMS:**
>
> **1.** Perform background and reference checks on the third party.
>
> **2.** Require the third party to complete a due diligence questionnaire (including questions on relationships with foreign officials).
>
> **3.** Screen the third party against sanctions databases.

2. UNDERSTAND THE BUSINESS PURPOSE FOR THE THIRD-PARTY RELATIONSHIP

Understanding a third party's role — from a business perspective — in a given transaction is essential to assessing the third party's corruption risk. A company should be wary of involving a third party in a transaction if it does not have a lawful and legitimate business rationale for the third party's involvement.

> **ACTION ITEMS:**
Some actions a company can take to ensure a third party is engaged for the right reasons include

1. Ensure the third party's contract terms specifically describe the services to be performed.
2. Assess the difference, if any, between the third party's payment terms and the payment norms within the industry, country involved, and company.
3. Determine the circumstances surrounding the third party's entrance into the business.
4. Audit the payments to the third party to ensure that its compensation is consistent with the services performed and that the services specifically described in the contract are actually being done.

3. MAKE THE THIRD PARTY AWARE OF YOUR COMMITMENT TO COMPLIANCE

DOJ and SEC noted in the Guide that they "also assess whether the company has informed third parties of the company's compliance program and commitment to ethical and lawful business practices."

> **ACTION ITEMS:**

1. Ensure your company's retention agreement with the third party contains representations, warranties and covenants regarding compliance with the FCPA and other applicable anti-corruption laws and termination rights for your company; and
2. Consider requiring the third party to complete anti-corruption training and/or requesting compliance assurances from the third party (e.g., through certifications) based on risks.

4. MONITOR YOUR THIRD-PARTY RELATIONSHIPS ROUTINELY

Companies should periodically assess the effectiveness of their due diligence and third-party anti-corruption compliance measures.

> **ACTION ITEMS:**
> Based on risk
>
> **1.** Exercise contractual audit rights.
>
> **2.** Seek annual compliance certifications from the third party.
>
> **3.** Assess the sufficiency of the company employees' oversight of the third party's work and conduct.

SUMMARY

Third-party relationships will continue to be an area of significant corruption risk for companies conducting business internationally.

A recent survey conducted by Kroll Advisory Solutions found that corporate compliance officers at U.S. multinational corporations reported that third parties pose the largest overall risk for corporate compliance programs.

To mitigate this risk, companies should be diligent in understanding and identifying third-party red flags and implementing risk-based due diligence throughout the lifetime of a third-party relationship, based in part on the guiding principles noted above.

These efforts to prevent and detect third-party problems will be mostly futile if a company fails to address a problem with meaningful action, such as determining the scope of the problem through an internal investigation, cutting ties with culpable third parties and updating your compliance program to reduce the risk of recurrence.

Gifts, Hospitality and Entertainment

BASS BERRY • SIMS PLC

This section provides: (1) a concise explanation of the Guide's general principles regarding gifts, travel and entertainment; (2) a summary of the Guide's examples of expenses that are either clearly appropriate or illegal; and (3) practical action items.

GIFT-GIVING AND HOSPITALITY FCPA RISK

Gift-giving and hospitality have been considered business activities posing heightened FCPA risk, particularly after recent enforcement actions like *SEC v. Veraz Networks, Inc.*, in which the SEC cited flowers for a CEO's wife as a "questionable" expense. In the Guide, however, DOJ and SEC have given further advice to companies regarding corporate hospitality.

GENERAL PRINCIPLES OF GIFT-GIVING AND HOSPITALITY

The Guide recognizes that providing corporate hospitality is often an appropriate way to conduct business. In addition to specific examples discussed below, the government sets out "hallmarks" of appropriate gift-giving, including:

- Giving the gift openly and transparently;
- Properly recording the gift on the giver's books and records;
- Providing the gift only to reflect esteem or gratitude; and
- Ensuring the gift is permissible under local law.

SPECIFIC SAFEGUARDS TO REDUCE THE RISK OF HOSPITALITY-RELATED FCPA VIOLATIONS

In the context of the affirmative defense of "reasonable and bona fide" expenditures, the Guide also identifies safeguards related to hospitality expenses (as compiled from previous DOJ releases) which can be incorporated into a company's anti-corruption training and procedures:

- Do not select the particular officials who will participate in a trip or program, or select them based on pre-determined, merit-based criteria;
- Pay all costs directly to vendors and/or reimburse costs only upon presentation of a receipt;
- Do not advance funds or pay for reimbursements in cash;

- Ensure that any stipends are reasonable approximations of costs likely to be incurred and/or that expenses are limited to those that are necessary and reasonable;
- Ensure the expenditures are transparent, both within the company and to the foreign government;
- Obtain written confirmation that payment of the expenses is not contrary to local law; and
- Ensure that costs and expenses on behalf of the foreign officials are recorded accurately in the company's books and records.

