FCPA: DOJ and SEC Guidance (Part 5)

Hallmarks of an Effective Compliance Program

Introduction

In this fifth part of our client alert series on the Foreign Corrupt Practices Act ("FCPA"), we focus on the hallmarks of an effective compliance program. As in the first four parts of the series, the presentation is based on "*A Resource Guide to the U.S. Foreign Corrupt Practices Act*" (the "Guide"), issued by the U.S. Department of Justice ("DOJ") and the U.S. Securities and Exchange Commission ("SEC").[1]

Benefits Of An Adequate And Effective Compliance Program

There are a number of benefits associated with an adequate and effective compliance program. As indicated by the Guide, it "promotes 'an organizational culture that encourages ethical conduct and a commitment to compliance with the law.'"[2] Additionally, an effective compliance program "protects a company's reputation, ensures investor value and confidence, reduces uncertainty in business transactions, and secures a company's assets."[3] Moreover, an effective compliance program "helps prevent, detect, remediate, and report misconduct, including FCPA violations."[4]

Importantly, when deciding whether to take any action, and, if so, what action to take, the DOJ and SEC consider the adequacy of a compliance program, including "its design and good faith implementation and enforcement."[5] This consideration may result in the government declining to pursue charges, or resolving a company's charges through a deferred prosecution agreement or non-prosecution agreement.[6] Additionally, an adequate compliance program "will often affect the penalty amount and the need for a monitor."[7]

Tailoring

The Guide expressly states that there is "no one-size-fits-all" compliance program."[8] Every company must tailor its compliance program to its own "specific needs, risks, and challenges," and the government recognizes that "small- and medium-sized enterprises likely will have different compliance programs from large multi-national corporations."[9] Nevertheless, the Guide provides insight into the elements of a compliance program that the DOJ and SEC will ordinarily assess to determine its adequacy and effectiveness.[10]

---

[1] Crim. Div., U.S. DOJ & Enforcement Div., U.S. SEC, A Resource Guide to the U.S. Foreign Corrupt Practices Act (Nov. 14, 2012). In Part 1 of our series, we addressed the FCPA's jurisdictional reach as reflected in the Guide. In Part 2, we addressed FCPA liability under principles of parent-subsidiary and successor liability. In Part 3, we addressed who constitutes a "foreign official" under the FCPA. In Part 4, we addressed what payments and gifts are prohibited, or permitted, under the FCPA.

[2] Guide, supra note 1, at 56 (quoting U.S. Sentencing Guidelines § 8B2.1(a)(2)).

[3] Guide, supra note 1, at 56.

[4] Guide, supra note 1, at 56.

[5] Guide, supra note 1, at 56.

[6] Guide, supra note 1, at 56.

[7] Guide, supra note 1, at 56.

[8] Guide, supra note 1, at 57.

[9] See Guide, supra note 1, at 57.

[10] See Guide, supra note 1, at 57. Insight into the government's view of adequate compliance programs can also be found in a number of the DOJ's non-prosecution agreements. These agreements often require that a company implement or modify its compliance program to include, at a minimum, certain elements. These elements are substantially similar to those outlined in the Guide. See, e.g., Non-Prosecution Agreement, In re Lufthansa Technik AG (Dec. 21, 2011), available at http://www.justice.gov/criminal/fraud/fcpa/cases/lufthansa-technik/2011-12-21-lufthansa-npa.pdf; Non-Prosecution Agreement, In re RAE Sys. Inc. (Dec. 10, 2010), available at http://www.justice.gov/criminal/fraud/fcpa/cases/rae-

Hallmarks of an Adequate and Effective Compliance Program

The Guide sets out a number of elements that it states are the "hallmarks" of an adequate and effective compliance program.

