The ANTI-CORRUPTION REPORT
Formerly the FCPA Report
An Acuris Company

www.anti-corruption.com Volume 7, Number 5 March 7, 2018

ANTI-CORRUPTION POLICY

The "Human" Side of FCPA Compliance: How to Best Work With HR in the Current Global Enforcement Environment

By Alex Oh Paul, Weiss, Kim Vinocour Paul, Weiss

Recent DOJ guidance on FCPA enforcement makes clear that coordination between the compliance department and the human resources department helps ensure the best outcome in the case of corruption-related misconduct. A cross-functional approach allows the company to receive maximum cooperation credit while satisfying local labor and data privacy law requirements and meeting employee expectations. Further, the HR department can play an important role in preventing anti-corruption violations in the first place.

This article explains the practical implications of the recent guidance, corporate enforcement policy, and enforcement actions for corporate compliance and HR departments, particularly with regard to hiring decisions and the investigation of, and disciplinary actions for, potential FCPA misconduct.

Preventing Hiring-Related Corruption

Hiring decisions have become a significant FCPA compliance issue in light of recent regulatory actions that focus on employment opportunities as a "thing of value" in the context of the FCPA.

Recent Enforcement Actions

In November 2016, JPMorgan Chase & Co and its Hong Kong subsidiary, JPMorgan Securities (Asia Pacific) Limited, agreed to pay $264.4 million to the DOJ, the SEC, and the Federal Reserve to settle FCPA charges for providing internships and other employment opportunities to relatives and friends of Chinese government officials in an effort to obtain mandates for transactions.

The government has recently prosecuted several other companies for similar conduct. In August 2015, Bank of NY Mellon paid almost $15 million to the SEC to settle charges that it violated the FCPA by offering employment opportunities to family members of officials associated with an unidentified Middle Eastern sovereign wealth fund. And, HSBC announced in February 2016 that the SEC is "investigating multiple financial institutions, including HSBC, in relation to hiring practices of candidates referred by or related to government officials or employees of state-owned enterprises in Asia-Pacific."

Effective Background Checks

Despite this recent enforcement trend, a 2017 benchmarking study[1] by HireRight, a provider of global background checks, found that only 13 percent of organizations screen backgrounds of employees based outside the U.S., and only 15 percent verify international backgrounds of U.S.-based employees.

Further, according to the same study, only 21 percent of employees are screened post-hire when they are promoted or retained. This is despite the fact that the U.S. Sentencing Guidelines have long suggested that companies conduct due diligence on certain employees as part of an effective compliance program.[2]

In terms of baseline hiring practices, a company's human resources department should coordinate with its anti-corruption compliance personnel to carefully consider what kind of background checks should be performed for each category of employees, and at what stages of the hiring and retention processes those checks need to be completed. Given the recent enforcement actions described above, background due diligence should not be limited to executive-level employees, but should be conducted more broadly depending on the risks relating to the hire, taking the risk profile of the location into account.

Evaluating Candidate Qualifications

Companies should also consider procedures that would ensure that candidates hired are suitably qualified for the position and have not been hired for improper reasons. Depending on the risk profile of the candidate, a company also may want to conduct an in-depth check of an individual's background and connections using a more specialized outside service. The company can also ask the candidates to provide more detailed information about their relatives and their employment.

Special Procedures for Family Members of Government Officials

The ANTI-CORRUPTION REPORT
Formerly the FCPA Report
An Acuris Company

www.anti-corruption.com Volume 7, Number 5 March 7, 2018

A company should also consider putting in place specific policies and procedures that govern the hiring of family members of government officials, as well as procedures that would ensure that such hires will be visible to compliance regardless of how the hiring occurs. In addition, companies should consider having a compliance officer involved in the review of an application before an offer of employment or promotion is made to a family member of a government official. Finally, a company must provide its human resources personnel with sufficient anti-corruption training to enable them to identify and elevate red flags as appropriate.

See "Hiring Practices and FCPA Compliance in the Wake of the BNY Settlement (Part One of Two)" (Jan. 13, 2016); Part Two (Jan. 27, 2016).

Addressing Corruption and Privacy Issues When Misconduct is Discovered

Another pivotal moment where human resources issues intersect with FCPA compliance issues is when potential misconduct is discovered.

