BakerHostetler

AN OVERVIEW OF THE DODD-FRANK ACT WHISTLEBLOWER PROVISIONS AND THE FOREIGN CORRUPT PRACTICES ACT

I. DODD-FRANK

On July 21, 2010, President Obama signed into law the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act" or "Dodd-Frank"), a wide-reaching statute designed to address the causes of the 2008-2009 financial crisis. The Dodd-Frank Act contains, among other things, significant whistleblower incentives and programs, including the creation of a whistleblower program for the United States Securities and Exchange Commission (the "SEC"), the agency primarily responsible for enforcement of United States federal securities law. It also expanded whistleblower protections under the Sarbanes-Oxley Act of 2002 ("SOX") and created a new whistleblower cause of action for employees performing tasks in the consumer financial products and services sector.

Section 922 of the Dodd-Frank Act amended the Securities Exchange Act of 1934 (the "Exchange Act") by adding section 21F, which created a whistleblower bounty program. The program provides monetary incentives for whistleblowers to report securities law violations to the SEC. Specifically, it requires the SEC to pay an award to one or more whistleblowers that voluntarily provide original information to the SEC that leads to the successful enforcement of a violation of federal securities laws resulting in monetary sanctions exceeding $1 million. The award must range from at least 10 percent to a maximum of 30 percent of the total monetary sanctions imposed in the enforcement action. Section 922 of the Dodd-Frank Act also prohibits retaliation by employers against individuals who provide the SEC with information about possible securities law violations.

The SEC issued final rules implementing the Dodd-Frank whistleblower provisions, effective August 12, 2011, and established a separate office, the SEC Office of the Whistleblower, to administer and enforce its whistleblower program.[1] The SEC whistleblower program was highly anticipated by various constituencies, from plaintiffs' attorneys to corporate counsel, due to its potential to greatly increase reporting of possible corporate misconduct to the SEC. This fear does not appear to be unfounded if the number of tips received in the first seven weeks after the rules became effective—334 tips, i.e., an average of almost seven tips per day—is any indication of what is to come.[2] Indeed, as discussed further below, the number of tips has only increased in fiscal year 2012 to 3,001 whistleblower tips, an average of eight tips per day. Below is an overview of some of the key whistleblower provisions.

A. The SEC Whistleblower Program

1. Whistleblower Definition

Section 922 and the final SEC whistleblower rules define a whistleblower as any individual, alone or jointly with others, who provides information to the SEC, in accordance with set procedures specified by the SEC, relating to a possible violation of federal securities laws (including any rules and regulations thereunder).[3] Entities do not qualify to receive a bounty.[4] Moreover, the SEC has stated that the term

---

[1] Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934, Release No. 34-64545 (Aug. 12, 2011) ("Final Rules"), *available at* http://www.sec.gov/rules/final/2011/34-64545.pdf; 17 C.F.R. pts. 240 & 249.
[2] Sec. Exch. Comm'n, Annual Report on the Dodd-Frank Whistleblower Program for Fiscal Year 2011 (Nov. 2011), *available at* http://www.sec.gov/about/offices/owb/whistleblower-annual-report-2011.pdf.
[3] 15 U.S.C. § 78u-6(a)(6); 17 C.F.R. § 240.21F-2(a).
[4] *Id*.

"possible violation" requires that the information "should indicate a facially plausible relationship to some securities law violation—frivolous submissions would not qualify for whistleblower status."[5]

2. Eligibility for an Award

a. Voluntary Submission

Only individuals who submit information to the SEC "voluntarily" are entitled to a bounty.[6] That means the submission is not due to a legal or contractual duty and is made prior to the whistleblower's receipt of a request, inquiry or demand for information related to the submission from the SEC, Congress or another regulatory/enforcement agency or self-regulatory organization.[7]

b. Original Information

In addition, to qualify for an award, information provided by a whistleblower must be original.[8] To be deemed "original" the information provided by the whistleblower must be, among other things, derived from the "independent knowledge or analysis" of the whistleblower.[9] The SEC rules define "independent knowledge" as factual information in the whistleblower's possession that she did not derive from publicly available sources and explain that a whistleblower may gain independent knowledge from her experiences, communications and observations from business or social interactions.[10] The rules define "independent analysis" as the whistleblower's examination and evaluation, whether done alone or in combination with others, of information that may be publicly available, but which reveals information not generally known or available to the public.[11] The implication of these provisions is that they create a race to report as only the first person to report a violation is eligible to receive an award.

c. Exclusions From Award Eligibility

Not everyone is entitled to receive an award. Certain people such as employees of certain agencies (e.g., law enforcement agencies) and people criminally convicted in connection with the conduct are not entitled to an award.[12] A culpable whistleblower will not receive an award based on the monetary sanctions she or any entity whose liability is based on conduct the whistleblower directed pays in the resulting SEC action.[13] Moreover, the following categories of professionals typically would not qualify as whistleblowers if the information they learn is obtained by virtue of their position:

- In-house and outside counsel, and other non-attorneys involved in the legal representation, who obtain the information through attorney-client privileged communications;[14]
- Officers, directors, trustees, or partners of an entity who learn the information from another person or in connection with the entity's process for identifying, reporting and addressing possible violations of the law;[15]
- Employees or independent contractors with compliance or internal audit responsibilities;[16]

[5] Final Rules at 13.
[6] 15 U.S.C. § 78u-6(b)(1); 17 C.F.R. § 240.21F-3(a)(1).
[7] 17 C.F.R. § 240.21F-4(a).
[8] 15 U.S.C. § 78u-6(b)(1); 17 C.F.R. § 240.21F-3(a)(2).
[9] 15 U.S.C. § 78u-6(a)(3)(A); 17 C.F.R. § 240.21F-4(b)(1).
[10] 17 C.F.R. § 240.21F-4(b)(2).
[11] 17 C.F.R. § 240.21F-4(b)(3).
[12] 15 U.S.C. § 78u-6(c)(2).
[13] 17 C.F.R. § 240.21F-16.
[14] 17 C.F.R. § 240.21F-4(b)(4)(i)-(ii).
[15] 17 C.F.R. § 240.21F-4(b)(4)(iii)(A).

- Persons employed or associated with a firm retained to conduct an inquiry or investigation into possible violations of law;[17] or

- Persons employed or associated with a public accounting firm who learned the information through the performance of an engagement required of an independent public accountant under the federal securities laws and the information relates to a violation by the engagement client or the client's directors, officers or other employees.[18]

The professionals listed above—other than in-house and outside counsel—would be entitled to an award, however, if: (1) they reasonably believe disclosure may prevent substantial injury to the financial interest or property of the entity or investor; (2) they reasonably believe that the entity is engaging in conduct that will impede an investigation of the misconduct; or (3) at least 120 days have elapsed since they reported the information to their supervisor or the entity's audit committee, chief legal officer, chief compliance officer, or at least 120 days have elapsed since they received the information and they received the information under circumstances indicating that these individuals were already aware of the information.[19]

3. Award Amounts

If the whistleblower meets the conditions set forth above, the SEC must pay an award of at least 10 percent and not more than 30 percent of the monetary sanctions collected in the case.[20] The SEC can also pay an award to a whistleblower based on monetary sanctions that are collected from "related actions," such as an enforcement action commenced by the United States Department of Justice (the "DOJ") or another governmental agency.[21]

The SEC must consider the following criteria which may increase a whistleblower's percentage award: (1) the significance of the information provided; (2) the degree of assistance provided by the whistleblower; (3) law enforcement interest in making a whistleblower award; and (4) participation in internal compliance systems.[22] Additional criteria that the SEC will consider, may decrease the award, including: (1) culpability of the whistleblower; (2) unreasonable reporting delay by the whistleblower; or (3) interference with internal compliance and reporting systems by the whistleblower.[23] Notably, while the SEC contends that the whistleblower rules are meant to encourage the use of internal compliance and reporting systems, the rules do not bar a person who has materially interfered with one of those systems from receiving an award.[24]

4. Anti-Retaliation Provisions for Employee-Whistleblowers

Employers may not retaliate against employee-whistleblowers who report securities law violations. The Dodd-Frank Act provides that no employer may discharge, demote, suspend, threaten, harass or in any other manner discriminate against a whistleblower in terms of employment.[25] The retaliation provisions protect employees who either: (1) provide information to the SEC pursuant to the whistleblower provisions; (2) initiate, testify in or assist in any SEC investigation or action pursuant to the

[16] 17 C.F.R. § 240.21F-4(b)(4)(iii)(B).
[17] 17 C.F.R. § 240.21F-4(b)(4)(iii)(C).
[18] 17 C.F.R. § 240.21F-4(b)(4)(iii)(D).
[19] 17 C.F.R. § 240.21F-4(b)(4)(v)(A)-(C).
[20] 15 U.S.C. § 78u-6(b)(1); 17 C.F.R. § 240.21F-5.
[21] *Id*.
[22] 15 U.S.C. § 78u-6(c)(1)(B)(i)(I)-(III); 17 C.F.R. § 240.21F-6(a).
[23] 15 U.S.C. § 78u-6(c)(1)(B)(i)(IV); 17 C.F.R. § 240.21F-6(b).
[24] Final Rules at 5.
[25] 15 U.S.C. § 78u-6(h)(1)(A).

whistleblower provisions; or (3) make disclosures that are required or protected under the SOX, the Exchange Act, or any other law subject to the SEC's jurisdiction. [26]

To obtain anti-retaliation protection, an employee must have a reasonable belief that the information provided relates to a possible securities law violation that has occurred, is ongoing or is about to occur.[27] The employee may bring an action against her employer directly in federal district court, which can result in a jury trial.[28] The applicable statute of limitations is the later of six years from the date of the alleged retaliation or three years from the date of discovery; an action, however, may not in any circumstance be brought more than 10 years after the date on which the violation occurs.[29] If an employee can establish retaliation, she will be entitled to reinstatement and two times back pay with interest.[30]

B. THE SEC WHISTLEBLOWER ANNUAL REPORT

In November 2012, the SEC issued an Annual Report on the whistleblower program, providing insight into the number of tips received during fiscal year 2012.[31] During this period, the SEC received 3,001 whistleblower tips—an average of eight tips per day.