The Guide does not insist upon specific procedures, but notes that "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 Guide also observes that some companies "have created web-based approval processes to review and approve routine gifts, travel, and entertainment involving foreign officials and private customers with clear monetary limits and annual limitations."

EXAMPLES OF EXPENSES VIEWED AS FCPA VIOLATIONS

The Guide collects the following actual or hypothetical examples of FCPA violations that included gifts or hospitality:

- "a $12,000 birthday trip for a government decision-maker from Mexico that included visits to wineries and dinners;"
- "$10,000 spent on dinners, drinks and entertainment for a government official;"
- "a trip to Italy for eight Iraqi government officials that consisted primarily of sightseeing and included $1,000 in 'pocket money' for each official;"
- "one defendant paid personal bills and provided airline tickets to a cousin and close friend of the foreign official whose influence the defendant sought in obtaining contracts;" and
- paying for a vacation to Paris for a foreign official and his girlfriend in exchange for confidential, non-public bid information from the company's competitors.

EXAMPLES OF EXPENSES VIEWED AS LAWFUL

The Guide also presents a series of detailed hypotheticals relating to gifts, travel and entertainment. In the hypotheticals, the government affirms that promotional, branded gifts of nominal value are permissible. The Guide also goes further, however, and states that no FCPA anti-bribery violation would occur in the following scenarios:

- A company invites customers (including some foreign officials) out for drinks and pays a moderate bar tab for the group;
- A company provides a "moderately priced crystal vase" to a foreign official as a wedding gift and a "token of esteem or gratitude;" and
- During the course of a contract with a foreign instrumentality, a company invites employees of the entity to its facilities in the U.S. to provide training. As part of the trip, the company pays for the hotel and transportation costs, including business class airfare. The company also pays for a moderately-priced dinner, a baseball game and a play.

To the extent they are not already part of your compliance program, consider implementing the following action items:

> **ACTION ITEMS:**

1. Incorporate the specific safeguards listed on pages 12-13 into company training and procedures so employees can better avoid and detect questionable expenses.
2. Require advance written approval of gifts, travel and entertainment expenses based on risk level.
3. Set expense limitations specific to each jurisdiction in which your company operates.
4. Track expenses that are related to particular government entities and/or officials so that the company can enforce annual limitations.
5. Retain local counsel in advance who can opine on the legality of providing gifts and hospitality under local law.
6. For larger organizations, establish web-based approval of routine expenses.

SUMMARY

While gift-giving hospitality and entertainment does not constitute *a per se* violation of the FCPA, companies should be vigilant regarding the benefits provided to foreign officials.

Mergers, Acquisitions and Joint Ventures

BASS BERRY • SIMS PLC

This section examines and summarizes the Guide's (1) enforcement positions with respect to successor and joint venture liability; (2) recommended pre-acquisition due diligence steps; and (3) recommended post-acquisition integration steps.

SUCCESSOR AND JOINT VENTURE LIABILITY

The Guide re-affirms DOJ and SEC's position that private and publicly-traded acquirers can be held liable for FCPA violations committed by their targets: "[s]uccessor liability applies to all kinds of civil and criminal liabilities, and FCPA violations are no exception."

Consistent with the emphasis on voluntary disclosure which permeates the Guide, DOJ and SEC point to the potential for declinations (and other alternatives to guilty pleas) when an acquirer voluntarily discloses past violations by the predecessor company, remediates the conduct, and cooperates with enforcers.

In the acquisition context, DOJ and SEC also emphasize that they frequently pursue enforcement actions against only the predecessor company — rather than the acquiring company — thus enabling the acquiring company to avoid potential debarment and other negative repercussions associated with a guilty plea. This is often cold comfort to a company whose new acquisition is devalued by a corporate criminal conviction.

The Guide also reiterates that an issuer can be held responsible for accounting violations of its joint venture partners. Specifically, an issuer can be held directly liable for the "fail[ure] to have adequate internal controls and fail[ure] to act on red flags indicating that its affiliates were engaged in bribery." As reflected in the text of the FCPA, however, if a company owns less than 50 percent of a subsidiary or affiliate, the company is required only to use its "best efforts" to implement adequate internal controls.

