THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 57 No. 16 September 25, 2024

SUSPECT CORRUPT PAYMENTS? HOW TO NAVIGATE A POTENTIAL CORPORATE CRISIS

In this article, the authors discuss the global surge in anti-corruption efforts, including how U.S. and foreign authorities are increasingly working together to combat and penalize those who engage in corrupt activities. Given the significant penalties for entities that violate anti-corruption laws, the authors discuss key steps companies should take when faced with corruption allegations and offer some considerations for response strategies.

By Laura Perkins, Michael DeBernardis, and Katherine Taylor *

Being embroiled in a corruption scandal can have significant consequences for a company. Not only can it result in reputational harm, but it can lead to lengthy investigations, hefty fines (with recent examples nearing $4 billion), costly litigation, and a resulting drop in stock prices. It is essential for companies to understand how to proactively and appropriately respond to corruption allegations when they come to light. Having a strong crisis response can mitigate corporate harm and liability.

UPTICK IN GLOBAL ANTI-CORRUPTION ENFORCEMENT

Enacted in 1977, the Foreign Corrupt Practices Act ("FCPA") was the first law of its kind. The FCPA prohibits (1) the payment of bribes to foreign officials in exchange for business advantages and (2) the use of fraudulent accounting practices to cover up those payments. The FCPA applies to U.S. companies, U.S. citizens, nationals or residents, and companies that are publicly traded on U.S. exchanges or are required to report to the U.S. Securities and Exchange Commission, as well as their personnel.[1,2] It also applies to foreign companies and foreign nationals who commit violations while in the United States.[3] Violators of the FCPA face numerous repercussions, including hefty criminal fines,[4] imprisonment,[5] and civil penalties.[6]

[1] This includes their officers, directors, employees, agents, and stockholders.

[2] 15 U.S.C.§§ 78dd-1(a), 78dd-2(a).

[3] 15 U.S.C.§§ 78dd-1(g), 78dd-2(i), 78dd 3(a).

[4] Companies and individuals who willfully violate the anti-bribery provisions of the FCPA face criminal fines of up to $2 million and $250,000 per violation, respectively, or an alternative fine of twice the pecuniary gain. 15 U.S.C.§§ 78ff(c), 78dd-2(g), 78dd-3(e); 18 U.S.C.§ 3571(b)(3), (d), (e). Organizations and individuals found to have willfully violated the internal accounting control provisions of the FCPA face maximum criminal fines of $25 million and $5 million, respectively, or, if greater, the alternative fine of twice the pecuniary gain. 15 U.S.C.§ 78ff(a); 18 U.S.C.§ 3571(d), (e).

[5] Individuals found to have willfully violated the anti-bribery provisions of the FCPA face up to five years of imprisonment. 15 U.S.C.§§ 78ff(c)(2)(A), 78dd- 2(g)(2)(A), 78dd-3(e)(2)(A). Individuals who willfully violate the internal accounting control provisions of the FCPA face up to 20 years of imprisonment. 15 U.S.C.§ 78ff(a).

* *LAURA PERKINS and MICHAEL DEBERNARDIS are partners and KATHERINE TAYLOR is an associate at Hughes Hubbard & Reed LLP's Washington, DC office. Their email addresses are laura.perkins@hugheshubbard.com, michael.debernardis@hugheshubbard.com, and katherine.taylor@hugheshubbard.com.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb.

The U.S. government began ramping up its efforts to enforce the FCPA in the early 2000s. The "modern era" of FCPA enforcement is often considered to have started with the 2008 FCPA-related corporate charges against Siemens AG, a German conglomerate with operations in telecommunications, power generation, transportation, and medical and industrial equipment.[7] With a criminal fine of nearly $450 million (and a total global penalty of almost $1 billion), the Siemens resolution served as a high-profile warning regarding the significant consequences of an FCPA violation.[8]

In recent years, the risks associated with a corruption violation have only increased. The DOJ and SEC, the two primary agencies in the United States charged with enforcing the FCPA, have dedicated teams and sophisticated tools to target foreign corruption. The DOJ and SEC are also receiving more help than ever from a variety of other U.S. government agencies and divisions in connection with FCPA investigations, with recent examples including the IRS, Department of Homeland Security, U.S. Postal Inspection Service, the Federal Reserve Bank of New York, the Department of Energy Office of Inspector General, and the Commodity Futures Trading Commission.