The report included an analysis of the tips based on the whistleblower's self-categorization. When a whistleblower submits a tip, either through the SEC's online questionnaire or by hard copy using the agency's Tip, Complaint or Referral form, they must classify the type of violation they are reporting. An analysis of the whistleblowers' self-categorization revealed that:

- The most common tips concerned: (1) corporate disclosures and financials (18.2 percent); (2) offering fraud (15.5 percent) and (3) market manipulation (15.2 percent).
- Nearly a quarter of the tips (23.4 percent) were classified by whistleblowers as "other," where the whistleblower did not use one of the SEC's defined categories.
- Less than 4 percent of the tips were FCPA violations.
- Less than 7 percent of the tips were related to insider trading.

The report also provided where the whistleblowers were located:

- A little more than half of the tips were received from domestic tipsters (64 percent) representing 37 states.
- California (17.4 percent), New York (9.8 percent), Florida (8.1 percent), and Texas (6.3 percent) were the source of almost half of the domestic tips.
- 10.8 percent of the tips were received from overseas, with the United Kingdom (74 tips), Canada (46 tips), India (33 tips), China (27 tips), and Australia (21 tips) making up more than half of the 324 tips received from international whistleblowers.
- Almost 6 percent of whistleblowers did not indicate their geographic location.

---

[26] *Id*.
[27] 17 C.F.R. § 240.21F-2(b)(1)(i).
[28] 15 U.S.C. § 78u-6(h)(1)(B)(i).
[29] 15 U.S.C. § 78u-6(h)(1)(B)(iii).
[30] 15 U.S.C. § 78u-6(h)(1)(C).
[31] Sec. Exch. Comm'n, Annual Report on the Dodd-Frank Whistleblower Program for Fiscal Year 2012 (Nov. 2012), *available at* http://www.sec.gov/about/offices/owb/annual-report-2012.pdf.

Though the final rules to the Dodd-Frank Act went into effect on August 12, 2011, anyone who submitted a tip to the SEC after July 21, 2010, is eligible to receive an award.[32] The whistleblower fund has more than $450 million available to pay whistleblowers. During fiscal year 2012, 143 enforcement judgments and orders were issued which resulted in sanctions of more than $1 million, all of which are eligible for a whistleblower reward.[33] On August 21, 2012, the SEC paid its first award—a modest $50,000. The agency went to great lengths to guard the whistleblower's anonymity, revealing only that the informant provided substantial information that led a court to order more than $1 million in sanctions, of which $150,000 had already been collected.[34] The SEC's second award, ordered in June 2013, is expected to be about $125,000 and will be split among three whistleblowers.[35] Although federal securities regulators have only made two whistleblower awards to date, the SEC has forecasted that the pace of whistleblower awards will likely quicken.

C. WHAT COMPANIES SHOULD DO

Companies should continue to expect an increase in whistleblower activity, and should recognize that the large potential awards, the dynamics of the SEC's rules, and the large number of law firms publicly recruiting whistleblowers, significantly increase the risk that employees will bypass internal reporting mechanisms and go straight to the SEC. Even if employees report internally first, the rules will put companies under increased pressure to investigate quickly and determine whether self-reporting to the SEC is appropriate.

Companies must reexamine their internal compliance programs and how they communicate necessary information to employees. Internal disclosure does not bar an award if the internal report leads the company to self-disclose. Therefore, companies should implement compliance programs that motivate employees to report internally first. These programs should be easy to understand and use. As part of any communication about the compliance program, companies should emphasize that they have a robust process by which employees can and are encouraged to report violations through the company's whistleblower hotline or should set one up, if they do not have one. The company also should emphasize that it will protect the employee's anonymity if so desired. Companies must remind employees that periodic certification and sub-certification programs require them to advise of suspected wrongdoing, and that internal reporting benefits the company by enabling it to sort through facts privately before deciding whether something is serious enough to require self-reporting to the SEC. Companies should further remind employees that some information they may encounter is subject to the company's attorney-client privilege, which is not subject to waiver by employees. In addition, companies should reinforce their policies against retaliating against whistleblowers and train their human resource executives and other business leaders on the anti-retaliation provisions of Dodd-Frank and SOX.

