

# ALLEN & OVERY

## *Anti-Bribery and Corruption Year in Review: 2018*

*Global developments in anti-bribery  
and corruption regulation, compliance  
and enforcement*

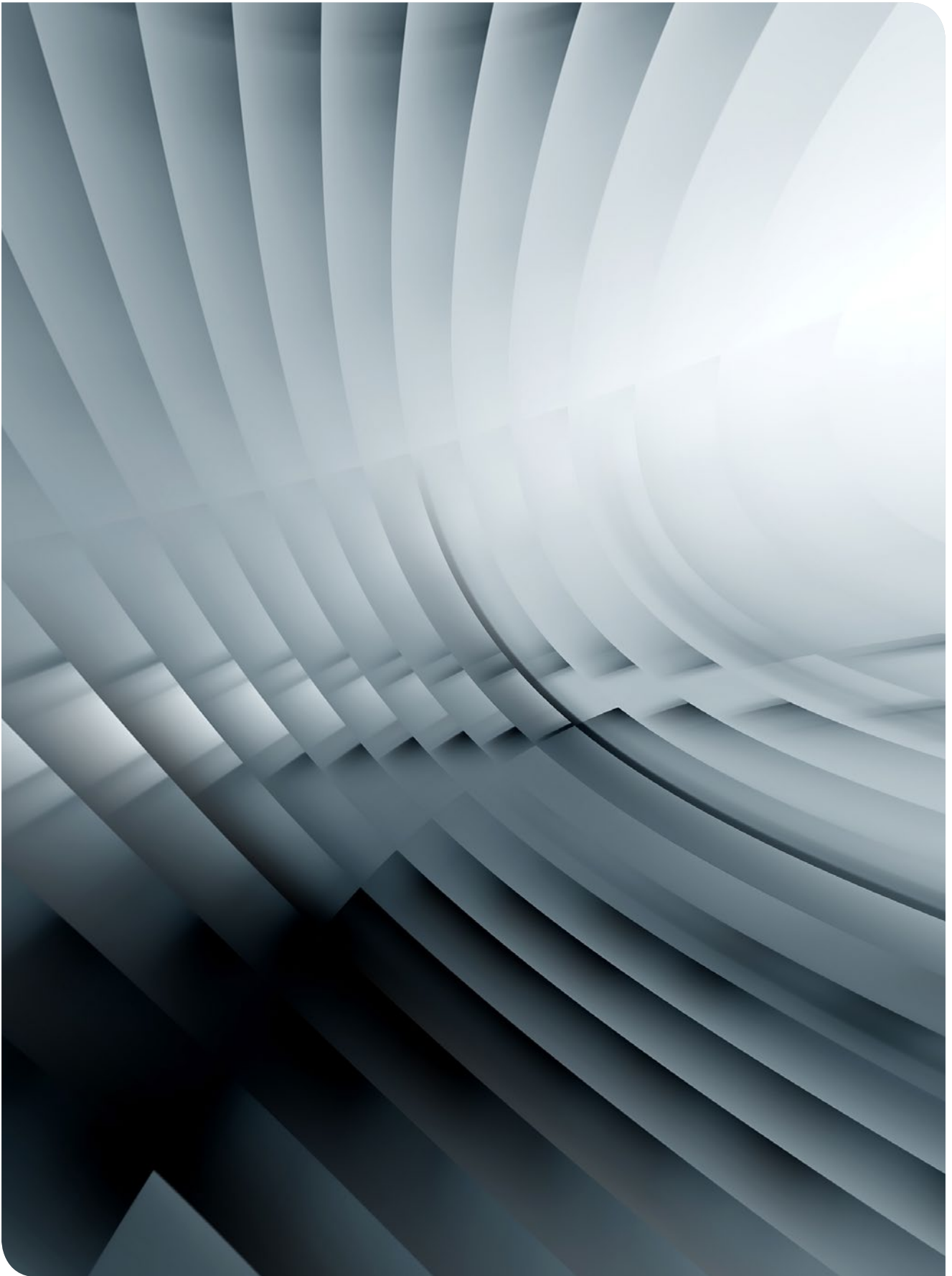
---

January 2019

---

# Contents

<b>Introduction</b>	<b>4</b>	<b>Part 2: Anti-corruption Developments around the World</b>	<b>45</b>
<b>Part 1: The U.S. Foreign Corrupt Practices Act</b>	<b>5</b>	<i>Australia</i>	46
<i>Year in Review</i>	6	<i>Brazil</i>	55
<i>Continued Increase in International Cooperation in FCPA Enforcement</i>	9	<i>Canada</i>	59
<i>The DOJ's Corporate Enforcement Policy in 2018</i>	13	<i>China</i>	61
<i>A Sea Change Underway? Negotiating Corporate Monitorships and Self-Reporting Undertakings in FCPA Settlements</i>	19	<i>Czech Republic</i>	66
<i>U.S. Appeals Court Narrows FCPA's Extraterritorial Reach But Beware – Enforcement Risk Remains</i>	24	<i>France</i>	68
<i>SEC Continues to Leverage Accounting Provisions of the FCPA to Pursue Aggressive Theories of FCPA Liability</i>	27	<i>India</i>	72
<i>Practical Steps for Managing FCPA Risk in M&amp;A: Lessons from FCPA Enforcement Actions in 2018</i>	32	<i>Indonesia</i>	75
<i>Overview of the SEC's Whistleblower Program in 2018</i>	36	<i>Malaysia</i>	77
<i>FCPA-related Policy Developments in 2018</i>	37	<i>Netherlands</i>	79
<i>"China Initiative" Announced by DOJ to Investigate and Prosecute Chinese Companies</i>	41	<i>Singapore</i>	83
<i>In Brief</i>	43	<i>South Africa</i>	86
		<i>Thailand</i>	89
		<i>United Kingdom</i>	91
		<i>Vietnam</i>	103
		<b>Appendix: Summaries of Corporate FCPA Enforcement Actions in 2018</b>	<b>106</b>
		<b>Contacts</b>	<b>152</b>
		<b>About Allen &amp; Overy's Global FCPA and Anti-Corruption Team</b>	<b>155</b>



# Introduction

Welcome to the latest edition of Allen & Overy's annual U.S. Foreign Corrupt Practices Act (**FCPA**) and anti-corruption update. The purpose of this publication is to provide an overview of key developments in anti-bribery and corruption-related policy, legislation and enforcement around the world, as well as to take a closer look at some of the most pressing issues in anti-bribery compliance.