In the same vein, enforcement agencies from around the world are also increasingly cooperating with the U.S. government to investigate and prosecute complex cross-border corruption cases. The DOJ and SEC rely upon and provide assistance to a growing number of non-U.S. enforcement agencies in complex bribery investigations. For instance, in 2022 the DOJ entered into its first coordinated resolution with South African authorities,[9] and in 2023 the DOJ coordinated its first-ever resolution with Colombia.[10] In recent years, the DOJ has credited authorities from the following countries, among others, for assistance in its FCPA prosecutions: Armenia, Australia, Brazil, Belize, British Virgin Islands, Canada, Colombia, Cyprus, Germany, Hong Kong, India, Indonesia, Latvia, Luxembourg, Mexico, the Netherlands, South Africa, Switzerland, Turkey, the United Arab Emirates, and the United Kingdom.[11]

As a result, authorities are now able to tackle increasingly complex corruption investigations that result in coordinated resolutions with penalties reaching into the billions of dollars. Where Siemens was once an outlier, recent years have seen multiple resolutions matching or surpassing Siemens both in the scope of the corrupt activity discovered and the scale of the penalty.

[6] Violations of the anti-bribery provisions can also result in civil penalties of up to $16,000 per violation, which may not be paid by the person's employer or principal. 15 U.S.C.§§ 78ff(c), 78dd-2(g), 78dd-3(e); *see also* DOJ & SEC, A Resource Guide To The Foreign Corrupt Practices Act (2012) (indicating that the maximum civil penalty for an anti-bribery provision violation is $16,000, but citing the SEC's announcement of the adjustment for issuers subject to SEC enforcement without citing a parallel DOJ announcement for domestic concerns and other persons). In addition, civil penalties for violations of the internal accounting control provisions can include disgorgement of any ill-gotten gains, or a civil penalty that updates annually based inflation. 15 U.S.C.§ 78u(d)(3), (5); *see also* 17 C.F.R. § 201.1001.

[7] Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to Pay $450 Million in Combined Criminal Fines: Coordinated Enforcement Actions by DOJ, SEC and German Authorities Result in Penalties of $1.6 Billion, U.S. Department of Justice (Dec. 15, 2008), https://www.justice.gov/archive/opa/ pr/2008/December/08-crm-1105.html.

[8] *Id.*

[9] ABB Agrees to Pay Over $315 Million to Resolve Coordinated Global Foreign Bribery Case, Office of Public Affairs, U.S. Department of Justice (Dec. 2, 2022), https://www.justice.gov/opa/pr/abb-agrees-pay-over-315-million-resolve-coordinated-global-foreign-bribery-case.

[10] Corficolombiana to Pay $80M to Resolve Foreign Bribery Investigations, Office of Public Affairs, U.S. Department of Justice (Aug. 10, 2023), https://www.justice.gov/opa/pr/corficolombiana-pay-80m-resolve-foreign-bribery-investigations.

[11] FCPA & Anti-Bribery Fall 2023 Alert, Hughes Hubbard & Reed LLP, at 8, https://www.hugheshubbard.com/news/hughes-hubbard-releases-fall-2023-fcpa-alert.

- VimpelCom – In 2016, VimpelCom Limited, an Amsterdam-based telecommunications company, and its wholly owned Uzbek subsidiary, Unitel LLC, agreed to pay $795 million to resolve charges from the DOJ, the SEC, and the Public Prosecution Service of the Netherlands.[12]

- Odebrecht – In 2016, Odebrecht S.A., a Brazilian construction conglomerate, and Braskem S.A., a company controlled and partially owned by Odebrecht, agreed to pay more than $3.5 billion to the DOJ, SEC, and authorities in Brazil and Switzerland.[13]

- Telia – In 2017, Telia Company AB, a Stockholm-based telecommunications company, and its Uzbek subsidiary, Coscom LLC, reached a coordinated resolution with the DOJ, SEC, and authorities in the Netherlands, resulting in a total financial penalty of $965 million.[14]

- Petrobras – In 2018, Brazil's state-owned oil company Petróleo Brasileiro S.A. reached a resolution with the DOJ, SEC, and Brazilian MPF resulting in a total financial penalty of more than $850 million.[15]

- Airbus – In 2020, Airbus SE, the global civilian and military aircraft manufacturer, agreed to pay more than $3.9 million in penalties to resolve foreign bribery charges with the DOJ and authorities in France and the United Kingdom.[16]

- Goldman Sachs – In 2020, Goldman Sachs Group, Inc., the global financial institution headquartered in New York, and its Malaysian subsidiary, Goldman Sachs (Malaysia) Sdn. Bhd., agreed to pay more than $2.9 billion in a coordinated resolution with the DOJ, SEC, and authorities in the United Kingdom, Singapore, Malaysia and elsewhere.[17]

Given these high risks, companies facing corruption allegations must be prepared to respond swiftly and effectively.