The company should further develop procedures on how to deal with a complaint once it is received to ensure an appropriate response. It also should document the receipt of the complaint and the steps taken to address the complaint. For fact-gathering and assessment purposes, the company should interview the complainant and any witnesses and identify and review any relevant documents. The company should consider putting a litigation hold in place. Further, to minimize any potential retaliation liability, the company should notify the complainant's supervisor of the filed complaint and prohibit the supervisor from taking any adverse action against the complainant as a result of the complaint. The company also should instruct the supervisor to refer any performance or other issues concerning the complainant to Human Resources to allow for careful and detailed documentation of any counseling sessions, performance evaluations or other discipline to create a strong record for any defense that the

[32] 17 C.F.R. § 240.21F-4(b)(1)(iv).
[33] *See* Annual Report on the Dodd-Frank Whistleblower Program for Fiscal Year 2012 at 8.
[34] Press Release, Sec. & Exch. Comm'n, *SEC Issues First Whistleblower Program Award* (Aug. 21, 2012), *available at* http://sec.gov/news/press/2012/2012-162.htm.
[35] Press Release, Sec. & Exch. Comm'n, *SEC Announces Whistleblower Action* (June 12, 2012), *available at* http://www.sec.gov/news/press/2013/2013-06-announcement.htm; Press Release, Sec. & Exch. Comm'n, *SEC Rewards Three Whistleblowers Who Helped Stop Sham Hedge Funds* (Aug. 30, 2013), *available at* http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539796657.

adverse action was non-retaliatory. Human Resources should also conduct an exit interview of a departing whistleblower to confirm that the departure, whether voluntary or performance-based, does not constitute retaliatory termination.

It is never too early to work with counsel experienced in SEC enforcement actions to establish procedures for handling whistleblower complaints, including communication protocols that will assure an employee that the company is taking the matter seriously. The adoption of the new whistleblower rules is a good reason for companies to revisit their internal process for dealing with SEC investigations and with internal complaints about securities violations. The handling of any whistleblower complaint will also require the assistance of employment counsel who can help navigate the anti-retaliation provisions once a whistleblower has been identified. Companies should connect now with counsel experienced in SEC investigations so that they do not waste any time selecting qualified counsel once an issue arises.

II. FOREIGN CORRUPT PRACTICES ACT

Since 1977, public companies and private domestic concerns have been subject to the Foreign Corrupt Practices Act (the "FCPA"), which aims to punish those who bribe foreign officials.[36] While individuals who actually engage in the bribery are charged and convicted by the government under the statute, it is still much more common for the individuals' companies to face criminal and civil liability under the FCPA. Companies may protect themselves from FCPA exposure by maintaining reasonable compliance procedures, internal controls, and accounting methods, conducting prompt internal investigations of potential FCPA violations, and taking appropriate corrective action if a FCPA violation is uncovered. FCPA actions continue to be a high priority for the DOJ and the SEC, so the procurement of counsel that is well-versed in the intricacies of FCPA regulation is becoming more necessary. The fact that the DOJ's and SEC's manual (the "Guide"), which sets forth in detail the FCPA's statutory requirements while also providing insight into DOJ and SEC enforcement practices, is 130-pages long clearly indicates that FCPA enforcement is here to stay, and highlights the complexity of the FCPA and the need for experienced counsel.[37]

A. FCPA Anti-Bribery Provisions

The anti-bribery provisions of the FCPA make it unlawful for a United States citizen or entity and certain foreign individuals and entities, to make a corrupt payment to a foreign official for the purpose of obtaining or retaining business for or with, or directing business to, any person.[38] Thus, a payment violates the anti-bribery provisions of the FCPA if it is: (1) a corrupt payment; (2) made to a foreign official; and (3) prompted by an improper purpose.

1. Corrupt Payment

A "corrupt payment" includes the payment, offer, gift, or authorization of the giving of money or of "anything of value."[39] The payment need not be monetary. The FCPA prohibits the payment, or offer of

[36] 15 U.S.C. §§ 78(m), 78dd(1)-(3), 78ff (2006).
[37] U.S. Dep't of Justice & U.S. Sec. & Exch. Comm'n, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (the "Guide"), available at http://www.justice.gov/criminal/fraud/fcpa/guidance/, and http://www.sec.gov/spotlight/fcpa.shtml. Released in November 2012, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* is the DOJ's and SEC's detailed compilation of information about the FCPA, its provisions, and enforcement. The Guide provides a comprehensive overview of the nuts and bolts of the FCPA – who it covers, the jurisdictional scope and what it prohibits. Of greater significance, though, is the Guide's treatment of numerous hot-button issues. As FCPA enforcement actions have grown over the past five years, companies have found themselves in an increasingly difficult position of not knowing where permissible conduct crosses into impermissible violations of the FCPA. The Guide addresses these hot button issues including the definition of a "foreign official," the use of "facilitation payments" and the scope of successor liability. On these and other topics, the Guide takes a multi-faceted approach, setting forth in detail the statutory requirements while also providing insight into DOJ and SEC enforcement practices through hypotheticals, examples of enforcement actions and anonymized declinations, and summaries of applicable case law and DOJ opinion releases.
[38] 15 U.S.C. §§ 78dd(1)-(3).
[39] 15 U.S.C. §§ 78dd-1(a), 78dd-2(a).