1. Commitment from Senior Management and a Clearly Articulated Policy Against Corruption

Recognizing that employees take their cues from senior management, the Guide states that "compliance with the FCPA and ethical rules must start at the top."[11] The board of directors and senior executives should set "the proper tone" – that is, commit to a "culture of compliance."[12] A culture of compliance is reflected where "senior management has clearly articulated company standards, communicated them in unambiguous terms, adhered to them scrupulously, and disseminated them throughout the organization" – conduct that the DOJ and SEC evaluate in determining whether a company's compliance program is adequate.[13]

2. Code of Conduct and Compliance Policies and Procedures

The government encourages companies to have effective codes of conduct, which are "clear, concise, and accessible to all employees and to those conducting business on the company's behalf," and they should be available in the local language.[14] When assessing a compliance program, the government will evaluate steps taken to ensure that a company's code of conduct remains current and effective. Thus, companies should periodically review and update their code of conduct.[15]

Additionally, the government considers whether "a company has policies and procedures that outline responsibilities for compliance within the company, detail proper internal controls, auditing practices, and documentation policies, and set forth disciplinary procedures."[16] Policies and procedures will vary among companies, depending on the size and nature of a company's business and the corruption risks associated with the business.[17] Regardless of the policies and procedures that are implemented, companies must ensure that they are equally applied to personnel at all levels of a company.

3. Oversight, Autonomy, and Resources

Companies must assign responsibility for the oversight and implementation of company compliance programs to one or more senior executives who possess "appropriate authority within the organization, adequate autonomy from management, and sufficient resources to ensure that the company's compliance program is implemented effectively."[18] Adequate autonomy "includes direct access to an organization's governing authority, such as the board of directors and committees of the board of directors (e.g., the audit committee)."[19]

In assessing whether companies have adequate internal controls, the government considers whether companies devote adequate staffing and resources to their compliance program.[20] The government, however, recognizes that "the amount of resources devoted to compliance will depend on the company's size, complexity, industry, geographical reach, and risks associated with the business.[21]

systems/12-10-10rae-systems.pdf; Non-Prosecution Agreement, In re Paradigm B.V. (Sept. 21, 2007), available at http://www.justice.gov/criminal/fraud/fcpa/cases/paradigm/09-21-07paradigm-agree.pdf.

[11] See Guide, supra note 1, at 57.
[12] See Guide, supra note 1, at 57.
[13] Guide, supra note 1, at 57.
[14] See Guide, supra note 1, at 57.
[15] Guide, supra note 1, at 57-58.
[16] Guide, supra note 1, at 58.
[17] See Guide, supra note 1, at 58.
[18] See Guide, supra note 1, at 58.
[19] See Guide, supra note 1, at 58.
[20] Guide, supra note 1, at 58.
[21] See Guide, supra note 1, at 40, 58.

4. Risk Assessment

Assessment of risk is "fundamental to developing a strong compliance program" and is considered by the government when evaluating a company's compliance program.[22] The Guide cautions companies to avoid focusing their FCPA resources on low-risk markets to the detriment of high-risk markets.[23] Notably, the 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."[24] On the other hand, "a company that fails to prevent an FCPA violation on an economically significant, high-risk transaction because it failed to perform a level of due diligence commensurate with the size and risk of the transaction is likely to receive reduced credit based on the quality and effectiveness of its compliance program."[25] For example, a company with limited FCPA resources should place more scrutiny on a multi-million contract in a high risk country than on the provision of modest gifts and entertainment to foreign officials.[26]

If a company's risk of potential FCPA violations increases, the company should consider increasing its compliance procedures, including due diligence and periodic internal audits.[27] The degree of appropriate due diligence is fact-specific and depends on, among other things, "the country and industry sector, the business opportunity, potential business partners, level of involvement with governments, amount of government regulation and oversight, and exposure to customs and immigration in conducting business affairs."[28]

5. Training and Continuing Advice

The government will evaluate "whether a company has taken steps to ensure that relevant policies and procedures have been communicated throughout the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners."[29] Training should cover "company policies and procedures, instruction on applicable laws, practical advice to address real-life scenarios, and case studies."[30] Additionally, training should be appropriate for the targeted audience. For example, companies should train their sales personnel differently from their accounting personnel in order to cover the different types of scenarios that each may encounter. Training should also occur in the local language.