Even putting to one side the significant amount of announced FCPA enforcement activity, 2018 was a particularly active year for FCPA-related activity for other reasons. Notably, the United States Department of Justice (**DOJ**) was busy in announcing several new enforcement policies and initiatives or extending existing policies, all of which will have the effect of directly or indirectly impacting FCPA enforcement; we saw a rare appellate court decision on the jurisdictional reach of the FCPA; the United States Securities and Exchange Commission (**SEC**) continued to push the jurisdictional boundaries of the FCPA's accounting provisions; and, multi-jurisdictional cooperation and coordination in foreign bribery enforcement actions continued a recent trend. Each of these issues, among others, will be explored in depth in this update.

Outside of the United States, several jurisdictions around the world, for example, China, India, Vietnam, Singapore and Thailand, enhanced their anti-bribery and corruption laws, created new institutions designed to pursue wrongful conduct, or increased the tools available to local prosecutors to pursue bribery and corruption cases. In many cases, these changes have signalled—at least on paper—far bolder anti-corruption regimes around the world. While questions may remain about the effectiveness and independence of enforcement of anti-bribery and corruption laws in several of these jurisdictions, this clear trend of introducing new, or revising existing, laws relating to bribery and corruption has seen the laws of many jurisdictions coalesce around many of the same international laws and norms. Multinational companies doing business in these and other jurisdictions should make themselves aware of their heightened exposure to criminal liability, and train their employees on not just the FCPA and UK Bribery Act but the local criminal and regulatory risks.