payment, of "anything of value" and "anything of value" may include even items of *de minimis* value.[40] Distinguishing between legitimate business entertaining expenses, especially in countries such as China where business gifts are customary, can present challenges to companies conducting business abroad. Factors to consider when evaluating whether a gift qualifies as an improper payment include the value and reasonableness of the gift, whether the gift was proper under local laws and customs, and whether it was made openly and transparently.[41]

The DOJ and SEC distinguish legitimate gifts and business entertaining expenses from improper payments based on corrupt intent. The Guide states that items of nominal value, such as cab fare, reasonable meals and entertainment expenses, or a company's promotional items, are unlikely to improperly influence an official and, as a result, are not, without more, items that have resulted in enforcement actions by the DOJ or SEC.[42] However, larger, extravagant gifts, such as sports cars and fur coats, as well as widespread gifts of smaller items, may form the basis of an enforcement action because such gifts more likely evince a corrupt intent.[43]

2. Foreign Official

The FCPA defines "foreign official" as "any officer or employee of a foreign government or any department, agency or instrumentality thereof."[44] While identifying a foreign official may seem to be an easy task at times, a hot-button issue is whether the definition of foreign official under the FCPA includes employees of state-owned entities. According to the DOJ and SEC, it can. Whether a particular entity constitutes an "instrumentality" under the FCPA, and thus, is included under the FCPA's anti-bribery provisions, requires a fact-specific analysis of an entity's ownership, control, status, and function.[45] United States courts have identified several factors in making this determination, including: (1) the foreign state's characterization of the entity and its employees; (2) the foreign state's degree of control over the entity; (3) the purpose of the entity's activities; and (4) the extent of the foreign state's ownership of the entity and level of financial support, such as subsidies, special tax treatment, and loans.[46]

The DOJ and SEC have pursued cases for corrupt payments made to employees of state-owned companies since the enactment of the FCPA, and have long used an analysis of ownership, control, status, and function to determine whether a particular entity is an agency or instrumentality of a foreign government.[47] In one case, Miami telecommunications executives were charged with paying bribes to employees of Haiti's state-owned and controlled telecommunications company. The company was 97 percent owned and 100 percent controlled by the Haitian government, and its director was appointed by Haiti's president.[48]

According to the DOJ and SEC, as a practical matter, an entity is unlikely to be deemed an instrumentality if a government does not own or control a majority of its shares.[49] The DOJ and SEC, however, have brought a limited amount of actions against entities where the foreign government owns less than a majority, but nonetheless held veto power over major expenditures and controlled important operational decisions, and where most senior company officers were political appointees.[50]

---

[40] *Id.*
[41] Guide at 17.
[42] *Id.* at 15.
[43] *Id.*
[44] 15 U.S.C. § 78dd-2(h)(2)(A).
[45] Guide at 20.
[46] *See, e.g.*, *United States v. Carson*, No. SACR 09-00077-JVS, 2011 WL 5101701 (C.D. Cal. May 18, 2011); *United States v. Aguilar*, 783 F. Supp. 2d 1108 (C.D. Cal. 2011).
[47] Guide at 20.
[48] *Id.* at 21.
[49] *Id.*
[50] *Id.*

3. Improper Purpose

As a general rule, the business nexus test determines whether the purpose of the payment is improper or not. To satisfy the business nexus test, an individual or entity must make a payment with the intent to induce a foreign official to act in consideration of a payment for the purpose of obtaining or retaining business, or for directing business to another person.[51] The government interprets this provision liberally and, due to infrequent litigation, its interpretation is rarely challenged. One of the most extensively litigated FCPA cases is *United States v. David Kay and Douglas Murphy*.[52] The case was heard twice by the Fifth Circuit Court of Appeals which expansively interpreted the business nexus element of the FCPA. The Fifth Circuit held that corrupt payments designed to obtain a tax benefit can satisfy the business nexus element of the FCPA.[53] The government also must establish a link between the reduced taxes and obtaining or retaining business to satisfy the business nexus test.[54]

Significantly, the business obtained does not necessarily have to be with the government. If the bribe is paid to a government agency or official, or in some instances a state-owned company or one of its employees, it can still result in FCPA liability if it facilitates the company's ability to do business with a private entity.[55]

B. Exceptions/Affirmative Defenses to FCPA Bribery Prohibition

The FCPA's bribery prohibition excludes facilitating payments, which are payments made "to secure the performance of a routine governmental action."[56] The line between facilitating payments and bribes is a fine one that requires the analysis of the facts and circumstances. Typically, however, the FCPA allows facilitating payments if the local law entitles the company to the end outcome achieved by making the payment.[57] The Guide offers examples of permissible facilitating payments, such as payments for processing visas, providing police protection or mail service, and supplying utilities like phone service, power, and water.[58] The Guide cautions, however, that routine government action does not include a decision to award new business or to continue business with a particular party, nor does it include acts that are within a foreign official's discretion or that would constitute misuse of an official's office.[59] Thus, while paying a government official a small amount to have the power turned on in a factory at night might be considered a facilitating payment, paying an inspector to ignore the fact that the company does not have a valid permit to operate the factory would not. In determining what constitutes a facilitating payment, the size of the payment is telling, but the purpose of the payment is dispositive.[60]