The government also encourages companies to develop measures, depending on the size and sophistication of the company, to "provide guidance and advice on complying with the company's ethics and compliance program, including when such advice is needed urgently."[31] For example, a large company conducting business in high-risk countries may want to set up an ethics and compliance hotline.

6. Disciplinary Measures and Incentives

The government considers whether a company enforces its compliance program appropriately. Thus, the government will evaluate whether a company "has appropriate and clear disciplinary procedures, whether those procedures are applied reliably and promptly, and whether they are commensurate with the violation."[32] A company's disciplinary measures should be fairly and consistently applied to employees at every level of a company.

[22] Guide, supra note 1, at 58.
[23] See Guide, supra note 1, at 58.
[24] Guide, supra note 1, at 59.
[25] Guide, supra note 1, at 59.
[26] See Guide, supra note 1, at 58-59.
[27] See Guide, supra note 1, at 59.
[28] Guide, supra note 1, at 59.
[29] Guide, supra note 1, at 59.
[30] See Guide, supra note 1, at 59.
[31] Guide, supra note 1, at 59.
[32] Guide, supra note 1, at 59.

Additionally, the government recognizes that compliant behavior can be encouraged through positive incentives, "such as personnel evaluations and promotions, rewards for improving and developing a company's compliance program, and rewards for ethics and compliance leadership."[33] The Guide further notes that some companies have made adherence to compliance a large metric for determining management bonuses, which has the consequential effect of making compliance an everyday concern for management.[34]

7. Third-Party Due Diligence and Payments

Given that third parties are often used as a means to conceal bribes to foreign officials, the government views risk-based due diligence with respect to third parties as particularly important. As indicated by the Guide, factors that might lead a company to perform heightened due diligence when engaging a third party to assist in transacting business in another country include the following:

- the market (high-risk country);
- the size and significance of the deal to the company;
- the company's first-time use of the third party;
- the third party's strong ties to political and government leaders;
- if the third party's fee is, in part, dependent on the success of the deal or if the third party requests an up front allowance; and
- if the contract with the consultant defines the services to be performed in vague terms.[35]

The Guide provides the following principles that should be applied when companies deal with third parties:

- Companies should understand the qualifications and associations of the third party, including its business reputation and relationship with foreign officials.[36]
- Companies should understand the business rationale for including a third party in a transaction and ensure that the contract terms specifically describe the services to be performed and that the compensation is commensurate to those services.
- Companies should monitor third-party relationships on an ongoing basis, which may include exercising audit rights and providing periodic training.[37]

In order to mitigate third-party risk, the Guide encourages companies to educate third parties about the companies' compliance program and commitment to ethical and lawful business practices.[38] Additionally, companies may seek assurances from third parties by requesting FCPA compliance certifications.[39]

8. Confidential Reporting and Internal Investigation

The Guide states that an effective compliance program "should include a mechanism for an organization's employees and others to report suspected or actual misconduct or violations of the company's policies on a confidential basis and without fear of retaliation."[40] For example, a company may set up an anonymous hotline, or employ ombudsmen.[41] If suspected misconduct is reported, companies should have an efficient, reliable, and properly funded process for investigating the report. Additionally, the company's response should be documented, including all disciplinary and remedial measures taken.[42]

[33] Guide, supra note 1, at 59-60.
[34] Guide, supra note 1, at 60.
[35] See Guide, supra note 1, at 63.
[36] While it is not illegal to contract with a third party closely connected to a foreign official, such relationships can be susceptible to corruption. Guide, supra note 1, at 63.
[37] Guide, supra note 1, at 60, 63.
[38] Guide, supra note 1, at 60-61.
[39] Guide, supra note 1, at 61.
[40] Guide, supra note 1, at 61.
[41] Guide, supra note 1, at 61.
[42] Guide, supra note 1, at 61.