DOJ Policies Affecting Internal Investigations

Both the DOJ Pilot Program announced in April 2016 and the new DOJ FCPA Corporate Enforcement Policy, which was announced in November 2017, are intended to encourage companies to make voluntary and timely disclosures of wrongdoing by clarifying the potential benefits for companies that self-report, fully cooperate in the investigation of, and remediate, any FCPA-related misconduct. Under the new policy, which applies only to DOJ criminal prosecutions, if a company voluntarily self-discloses misconduct, fully cooperates in an ensuing government investigation, and timely and appropriately remediates the misconduct, there will be a presumption of a declination unless certain aggravating circumstances are present. The new policy's emphasis on self-disclosure will change the calculus for companies as they conduct internal investigations and work with employees and regulators to resolve potential FCPA violations.

In the new FCPA Corporate Enforcement Policy, the DOJ defines "voluntary self-disclosure" as disclosure "prior to an imminent threat of disclosure or government investigation" that includes disclosure of "all relevant facts known to the company, including all relevant facts about individuals involved in the violations." A company seeking to avail itself of the self-disclosure credit now must conduct a prompt and thorough review of the misconduct at issue, including facts about individuals involved in the misconduct. This may require a company to make a variety of quick decisions about individuals involved in the misconduct, balancing U.S. regulators' expectations and other applicable laws.

See The Anti-Corruption Report's three-part series on the DOJ's FCPA Corporate Enforcement Policy: "What's New and What's Not" (Jan. 10, 2018); "How Important Is the Presumption of Declination?" (Jan. 24, 2018); and "Cooperation and Compliance Expectations" (Feb. 7, 2018).

Addressing Data Privacy Concerns When Investigating and Cooperating

One thorny issue that comes up repeatedly in this context is how to handle the various data privacy laws for multinational companies that have operations throughout the world. More than 100 countries around the world have some kind of data protection regime in place. While they all have different parameters, many such laws: require that employees are informed in advance about what kind of personal data their employers can access; how such data will be used and to whom it can be disclosed; place limits on sharing the data with third parties; and require that individuals be given meaningful choice about whether their personal data is collected.

In Germany, for example, the Federal Data Protection Act, or the Bundesdatenschutzgesetz (BDSG), requires specific justification for any handling of personal data. The BDSG prohibits the collection, processing, and use of "personal data," unless the affected individual consents to, or German law specifically authorizes, the activity. The BDSG defines personal data as "individual pieces of information about personal or factual circumstances about an identified or identifiable human being."

In China, the law on Guarding State Secrets restricts the export of electronic data outside the country and requires the review and clearance of sensitive information in advance (which can mean almost anything, given how broadly the law is drafted).

Given that the information that the DOJ expects to receive as part of cooperation often resides on servers in countries outside the U.S., a company's ability to maximize cooperation credit can be hampered by the data privacy laws or employment laws of other jurisdictions. The DOJ can be surprisingly unsympathetic to such dilemmas. When it launched the Pilot Program in April 2016, the DOJ warned companies that the burden would be on the company to explain why any data privacy law restrictions prevent its compliance with the DOJ's requests for information, and that

The ANTI-CORRUPTION REPORT
Formerly the FCPA Report
An Acuris Company

www.anti-corruption.com Volume 7, Number 5 March 7, 2018

the DOJ will "closely evaluate the validity of that claim."

Global companies therefore should work with human resources and local data privacy counsel to formulate a strategy in advance that appropriately balances data privacy concerns of employees with the companies' ability to obtain maximum cooperation credit under the DOJ's guidance should any misconduct be discovered.

See The Anti-Corruption Report's two-part series on China's State Secrets Law: "A Primer for Anti-Corruption Practitioners" (Jun. 29, 2016); and "Six Things to Consider When Engaging in Internal Investigations in China" (Jul. 13, 2016).

Avoiding Restrictions on an Employee's Ability to Report Misconduct

It is essential that companies do not enter into any agreements with employees that even remotely suggest an effort to silence the employees or restrict their ability to speak up about what they consider to be wrongdoing. For example, in a 2015 settlement between KBR and the SEC, which was the Commission's first action against a company for "using improperly restrictive language in confidentiality agreements," the Commission criticized KBR for using confidentiality agreements that could have impeded an employee from communicating violations of law to governmental agencies in breach of securities laws.