Many companies are now flatly prohibiting the use of facilitating payments because of the uncertainty in what could be safely considered a facilitating payment or are at least requiring pre-approval from the company's legal department. The guidance provided by the DOJ and SEC in this area is likely to be of little comfort to companies as the Guide is clear that even a permissible facilitating payment under the FCPA can create liability for a company if it violates "local law in the countries where the company is operating" or if "other countries' foreign bribery laws, such as the United Kingdom's, does not contain an exception for facilitating payments."[61]

---

[51] 15 U.S.C. § 78dd-1(a)(1); *see also United States v. Kay*, 359 F.3d 738, 740 (5th Cir. 2004) (referring to the "business nexus element" of an FCPA violation).
[52] 200 F. Supp. 2d 681 (S.D. Tex. 2002).
[53] *Kay*, 359 F.3d at 761.
[54] *Id.*
[55] Guide at 21.
[56] 15 U.S.C. §§ 78dd-1(b), 78dd-2(b).
[57] Guide at 25.
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.* Brazil's newly-enacted Anti-Bribery Act (Law 12.846), which becomes effective on January 28, 2014, also does not include an exception for facilitating payments, a common practice in many countries in Latin America and around the world.

In addition, the FCPA provides an affirmative defense if the payment was lawful in the foreign official's country or constituted a reasonable expenditure made on behalf of or by the foreign party for the promotion of services or execution of contracts already in place.[62] Examples of these types of payments are traveling and lodging expenses.

C. Books and Records and Internal Controls

In addition to the anti-bribery prohibitions of the FCPA, the act also requires domestic issuers to "make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer."[63] This provision, under which the bulk of FCPA actions are brought, requires that the company's records be compiled in accordance with accepted accounting standards. "Off-the-books" transactions are strictly prohibited.

The act also requires public companies listed on United States exchanges to maintain a system of internal accounting controls.[64] The internal controls must provide reasonable assurance that the company has executed transactions according to management authorization, recorded transactions as necessary to permit preparation of financial statements, and regularly compared recorded assets to actual assets and taken appropriate action to reconcile and/or address differences.[65]

D. Jurisdictional Reach of the FCPA

The FCPA's anti-bribery prohibitions apply to any issuers of American securities, "domestic concerns," and foreign entities with sufficient ties to the United States.[66] Issuers include the officers, directors and agents of the issuer and encompass not only companies incorporated in the United States, but also foreign corporations that list shares on American stock exchanges, particularly through American Depository Receipts.[67]

A domestic concern is defined as: "(A) any individual who is a citizen, national, or resident of the United States; or (B) any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship which has its principal place of business in the United States, or which is organized under the laws of a State of the United States."[68] Foreign corporations and individuals will be considered domestic concerns if they make use of the mails or other instrumentalities of interstate commerce or do any acts within the territory of the United States in furtherance of a violation of the FCPA.[69]

E. Particular Issues Concerning Mergers and Acquisitions

When a company merges with or acquires shares in another company, it typically assumes the liabilities of the target company.[70] Structuring the transaction as an asset purchase will not usually eliminate the risk of successor liability. Courts frequently look past the structure of the transaction and will impose successor liability if the acquiring company agreed to assume liability, was aware of the potential

---

[62] Guide at 93.
[63] 15 U.S.C. § 78m(b)(2)(A).
[64] 15 U.S.C. § 78m(b)(2)(B).
[65] *Id.*
[66] Guide at 10-12.
[67] *Id. at 11; see also* Press Release, DOJ, *U.S. Resolves Probe Against Oil Company that Bribed Iranian Official* (Oct. 13, 2006), *available at* http://www.usdoj.gov/usao/nys/pressreleases/October06/statoildeferredprosecutionagreementpr.pdf.
[68] 15 U.S.C. § 78dd-2(h)(1).
[69] Shearman & Sterling LLP, *FCPA Digest of Cases and Review Releases Relating to Bribes to Foreign Officials Under the Foreign Corrupt Practices Act of 1977* (Oct. 1, 2009), *available at* http://www.shearman.com/files/upload/fcpa_digest.pdf.
[70] *See United States v. Alamo Bank of Texas*, 880 F.2d 828, 830 (5th Cir. 1989) (holding that a successor bank could be held responsible for the predecessor bank's pre-merger violations of the U.S. Bank Secrecy Act).

liability, or if the transaction was merely a means of avoiding liability.[71] Thus, FCPA violations of the target company may become FCPA violations of the acquiring company.