9. Continuous Improvement: Periodic Testing and Review

Finally, as a company's business changes, so should its compliance program. The government evaluates whether companies "regularly review and improve their compliance programs and not allow them to become stale."[43] The Guide suggests that companies take the time to test their controls and discover potential weaknesses and risk areas.[44] For example, companies may have their employees take surveys designed to measure whether the company has succeeded in establishing a culture of compliance.[45] Companies may also perform targeted audits to ensure that their established internal controls are actually effective. Importantly, the Guide notes that the government will give "meaningful credit to thoughtful efforts to create a sustainable compliance program if a problem is later discovered."[46]

BOOKS AND RECORDS

A company's corporate policy against FCPA violations should specifically address the necessity of maintaining accurate books and records.[47] Bribery is often masked on a company's books and records through mischaracterization. For instance, the corrupt giving of gifts or making of payments should not be recorded on a company's books as "business fees" or "travel and entertainment" expenses.[48] As reflected in various non-prosecution agreements, an adequate and effective compliance program should include "a system of financial and accounting procedures, including a system of internal controls, reasonably designed to ensure the maintenance of fair and accurate books, records, and accounts to ensure that they cannot be used for the purpose of foreign bribery or concealing such bribery."[49]

The failure to maintain fair and accurate books and records may result in both civil and criminal liability. For example, a multinational engineering and electronics conglomerate, which "engaged in systematic efforts to falsify its corporate books and records and knowingly failed to implement and circumvent existing internal controls," pleaded guilty to criminal charges that it had violated the FCPA's internal controls and books and records provisions.[50] The company agreed to pay a criminal fine of $450 million, as well as $350 million in disgorgement of profits in order to settle a related SEC civil complaint.[51]

[43] Guide, supra note 1, at 62.
[44] Guide, supra note 1, at 62.
[45] See Guide, supra note 1, at 62.
[46] Guide, supra note 1, at 62.
[47] See Non-Prosecution Agreement, In re Lufthansa Technik AG (Dec. 21, 2011), available at http://www.justice.gov/criminal/fraud/fcpa/cases/lufthansa-technik/2011-12-21-lufthansa-npa.pdf; Non-Prosecution Agreement, In re RAE Sys. Inc. (Dec. 10, 2010), available at http://www.justice.gov/criminal/fraud/fcpa/cases/rae-systems/12-10-10rae-systems.pdf.
[48] See, e.g., Non-Prosecution Agreement, In re RAE Sys. Inc. (Dec. 10, 2010).
[49] See, e.g., Non-Prosecution Agreement, In re Lufthansa Technik AG (Dec. 21, 2011); Non-Prosecution Agreement, In re RAE Sys. Inc. (Dec. 10, 2010); Non-Prosecution Agreement, In re Paradigm B.V. (Sept. 21, 2007), available at http://www.justice.gov/criminal/fraud/fcpa/cases/paradigm/09-21-07paradigm-agree.pdf.
[50] See Press Release, DOJ, Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to pay $450 Million in Combined Criminal Fines (Dec. 15, 2008), available at http://www.justice.gov/opa/pr/2008/December/08-crm-1105.html; see also Plea Agreement, United States v. Siemens AG, No. 08-CR-367-RJL (D.D.C. Dec. 12, 2008), available at http://www.justice.gov/criminal/fraud/fcpa/cases/siemens/12-15-08siemensakt-plea.pdf.
[51] See Press Release, DOJ, Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to pay $450 Million in Combined Criminal Fines (Dec. 15, 2008); see also Plea Agreement, United States v. Siemens AG, No. 08-CR-367-RJL (D.D.C. Dec. 12, 2008).