HOW TO RESPOND TO A CORRUPTION CRISIS

How a company responds when confronted with significant corruption allegations can have a major impact on the repercussions it may ultimately face. We outline below some key steps and considerations for companies confronting allegations of corruption.

Select the Response Team

Upon learning of corruption allegations, a company should quickly assemble a team with the requisite qualifications, experience, and authority to assess and investigate (if appropriate)[18] the allegations and to identify and address any risks, whether legal, reputational, business, or safety-related, that may arise. Some companies find it helpful to proactively establish crisis response teams even before an issue arises, so they are prepared to respond immediately to issues as they

[12] VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than $795 Million; United States Seeks $850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme, Office of Public Affairs, U.S. Department of Justice (Feb. 18, 2016), https://www.justice.gov/opa/pr/vimpelcom-limited-and-unitel-llc-enter-global-foreign-bribery-resolution-more-795-million.

[13] Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History, Office of Public Affairs, U.S. Department of Justice (Dec. 21, 2016), https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve.

[14] Telia Company AB and Its Uzbek Subsidiary Enter Into a Global Foreign Bribery Resolution of More Than $965 Million for Corrupt Payments in Uzbekistan, Office of Public Affairs, U.S. Department of Justice, (Sept. 21, 2017), https://www.justice.gov/opa/pr/telia-company-ab-and-its-uzbek-subsidiary-enter-global-foreign-bribery-resolution-more-965.

[15] Petróleo Brasileiro S.A. – Petrobras Agrees to Pay More Than $850 Million for FCPA Violations, Office of Public Affairs, U.S. Department of Justice (Sept. 27, 2018), https://www.justice.gov/opa/pr/petr-leo-brasileiro-sa-petrobras-agrees-pay-more-850-million-fcpa-violations.

[16] Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case, Office of Public Affairs, U.S. Department of Justice (Jan. 31, 2020), https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case.

[17] Goldman Sachs Charged in Foreign Bribery Case and Agrees to Pay Over $2.9 Billion, Office of Public Affairs, U.S. Department of Justice (Oct. 22, 2020), https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion.

[18] Not all allegations warrant a full-blown crisis response. While having a crisis response team on standby to handle any and all allegations of misconduct can be useful, where misconduct is, on its face, baseless, a company may not need to conduct a full investigation and should adjust its response accordingly.

occur. Whether created in advance of or upon the emergence of an issue, companies should consider including individuals from the legal, compliance, and human resources departments, relevant senior executives or department heads (particularly executives in the division implicated in the misconduct), and other key operational staff (after ensuring that none are involved in or tainted by the allegations) in their crisis response teams.

Executives from the company's communications department or Investor Relations team should also be included in the crisis response team, or, if not on the team, quickly alerted to any aspects of the allegations or investigations that may result in negative media, stakeholder or investor attention, and added to the discussion of how to manage those issues. Allegations of misconduct can cause unease that affects a company's share price. Having a clear and consistent message around allegations of misconduct and any resulting investigations or litigation can alleviate some of this unease. Communications and Investor Relations teams can help a company determine when and how to publicly disclose the misconduct through press releases, earnings calls, public filings, and other communications to shareholders. Aligning with these teams can ensure that the public messaging is consistent with the company's legal response and does not draw the ire of regulators.

Companies should also bear in mind that corruption allegations, particularly FCPA allegations, often involve multiple jurisdictions and legal regimes. These added complexities may require the inclusion of employees from different subsidiaries or branch offices.