Other jurisdictions, such as Australia, continued legislative consideration of proposals to enhance their anti-bribery and corruption regime and considered the introduction of deferred prosecution agreement schemes in an effort to hold companies accountable for foreign bribery offenses that have proven difficult to pursue through incumbent laws and prosecution tools. Elsewhere, significant bribery and corruption-related investigations and inquiries are ongoing in jurisdictions including the United Kingdom, Brazil, South Africa and Malaysia (among others) in relation to possible money laundering, securities fraud, bribery, kickback, cheating and other offenses.

These and other developments which are discussed in this update combine to make the anti-bribery and corruption regulation and enforcement landscape all the more complex for companies operating across borders. Companies need to manage risks arising not only out of the anti-bribery and corruption regimes of countries that assert jurisdiction extraterritorially (such as the United States), but also risks arising out of increasingly complex local regulatory regimes and aggressive local enforcement agencies. This complexity makes it all the more challenging for companies to develop and enhance anti-bribery and corruption compliance programs designed to prevent and detect potential violations of law. It also raises the stakes for companies conducting internal investigations, considering voluntary disclosures, and interacting with government enforcement agencies around the world.

We hope you find this publication informative and helpful. Should you have any inquiries, please feel free to email the authors or your usual Allen & Overy contact.

**Allen & Overy**  
**January 2019**

Part 1:

*The U.S. Foreign  
Corrupt Practices Act*

# Year in Review

2018 did not suffer from a shortage of developments on the FCPA legal landscape. From judicial decisions, to policy announcements, and enforcement, it was an active year. The articles in this update are intended to provide in-house legal, compliance, audit, and executive suite personnel with comprehensive and accessible information about noteworthy developments in 2018.

## *No Decline in FCPA Enforcement in 2018*

There was much anticipation that President Donald Trump's administration would lose its resolve in bringing significant FCPA enforcement matters; however, more penalties were collected from companies in 2018 than in any prior year, with 16 companies paying a record USD2.89 billion.

Year	Number of companies reaching resolutions with DOJ/SEC	Penalties paid, including disgorgement
2018	16	USD2.89bn
2017	11	USD1.92bn
2016	27	USD2.48bn
2015	11	USD133m
2014	10	USD1.56m
2013	12	USD731.1m
2012	12	USD259.4m
2011	15	USD508.6m

Notably, three of the six largest FCPA cases of all time, based on penalties and disgorgement, have now been resolved during the Trump administration:

- Petrobras, S.A. agreed to pay collectively USD1.7bn to the U.S. and Brazilian authorities;
- Telia Company A.B. agreed to pay collectively USD965 million to the U.S., Dutch, and Swedish authorities; and
- Société Générale agreed to pay collectively USD585m to the DOJ and French authorities.

These cases cut across industries – oil and gas, telecommunications, and financial services, respectively – and also demonstrate the trend in international cooperation among regulators, which is likely to continue.

## *Drastic Reduction in FCPA Investigations Not Likely*

There are at least four developments that were evident in 2018 that suggest potential FCPA cases will continue to come to the attention of the DOJ and SEC and that a drastic reduction in their docket is unlikely:

### **1. Increase in cooperation among global regulators**

Foreign regulators are more likely than ever, given their own domestic efforts to prosecute corrupt conduct that falls within their jurisdiction, to contact U.S. regulators with information, evidence or tips regarding potential FCPA misconduct.

Given the DOJ's and SEC's demonstrated commitment to cooperation and the number of foreign regulators that are increasing their efforts to prosecute similar cases, companies subject to FCPA investigations in coming years are more likely to be facing inquiries and investigations from regulators in multiple jurisdictions. Responding to a multi-jurisdictional investigation requires commensurate resources and experience.