Case Studies

(a) Adequate Compliance Program

Under traditional principles of respondeat superior, a company is liable for the criminal acts of its directors, officers, and employees, undertaken within the scope of their employment, even if the company maintains policies and a compliance program designed to prevent the criminal conduct.[52] While this principle applies in the FCPA context, an adequate compliance program can play a role in persuading law enforcement authorities to decline to prosecute as a matter of prosecutorial discretion where there has been misconduct by an employee. As an example, the DOJ and SEC declined to take FCPA enforcement action against an investment bank where one of its executives "used a web of deceit" to evade the investment bank's efforts to maintain adequate anti-corruption internal controls.[53] In declining to take FCPA enforcement action against the investment bank, the government considered the following:

- The investment bank maintained a system of internal controls meant to ensure accountability for its assets and to prevent employees from offering, promising or paying anything of value to foreign government officials.
- The investment bank's internal policies, which were frequently updated, prohibited bribery and addressed corruption risks associated with the giving of gifts and payment of expenses related to entertainment, travel, lodging, and meals.
- The investment bank frequently trained its employees, including the executive involved in the misconduct, on its internal policies, the FCPA, and other anti-corruption laws.
- Compliance personnel regularly monitored transactions, randomly audited particular employees, transactions and business units, and tested to identify illicit payments.
- Compliance personnel had a direct reporting line to the board of directors.
- The investment bank conducted extensive due diligence on all new business partners, including those involved in the misconduct, and imposed stringent controls on payments made to business partners.[54]

[52] See United States v. Ionia Mgmt. S.A., 555 F.3d 303, 309-310 (2d Cir. 2009) (in affirming the conviction of a company based on the conduct of its employees, refusing to "adopt the suggestion that the prosecution, in order to establish vicarious liability, should have to prove as a separate element in its case-in-chief that the corporation lacked effective policies and procedures to deter and detect criminal actions by its employees"); United States v. Twentieth Century Fox Film Corp., 882 F.2d 656, 660 (2d Cir. 1989) (holding that defendant company's "compliance program, however extensive, [did] not immunize the corporation from liability when its employees, acting within the scope of their authority, fail[ed] to comply with the law" and violated an antitrust consent decree).

[53] See Guide, supra note 1, at 61; see also Press Release, DOJ, Former Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA (Apr. 25, 2012), available at http://www.justice.gov/opa/pr/2012/April/12-crm-534.html. The investment bank engaged in a joint venture with a Chinese state-owned entity, which purportedly sought to co-invest in a real estate transaction through a special purpose vehicle ("SPV") along side the investment bank. Unknown to the investment bank at the time, one of its executives had arranged the transaction in order to transfer a multi-million dollar ownership interest in the real estate to himself, a Canadian attorney, and a Chinese public official. Notwithstanding its comprehensive compliance program, the investment bank failed to detect, at the time of the investment, that the SPV was owned by the executive, the attorney, and the foreign official, rather than owned by the Chinese state-owned entity. As a result, when the transaction occurred, the foreign official realized a multi-million dollar gain. See Guide, supra note 1, at 61; see also Information, United States v. Peterson, 12-CR-224 (E.D.N.Y. 2012), available at http://www.justice.gov/criminal/fraud/fcpa/cases/petersong/petersong-information.pdf.

[54] See Guide, supra note 1, at 61; see also Press Release, DOJ, Former Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA (Apr. 25, 2012). The investment bank's due diligence on the Chinese state-owned entity consisted of the following:

Given the investment bank's adequate compliance program, along with its voluntary disclosure of the misconduct and cooperation with the government's investigation, no FCPA enforcement action was taken against the investment bank.[55]

(b) Inadequate Compliance Program

Failing to implement or maintain an adequate compliance program can have costly repercussions. For example, a telecommunications company, lacking an adequate compliance program, pleaded guilty to violating the FCPA's anti-bribery and accounting provisions and was ordered to pay a $13 million criminal fine.[56] The telecommunications company also settled with the SEC, agreeing to pay $15.4 million in disgorgement and prejudgment interest.[57]

The criminal information charging the telecommunications company with violating the FCPA focused on the company's lack of internal controls, which included the following:

- The company never had a formal FCPA compliance program or procedures.
- The company did not enforce its only FCPA-related policy, set forth in the company's Code of Ethics, which was that "employees must be fully familiar with and strictly adhere to such provisions of the [FCPA] that prohibit payments or gifts to foreign government officials for the purpose of influencing official government acts or assistance in obtaining business."
- The company did not require employees of its wholly-owned subsidiary to sign the company's Code of Ethics.
- The company provided its employees with no information concerning the FCPA or its purpose.
- The company never conducted any FCPA compliance training.
- The company did not maintain any due diligence files on its foreign agents.
- The company failed to perform adequate due diligence on the foreign consultant who was the recipient of millions of dollars from the company.
- The company failed to investigate properly warnings from its external auditor that the company's subsidiary did not have a reliable accounting system in place and that various payments could not be substantiated.
- The company failed to take corrective action with respect to the external auditor's warnings

---

- reviewing Chinese government records;
- speaking with sources familiar with the local Chinese real estate market;
- checking the government entity's payment records and credit references;
- conducting an on-site visit and placing a pretextual telephone call to the entity's offices;
- searching media sources; and
- conducting background checks on the entity's principals.

Additionally, the investment bank's due diligence on the SPV, as well as other SPVs connected to the Chinese state-owned entity, included:

- obtaining a letter with designated bank account information from a Chinese official associated with the government entity;
- using an international law firm to request and review 50 documents from the SPVs' Canadian attorney;
- interviewing the Canadian attorney; and
- interviewing the SPVs' management.

See Guide, supra note 1, at 61.

[55] The investment bank executive directly responsible for the misconduct pleaded guilty to conspiracy to violate the FCPA's internal control provisions and also settled with the SEC. See Press Release, DOJ, Former Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA (Apr. 25, 2012).

[56] Plea Agreement, United States v. Titan Corp., No. 05-CR-314-BEN (S.D. Cal. Mar. 1, 2005), available at http://www.justice.gov/criminal/fraud/fcpa/cases/titan-corp/03-01-05titan-plea.pdf.

[57] Lit. Rel. No. 19107, SEC v. Titan Corp., No. 05-0411 (D.D.C. Mar. 1, 2005), available at https://www.sec.gov/litigation/litreleases/lr19107.htm.

and failed to report the issues to its internal audit committee.[58]

In addition to the costly criminal and civil fines and penalties, the telecommunications company was ordered to serve three years of supervised probation conditioned on the institution of a strict compliance program and internal controls designed to prevent future FCPA violations.[59]

Conclusion

Companies should implement and maintain adequate and effective compliance programs to reduce the likelihood of FCPA violations and subsequent government enforcement action. To that end, the Guide provides useful insight into the government's view of the hallmarks of an adequate and effective compliance program. Adapting and applying those hallmarks will greatly enhance a company's compliance program.

Given that the DOJ and SEC "may decline to pursue charges against a company based on the company's effective compliance program," companies should ensure that their compliance programs feature the hallmarks indicated in the Guide.[60]

ABOUT CURTIS

Curtis, Mallet-Prevost, Colt & Mosle LLP is a leading international law firm. Headquartered in New York, Curtis has sixteen offices in the United States, Mexico, Europe, the Middle East and Central Asia. Curtis represents a wide range of clients, including multinational corporations and financial institutions, governments and state-owned companies, money managers, sovereign wealth funds, family-owned businesses, individuals and entrepreneurs.

For more information about Curtis, please visit www.curtis.com.

For further information, contact:

Jacques Semmelman, New York Partner

E-mail: jsemmelman@curtis.com

Tel.: 212 696-6067

Myles K. Bartley, New York Counsel

E-mail: mbartley@curtis.com

Tel.: 212 696-6098

Matthew McCullough, Washington, D.C. Counsel

E-mail: mmccullough@curtis.com

Tel: 202 452-7327

[58] Information, United States v. Titan Corp., No. 05-CR-314-BEN (S.D. Cal. Mar. 1, 2005), available at http://www.justice.gov/criminal/fraud/fcpa/cases/titan-corp/03-01-05titan-info.pdf.
[59] Plea Agreement, United States v. Titan Corp., No. 05-CR-314-BEN (S.D. Cal. Mar. 1, 2005).
[60] Guide, supra note 1, at 56.

Andrew Kaspersen, Associate (New York), assisted in the preparation of this Client Alert.