Typically, the response team should also include outside counsel. Internal counsel or investigators often have a good understanding of the company's structure, operations, and policies, and may have the trust of the employees involved in the allegations. However, engaging external counsel with sufficient experience and credentials early on will ensure that the response benefits from a thorough understanding of the potential risks and legal issues implicated by the misconduct. Further, external counsel will ensure that the company is able to handle the resource intensive nature of the resulting investigation, especially on the increasingly aggressive timelines U.S. regulators are expecting from companies. Finally, external counsel are more likely to have specialized knowledge of the legal issues surrounding corruption allegations and the best methods for investigating complex, multijurisdictional issues. This expertise, combined with external counsel's independence from the company, can add credibility to a crisis response.

While likely not part of the crisis response team, the team should consider at the early stages when and how it will involve or alert the company's board of directors to the issue. The team should also consider whether the issue should be raised to the entire board or to a subcommittee of the board, like the audit committee. Keeping the board properly apprised can be beneficial at significant decision points (e.g., whether to self-report potential violations to authorities) and at the conclusion of the investigation, particularly if the investigation results in an action requiring board approval.

Fact and Information Gathering

Once a response team is established, the next step is to collect facts and information about the alleged misconduct. This includes properly scoping any ensuing investigation.[19] It is important that the scope of the investigation be appropriately tailored to the alleged misconduct — an unduly narrow scope can look superficial and may not uncover ongoing misconduct, while an overbroad scope can waste corporate resources and take a needlessly long amount of time.

To properly scope an investigation, investigators should assess the allegations and, at least initially, tie the scope of the investigation to the allegations. As the investigation progresses, if facts develop that suggest the misconduct may be broader than the initial allegations, investigators should adjust the scope accordingly. Conversely, if the facts suggest the misconduct is more limited, investigators should consider narrowing the scope to better target the investigation. This flexibility ensures that resources are utilized appropriately and that potential problems are not neglected or missed.

If the misconduct spans several countries, it is important to understand any potentially restrictive or conflicting laws that may affect the ability to collect information. For example, countries have different data privacy and protection provisions that govern what types of information or data can be gathered and shared with others.[20] In addition, local labor and employment laws may impact a company's ability to gather information from employees in certain countries or to discipline

[19] Evaluation of Corporate Compliance Programs (Updated March 2023), U.S. Department of Justice Criminal Division, at 16, https://www.justice.gov/opa/speech/file/1571911/dl.

[20] For example, the EU's General Data Protection Regulation ("GDPR") governs how individuals' personal data can be transferred. E.U Reg. 2016/69 (Apr. 27, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679.

those employees during, or as a result of, the investigation. Thus, companies should understand how those laws may affect their investigation.

Finally, companies must ensure that their crisis response team has the resources it needs to properly investigate the allegations of misconduct. For corruption investigations, those resources may include specialized internal or external forensic accountants to carefully review financial transactions, internal or external IT resources needed to preserve, collect, and process potentially significant amounts of electronic data in a forensically sound manner,[21] and resources required to answer legal questions in various relevant jurisdictions (e.g., "Are there any laws preventing us from collecting employee cell phones in country X?").

Assessing Other Potential Implications

Beyond assessing the potential direct consequences of an FCPA violation (i.e., type of resolution, monetary penalty), the cross-disciplinary crisis response team must consider potential collateral consequences or requirements as well. As FCPA enforcement has increased and a greater emphasis has been placed on FCPA-compliance across industries, FCPA-related covenants are regularly included in various contracts and other agreements. For example, corruption-related warranties and representations in loan documents are now commonplace. The crisis response team will need to consider whether findings of corrupt activity by the company could potentially be considered an event of default in those agreements. Other types of business agreements, such as joint venture agreements, may include an obligation to disclose the investigation, even before finalizing the findings. Companies involved in government contracting should consider the potential impact a guilty plea or deferred prosecution might have on future eligibility for government contracts or whether such contracts require disclosure of the investigation and, if so, at what stage of the investigation. Publicly traded companies must consider whether and when to disclose the investigation in their SEC filings. Companies in regulated industries may be under obligations to disclose misconduct such as corruption to specific regulators. Companies should also consider whether their insurance policies provide coverage for affected individuals or even certain company costs and whether notice requirements exist for such coverage.

Considerations Regarding Reporting to Authorities

Enforcement authorities are increasingly seeking to incentivize companies to voluntarily self-disclose potential violations. In the U.S., the DOJ offers a number of benefits to companies that self-report, cooperate, and remediate the misconduct, including the potential for a declination (i.e., that the DOJ will decline to prosecute even if a violation occurred) or a more favorable resolution and a decrease in the otherwise applicable fine.[22] In addition to the potential benefits explicitly offered by the DOJ, self-reporting can also allow a company to better control the narrative around the misconduct and potentially even the scope of the government's investigation. However, if the government is not already aware of the potential misconduct, a self-report may result in a government investigation and resolution (and potentially follow-on shareholder litigation and reputational harm) that would otherwise never have materialized. Thus, the decision to self-report is one that needs to be carefully considered.