BASS BERRY • SIMS PLC

PRE-ACQUISITION

Given the high costs of an FCPA enforcement action (including investigation, defense, and collateral litigation costs) and the devaluation that often follows an enforcement action, the Guide stresses the importance of pre-acquisition anti-corruption due diligence. Not only can such due diligence prevent the company from buying a corrupt business, the Guide suggests that good faith due diligence efforts can help prevent a criminal prosecution in the event that due diligence fails to catch an existing problem.

Though the Guide does not mandate particular due diligence steps, a company negotiating the acquisition of a foreign target should consider the following action items:

> **ACTION ITEMS:**

1. Determine the extent of the target's international operations, including agents, distributors, and sourcing.
2. Have the company's legal, accounting, and compliance departments review the target's sales and financial data, its customer contracts, and its third-party and distributor agreements.
3. Perform a risk-based analysis of the target's customer base.
4. Perform an audit of selected transactions engaged in by the target.
5. Engage in discussions with the target's general counsel, vice president of sales, and head of internal audit regarding all corruption risks, compliance efforts, and any other major corruption-related issues that have surfaced at the target over the past 10 years.
6. Seek, in particularly difficult cases, an opinion release from DOJ (which SEC also honors).

POST-ACQUISITION INTEGRATION

The Guide also emphasizes the importance of swiftly integrating an acquired company into the parent's compliance program and remediating any problems that were not discovered until after the acquisition has closed.

In particular, DOJ and SEC encourage companies to take the following steps after acquisitions:

> **ACTION ITEMS:**

1. Ensure that the acquiring company's code of conduct and anti-corruption compliance policies and procedures apply as quickly as is practicable to newly acquired businesses or merged entities.
2. Provide anti-corruption training to the directors, officers, and employees of newly acquired businesses or merged entities (and to agents and business partners, when appropriate).
3. Conduct an FCPA-specific audit of all newly acquired or merged businesses as quickly as practicable.
4. Disclose any corrupt payments discovered during due diligence or post-acquisition integration.

These steps may decrease the likelihood of an enforcement action even "when pre-acquisition due diligence is not possible."

SUMMARY

Acquisitions and joint ventures can pose significant anti-corruption risks. Taking risk mitigation steps suggested by enforcers may help companies reduce the threat of a substantial enforcement action arising from a merger, acquisition or joint venture.

Responding to Red Flags and Reports

BASS BERRY • SIMS PLC

This section details and summarizes (1) DOJ and SEC's expectations for companies in identifying and responding to red flags, (2) recommended steps before a red flag is raised, and (3) recommended actions in responding to a red flag.

IDENTIFYING AND RESPONDING TO RED FLAGS

DOJ and SEC emphasize in the Guide that an effective compliance program should include a mechanism for the confidential reporting of suspected or actual misconduct, along with "an efficient, reliable, and properly funded process for investigating the allegation and documenting the company's response" to the allegation. In weighing the adequacy of a company's response to alleged violations, DOJ and SEC "place a high premium" on voluntary disclosure, cooperation and "meaningful" remedial measures.

GUIDANCE BASED ON ENFORCEMENT DECLINATIONS

Although the Guide does not reveal exactly how much credit a company will receive for its actions in response to a red flag, it does offer a rare glimpse into DOJ and SEC's expectations through the inclusion of six declinations, which customarily are not publicized.

DOJ and SEC cite some of the following response steps as reasons for the declinations:

- Improper payments detected in advance by company's internal controls and investigated by Audit Committee;
- Undertook thorough internal investigation;
- Immediately stopped misconduct;
- Terminated employees involved;
- Severed ties with third-party agents;
- Withdrew potentially tainted contract bid;
- Terminated law firm in foreign locale providing improper advice;
- Voluntarily disclosed investigation and red flag to DOJ and/or SEC;
- Substantially updated compliance program (e.g., improved training program); and
- Developed plan to investigate and remediate subsidiary's red flags post-acquisition, and integrate subsidiary into compliance program (in M&A context).