The principle also applies to severance agreements, and the SEC has entered into several settlements since then based in part on the use of restrictive language in severance agreements. In one, with BlueLinx Holdings in 2016, the SEC criticized language in termination agreements that forced employees "to choose between identifying themselves to the company as whistleblowers or potentially losing their severance pay and benefits," which, in the Commission's view, removed the "important financial incentives" given by the government to encourage communication about possible violations of law. As part of its remediation, BlueLinx agreed to amend its separation agreements and contact former employees and inform them of BlueLinx's revised policy on communications with the government.

See "Promoting Values to Encourage Reporting and Discourage Retaliation" (Feb. 21, 2018).

Taking FCPA-Compliant Disciplinary Actions

Another human resources issue faced by companies that discover FCPA misconduct is what disciplinary action to take against wrongdoers consistent with any local law restrictions.

The DOJ's February 2017 Evaluation of Corporate Compliance Programs, which clarified the type of questions that the Department will ask when evaluating corporate compliance programs, indicates that the DOJ specifically will assess a company's compliance program from an HR perspective, looking at what incentives or disciplinary measures are provided for FCPA-related conduct. Specifically, the evaluation criteria include what steps senior leadership, including human resources personnel, have taken to demonstrate their commitment to FCPA compliance.

The Department further breaks down this area into four separate questions, which relate to:

1. accountability: what disciplinary actions a company took in response to misconduct and when, and what a company's record is in terms of termination and discipline for the misconduct at issue;

2. process: what the human resources process was and who from a company participated in making the disciplinary decisions for the type of misconduct at issue;

3. disciplinary actions: how fairly and consistently disciplinary actions were taken across the company; and

4. incentives: how the company has incentivized compliance and ethical behavior, including in terms of its systems of rewards and incentives, such as promotions.

The February 2017 Guidance thus highlights the importance of proactively addressing potential human resources issues that may arise when a company discovers potential FCPA misconduct.

Proper Disciplinary Action

Other recent enforcement actions also demonstrate the importance of disciplinary actions as part of remediation. For example, in the recent Odebrecht plea agreement with the Department, the DOJ approvingly highlighted Odebrecht's remedial employment decision, including the decision to fire 51 employees who were involved in misconduct, the decision to retain under strict supervision by a monitor 26 employees who were also involved in misconduct, and the imposition of disciplinary actions ranging from demotion to suspension without pay, and other financial penalties.

In addition to local labor laws, a company must also take into account the particulars of an employee's

contract when evaluating disciplinary decisions. In some countries, employment law can present difficulties. In Germany, for example, the Termination Protection Act (Kündigungsschutzgesetz) restricts the termination of an employment relationship except for terminations based on a set of enumerated reasons and only if an employer follows a specific protocol for termination. As another example, Japan has a "lifetime employment" system which makes it virtually impossible to fire employees except on certain enumerated grounds that do not include corrupt behavior.

Human resources employees should be working with anti-corruption compliance personnel to consider all forms of potential disciplinary actions in advance – before the misconduct occurs – as potential remedial responses to FCPA violations.

See The Anti-Corruption Report's three-part series on employee discipline for anti-corruption issues: "Predictability and Consistency in the Face of Inconsistent Laws" (Nov. 1, 2017); "Investigation and Documentation to Smooth the Discipline Process" (Nov. 15, 2017); and "Due Process for a Just and Effective System" (Nov. 29, 2017).

Alex Oh is the co-chair of the Paul, Weiss anti-corruption and FCPA practice group and deputy managing partner of the Washington, DC office. She has an extensive white collar defense and regulatory investigations practice focusing on the FCPA, as well as on securities and accounting fraud issues. Oh also conducts cross-border internal investigations for multinational corporations and regularly counsels Fortune 100 companies on compliance matters. Prior to joining Paul, Weiss, Alex served for nearly four years as an Assistant U.S. Attorney in the Criminal Division of the U.S. Attorney's Office for the Southern District of New York.

Kim Vinocour, who until recently was a senior compliance attorney at Paul, Weiss, focuses her practice on anti-corruption and FCPA matters, as well as sanctions and export controls. Her experience includes counseling, compliance program design and implementation, M&A and transactional due diligence and corruption-related internal investigations and corporate governance issues.

[1] The report can be accessed here.

[2] Specifically, the Guidelines state: the "organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program." United States Sentencing Comm'n, Chapter 8 – Sentencing of Organizations § 8B2.1.b(3) (2015) (emphasis added).