---

[21] Evaluation of Corporate Compliance Programs (Updated March 2023), U.S. Department of Justice Criminal Division, at 17, https://www.justice.gov/opa/speech/file/1571911/dl ("Policies governing such applications should be tailored to the company's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company.").

[22] The DOJ Criminal Division's Corporate Enforcement and Voluntary Self-Disclosure Policy provides for: (1) the possibility of declinations even where aggravating factors are present; (2) greater available maximum fine reductions where a company voluntarily discloses and appropriately remediates misconduct when a criminal resolution is warranted; and (3) the availability to credit, up to a 50% reduction off the low end of the U.S. Sentencing Guidelines fine range, where a company fails to voluntarily self-disclose but provides "extraordinary cooperation" and appropriately remediates. 9-47.120 Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy, U.S. Department of Justice, (updated Mar. 2024), https://www.justice.gov/criminal/criminal-fraud/file/1562831/dl. Aggravating factors can include the involvement of senior executives in the misconduct, significant corporate profit from the misconduct, egregious or pervasive misconduct, and criminal recidivism. *Id.* Under the revised policy, companies who self-disclose, fully cooperate, and timely and appropriately remediate misconduct may receive a reduction of at least 50% and up to 75% from the low end of the U.S. Sentencing Guidelines fine range. *Id.* Finally, "extraordinary cooperation" means immediate cooperation which leads to evidence the Government could not otherwise obtain and that results in additional convictions or trial testimony; however, the credit for extraordinary cooperation is not available for criminal recidivists. *Id.*

When deciding whether to self-disclose potential misconduct, companies should consider a number of factors, including the following:

First, how likely is the misconduct to be discovered? Is the company's industry highly regulated? Is there a whistleblower involved? Is the conduct required or likely to be disclosed by an existing agreement or other business circumstances? Misconduct is more likely to be discovered in highly-regulated industries and the presence of a whistleblower greatly increases the likelihood that authorities will discover the misconduct whether or not the company self-reports it.

Second, how serious is the misconduct? Is it widespread? Does it involve employees across multiple levels of the company? How elaborate was the corruption scheme and how serious are the potential penalties? Where misconduct is serious and the potential penalties are high, a company faces a higher risk of prosecution, thus self-reporting the misconduct may be beneficial in obtaining a more favorable resolution. Conversely, widespread misconduct can be an aggravating factor in DOJ's analysis, thus decreasing some of the potential benefits of a self-report.

Third, what are the potential cooperation expectations? Each regulatory authority has different expectations regarding cooperation, and self-disclosure on its own rarely results in no prosecution. To take advantage of the benefits of voluntary disclosure policies, companies must also agree to cooperate with any resulting government investigation and engage in efforts to remediate the misconduct (this can include implementing internal controls, disciplining or terminating the employees involved, revising compliance policies, etc.).

Fourth, does the company have the right resources to support an investigation? To address any resulting litigation? Oftentimes, self-reporting misconduct leads to a government investigation which can rapidly consume corporate resources. Not only does responding to these investigations cost money, but it also takes up employee time, as employees are needed to track down and provide information. In addition, investigations can lead to costly litigation, which may require the hiring of external legal counsel.

Finally, what kind of reputational risk may result from self-disclosure? Self-reporting misconduct to a government agency increases the risk that the misconduct itself may become public and public disclosure of an external investigation into misconduct can negatively impact the company's reputation and its stock price. However, if there is a high likelihood that misconduct will be revealed, proactive self-disclosure may be a means by which to mitigate reputational harm.

CONCLUSION

Dealing with potentially significant allegations of corruption requires a multi-disciplinary response. While prevention is the best medicine, companies should be prepared to respond to the worst-case scenario. Companies should have a well-thought-out strategy to handle serious allegations of corruption, which includes having a process in place to understand the scope of the misconduct, identifying the key individuals to be involved in the crisis response, and obtaining and providing the resources necessary to properly investigate and remediate the misconduct and appropriately address any consequences. ■