BEFORE A RED FLAG ARISES

A company should prepare for problems in advance by considering the following action items:

> **ACTION ITEMS:**

1. **Implement an Effective Compliance Program.** In addition to helping to prevent and more quickly detect problems, the existence and strength of a company's pre-existing compliance program will be a key factor in whether DOJ and SEC decide to bring an enforcement action against a company.
2. **Enable Confidential Reporting.** Companies should consider establishing a mechanism for two-way confidential reporting through, for example, an ethics line answered by a person, email address or the company's intranet.
3. **Develop a Well-Rounded Response Team.** A company can avoid many of the pitfalls that often occur during an internal investigation by identifying and readying internal resources that will often be quickly needed when a problem occurs (e.g., legal, compliance, finance, operations and internal audit, as necessary).
4. **Identify Outside Anti-Corruption Counsel and Foreign Local Counsel.** By identifying external resource options (and sometimes retaining them) in advance, companies can better compare suitability, cost-effectiveness and fit, rather than rushing to identify, hire and integrate outside counsel in the midst of a crisis.
5. **Establish and Update Incident Response Plan.** Developing a response plan in advance will help a company identify, consider and better prepare for contingencies, improve its response time, avoid running afoul of local laws, and increase the cost-effectiveness of a response.

RESPONDING TO A RED FLAG

A company assessing how to respond to an alleged violation should consider the following action items:

> **ACTION ITEMS:**

1. **Evaluate the Big Picture and Scale Response.** Companies should develop a risk-based strategy and consider execution practicalities at the outset of their response.
2. **Establish and Protect Legal Privileges.** A company should involve in-house counsel as soon as the company becomes aware of a potential problem so that legal privileges can be quickly applied. Failure to do so can result in all aspects of the company's response being subject to disclosure to the government and future civil litigants.
3. **Conduct Internal Investigation.** A company should investigate red flags and reports quickly and thoroughly while being mindful of the need to protect the attorney-client privilege, preserve data, comply with local laws and document its efforts.
4. **Stop Questionable Activities.** Companies should act quickly to identify and halt any questionable business practices. Companies should discipline any culpable employees, replace responsible management and terminate tainted third-party relationships.
5. **Consider Self-Disclosure.** In the Guide, DOJ and SEC repeatedly advise companies to self-report misconduct, including FCPA violations. In deciding whether to self-disclose, companies should consider a number of factors including the likelihood of the allegations being revealed through another means (e.g., whistleblower, press, industry-wide sweep, local enforcement action or SEC reporting obligations) and the cross-jurisdictional implications of self-disclosure.
6. **Update Compliance Program.** As the Guide notes, "[c]ompanies will want to consider taking 'lessons learned' from any reported violations and the outcome of any resulting investigation to update their internal controls and compliance program and focus future training on such issues, as appropriate."

SUMMARY

The Guide provides some welcome transparency regarding DOJ and SEC's expectations for companies in identifying and responding to red flags. By preparing for problems in advance, and then prudently considering and swiftly addressing problems when they arise, companies may be able to better satisfy government enforcers during an investigation and avoid a significant enforcement action.

About Bass, Berry & Sims PLC

Founded in 1922, Bass, Berry & Sims represents Fortune 500 and other domestic and international companies in complex corporate transactions, disputes and compliance matters. Our work for preeminent organizations includes serving as regulatory auditor for the New York Stock Exchange, representing a large healthcare company in a US$33 billion leveraged buyout (at the time, the largest in U.S. history), as well as serving as the SEC-approved monitor for a Big Four accounting firm.

ABOUT OUR GLOBAL ANTI-CORRUPTION TEAM

Our compliance and international investigations team has extensive experience, demonstrated capabilities, established credibility with government enforcers and proven global reach. Our Washington, D.C.-based team members have proximity to and interact regularly with key enforcement agencies, yet we provide exceptional cost-efficiency because many of our team members are based in lower-cost markets.

Our team provides these services:

- Leading international internal investigations
- Conducting anti-corruption risk assessments
- Designing, reviewing and implementing cost-effective anti-corruption compliance policies, procedures and internal controls
- Performing international due diligence and training
- Navigating anti-corruption compliance issues in cross-border M&A, joint ventures, sourcing, contracting, distribution and sales
- Serving in regulatory auditor and monitor roles for preeminent companies and organizations
- Negotiating settlements and resolutions with the U.S. Department of Justice, U.S. Securities and Exchange Commission, and other government agencies

For more information or assistance, please feel free to communicate with your regular contacts at Bass, Berry & Sims, or the attorneys listed below. For more information and resources on this topic, please visit Bass, Berry & Sims' webpage on *Global Anti-Corruption/FCPA Compliance & International Investigations*.

Ross Booher	(615) 742-7764	rbooher@bassberry.com
Wally Dietz	(615) 742-6276	wdietz@bassberry.com
John Kelly	(202) 827-2953	jkelly@bassberry.com
Taylor Phillips	(202) 827-2995	tphillips@bassberry.com
Eli Richardson	(615) 742-7825	erichardson@bassberry.com
Kathryn Walker	(615) 742-7855	kwalker@bassberry.com

bassberry.com/FCPA