F. Criminal and Civil Penalties and Collateral Consequences

The DOJ handles all criminal enforcement of the FCPA. The DOJ is also responsible for civil enforcement, except with respect to companies that issue registered securities or are required to file disclosure reports with the SEC. The SEC is responsible for civil FCPA enforcement against such companies.

Individuals who violate the anti-bribery provisions of the FCPA may face civil penalties of up to $16,000 per violation and, for willful violations, criminal fines of up to $100,000 and/or imprisonment of up to five years.[72] Under the Alternative Fines Act, the fine may be increased to twice the gross financial gain or loss resulting from the corrupt payment.[73] For violations of the FCPA's accounting provisions, individuals may face civil penalties of up to $150,000 and, for willful violations, criminal fines of up to $5 million or twice the gain or loss caused by the violation, and/or imprisonment for up to 20 years.[74] Criminal and civil fines imposed on individuals may not be paid directly or indirectly by the companies on whose behalf the individuals acted.[75]

Entities that violate the FCPA's anti-bribery provisions may face civil penalties of up to $16,000 per violation, and, for willful conduct, criminal fines of up to $2 million.[76] The Alternative Fines Act may increase the criminal fine to twice the gain or loss resulting from the corrupt payment.[77] Entities that violate the FCPA's accounting provisions may face civil penalties of up to $725,000, and, for willful conduct, criminal fines of up to $25 million or twice the gain or loss caused by the violation.[78] In addition to criminal and civil sanctions, individuals and entities that violate the FCPA may be subject to collateral consequences, including suspension or debarment from contracting with the federal government, cross-debarment by multilateral development banks, the suspension or revocation of certain export privileges, and "copycat" actions brought by the government of the country where the corrupt payment was made.

The overwhelming majority of FCPA enforcement actions end in plea agreements, deferred or non-prosecution agreements, or civil settlements, often including acceptance of substantial fines and other punitive measures. *United States v. Siemens Aktiengesellschaft*, 08-CR-367-RJL (D.D.C 2008), resulted in the largest combined penalty ever paid in an FCPA case – a $450 million criminal fine and $350 million disgorgement of profits – after the company pleaded guilty to several counts in connection with bribes paid by four of its subsidiaries in numerous countries and settled a civil enforcement action with the SEC.[79] The company was also prosecuted in Germany and as a result of the combined actions of the DOJ, SEC and German prosecutors, Siemens paid a total $1.6 billion in fines, penalties and disgorged profits. In *United States v. Johnson & Johnson*, 11-CR-099 (D.D.C 2011), the company entered a deferred prosecution agreement, agreed to pay $21.4 million in criminal penalties, and disgorged $48.6 million in profits to the SEC, in order to resolve improper payments made by subsidiaries to government officials in several European countries.[80]

---

[71] *See, e.g.*, Carolyn Lindsey, *More Than You Bargained For: Successor Liability Under the U.S. Foreign Corrupt Practices Act*, 35 Ohio N.U. L. Rev. 959, 966 (2009).
[72] 15 U.S.C. §§ 78dd-2(g)(1)(B), 78dd-3(e)(1)(B), 78ff(c)(1)(B); *see also* 17 C.F.R. § 201.1004 (providing adjustments for inflation).
[73] 18 U.S.C. § 3571(d).
[74] 15 U.S.C. §§ 78u(d)(3), 78ff(a); *see also* 17 C.F.R. § 201.1004 (providing adjustments for inflation).
[75] 15 U.S.C. § 78ff(c)(3).
[76] 15 U.S.C. §§ 78dd-2(g)(1), 78dd-3(e), 78ff(c); *see also* 17 C.F.R. § 201.1004 (providing adjustments for inflation).
[77] 18 U.S.C. § 3571(d).
[78] 15 U.S.C. §§ 78ff(a), 78u(d)(3); *see also* 17 C.F.R. § 201.1004 (providing adjustments for inflation).
[79] *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.
[80] *See* Press Release, DOJ, *Johnson & Johnson Agrees to Pay $21.4 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act and Oil for Food Investigations* (Apr. 8, 2011), *available at* http://www.justice.gov/opa/pr/2011/April/11-crm-446.html; *see also*

Notably, recent FCPA enforcement proceedings reveal that the United States will not hesitate to exert jurisdiction over foreigners. For example, in December 2011, a group of former non-United States resident Siemens AG executives were indicted for FCPA violations.[81] Further, of the 10 largest FCPA fines, nine have been paid by foreign companies.[82]

G. WHAT COMPANIES SHOULD DO

Both domestic and foreign companies should be aware that the conduct of their employees could subject them to severe criminal and civil penalties under the FCPA. The United States government has been especially active in FCPA cases and is not afraid to extend its enforcement reach to foreign jurisdictions and companies. Accordingly, all domestic and foreign companies with ties to the United States should have a rigorous system of internal compliance and accounting measures in place, so that in the event that a FCPA action is brought against them, they can challenge the higher fines and penalties that come from the FCPA. In addition, companies should be prepared to quickly investigate potential FCPA violations and take corrective measures should any violations be discovered.

1. Establishing and Maintaining a Strong FCPA Compliance Program

Any serious effort by a company to limit its FCPA exposure starts with a strong FCPA compliance program and more specifically, with a comprehensive, written FCPA compliance policy at its foundation. The policy should explain the purpose of the FCPA and summarize the act's salient provisions. The policy should emphasize that all employees are responsible for ensuring the company stays in compliance with the FCPA and provide a clear reporting mechanism for employees who have questions about the policy or wish to report potential FCPA violations. The policy should be distributed to all employees, and the company should conduct regular training sessions. Employees of all levels should be required to certify compliance with the FCPA. Additionally, the company should conduct regular, internal audits of its FCPA compliance program.

If a company discovers a possible FCPA violation, it should commission an internal investigation conducted by experienced FCPA outside counsel, terminate employees or agents who committed the violation, and consider reporting the violation to the DOJ and SEC. The government looks favorably on companies that maintain strong FCPA compliance programs and take swift and determinative corrective action upon discovering FCPA violations. This is illustrated by one action where the employee was penalized for FCPA violations, but not his company. On April 25, 2012, Garth R. Peterson, a former Morgan Stanley executive, pleaded guilty to criminal and civil charges for secretly funneling millions of dollars in bribes to a Chinese official, who then helped the company acquire business. In not also charging Morgan Stanley under the FCPA, the DOJ and SEC pointed to, among other things, the company's internal controls, which provided reasonable assurances that its employees were not bribing government officials, Peterson's repeated certifications that he was complying with the FCPA, and the company's voluntary disclosure of the matter and subsequent cooperation with the government.[83] In comparison, the *Siemens* case described above warns companies of the opposite result. There, the SEC

United States v. Titan Corp., 05-CR-314-BEN (S.D. Cal. 2005) (company pleaded guilty, sentenced to pay a combined criminal and civil fine of $28 million dollars, and ordered to serve three years of supervised probation for paying bribes to an individual in Benin who then funneled that money into the President of Benin's reelection campaign); *United States v. ABB Vetco, Inc.*, 04-CR-279 (S.D. Texas 2004) (United States and United Kingdom subsidiaries of a Swiss company pleaded guilty to violating the FCPA after paying bribes directly and indirectly to Nigerian officials responsible for overseeing oil extraction and awarding contracts for oil exploration projects: each subsidiary agreed to pay a fine of $5.25 million, and in a separate action the parent company agreed to pay a $10.5 million civil fine in addition to $5.9 million in restitution and interest).

[81] Kirsten Mayer et al., *Facing FCPA Charges in Foreign Countries*, LAW 360 (Jan. 3, 2012), *available at* http://www.law360.com/articles/295556/facing-fcpa-charges-in-foreign-countries.

[82] *Id.*

[83] 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.

specifically alleged that the company's inadequate internal controls and anti-FCPA corporate culture allowed the corrupt conduct of bribing government officials to flourish.[84]

2. Due Diligence in Mergers and Acquisitions

As discussed above, companies that merge with or acquire other companies with past FCPA violations may assume responsibility for those violations. However, certain measures can be taken to lessen the risk of assuming FCPA liability in mergers and acquisitions, including:

- Learning about the jurisdiction of the target company, and the types of prevalent business practices in such jurisdiction that might run afoul of the FCPA;
- Incorporating strong FCPA-related representations and warranties in the merger or acquisition contract, including requiring the target company to represent and warrant that none of its employees have engaged in conduct which might violate the FCPA;
- Terminating any employees who participated in FCPA violations before the merger or acquisition; and
- Immediately imposing a rigorous FCPA compliance program on the merged or acquired company.

Similar to the steps a company can take to lessen its FCPA exposure in the normal course, proper due diligence on the target company and prompt corrective measures if a FCPA violation is subsequently discovered may result in the DOJ or SEC looking favorably on the company should the target company's past FCPA violation become the subject of criminal or civil proceedings. In fact, the Guide provides some comfort for companies that did their homework: the "DOJ and SEC have declined to take action against companies that voluntarily disclosed and remediated conduct and cooperated with DOJ and SEC in the merger and acquisition context."[85] Enforcement actions against successor entities are likely to be limited to "cases involving egregious and sustained violations or where the successor company directly participated in the violations or failed to stop the misconduct from continuing after the acquisition."[86] Finally, even when thorough pre-acquisition due diligence is not feasible, the Guide states that the DOJ and SEC will still consider mitigating factors such as self-disclosure, "adequate" due diligence, and a robust compliance program.[87]

[84] Press Release, SEC, *SEC Charges Siemens AG for Engaging in Worldwide Bribery* (Dec. 15, 2008), *available at* http://www.sec.gov/news/press/2008/2008-294.htm.
[85] Guide at 28.
[86] *Id.*
[87] *Id.* at 62.