For more detail, see: *Continued Increase in International Cooperation in FCPA Enforcement*.

### **2. DOJ's Corporate Enforcement Policy incentivizes companies to voluntarily disclose conduct**

In late 2017, the DOJ formalized the preceding Pilot Program on corporate cooperation, increasing the presumptions and benefits to provide, for example, a presumption in favor of declination for companies that voluntarily disclose potential misconduct, fully cooperate with the DOJ's investigation, and fully remediate their misconduct at issue.

The new Policy is intended to render the company's analysis as to whether to disclose misconduct about which the DOJ is otherwise unaware in favor of early disclosure. As a result, companies are likely to continue to bring potential FCPA misconduct to the DOJ in the hopes of an improved result against the company.

For more information about the Policy and how it has been augmented and implemented in 2018, see: *The DOJ's Corporate Enforcement Policy in 2018*.

### 3. Increase in whistleblower tips to the SEC

As recently reported in the SEC's November 2018 Whistleblower Report, in FY 2018, the SEC's Whistleblower Office received a record number of 5,200 tips from 72 countries. This is a 76% increase in the number of tips since FY 2012. The number of FCPA-specific tips has held steady at more than 200 per year since 2016.

In FY 2018, whistleblower awards also hit record highs, including in providing awards to individuals living abroad. As the incentives to blow the whistle to the SEC are only increasing, we can expect tips to continue, including those that implicate potential FCPA misconduct. While many tips may not result in an enforcement case, the existence of the Program and size of rewards ensures that there is an incentive for individuals with knowledge of potential misconduct to come forward.

For more information on whistleblowers and the FCPA, see: *Overview of the SEC's Whistleblower Program in 2018*.

### 4. The DOJ's China Initiative

In an unprecedented move, the DOJ announced a new policy to make clear that the Department would be focusing on enforcement against Chinese companies, predominantly in connection with trade secrets and national security, but specifically enumerating that the Department should "identify FCPA cases involving Chinese companies that compete with American businesses." This initiative does not appear limited to conduct that occurs in China, but rather Chinese companies, regardless of where they operate (or where the potential FCPA misconduct may occur).

Historically, the U.S. authorities have been steadfast that the FCPA is not used to punish companies headquartered abroad or to create a competitive advantage for American companies. This new initiative suggests that Chinese-headquartered companies should be particularly careful in preventing and detecting potential FCPA misconduct.

For more detail, see "*China Initiative*" announced to investigate and prosecute Chinese Companies.

### DOJ Policy Announcements

In late 2017 and throughout 2018, the DOJ has issued a number of changes to existing policy or issued new policies that relate to FCPA enforcement. In addition to the significant announcement of the FCPA Corporate Enforcement Policy in late 2017, and its subsequent expansion to the M&A context, the DOJ had a busy year adopting several new policies. These policies covered a variety of subject matters, including when the DOJ would consider the need to impose a monitorship on a company when resolving an FCPA matter and the so-called "non-piling on policy," which allows the DOJ to formally recognize penalties and disgorgement paid to domestic and foreign regulators to reduce the penalty or disgorgement paid to the DOJ itself. The unprecedented "China Initiative," also suggests a potential shift in enforcement resourcing towards Chinese companies that compete with American companies.

For more information on these policy announcements, see our articles below:

- *The DOJ's Corporate Enforcement Policy in 2018*;
- *A Sea Change Underway? Negotiating Corporate Monitorships and Self-Reporting Undertakings in FCPA Settlements*;
- *Continued Increase in International Cooperation in FCPA Enforcement (addressing the non-piling on policy)*; and
- "*China Initiative*" announced to investigate and prosecute Chinese Companies.
- *FCPA-related Policy Developments in 2018*

### *SEC FCPA Enforcement Through the Accounting Provisions*

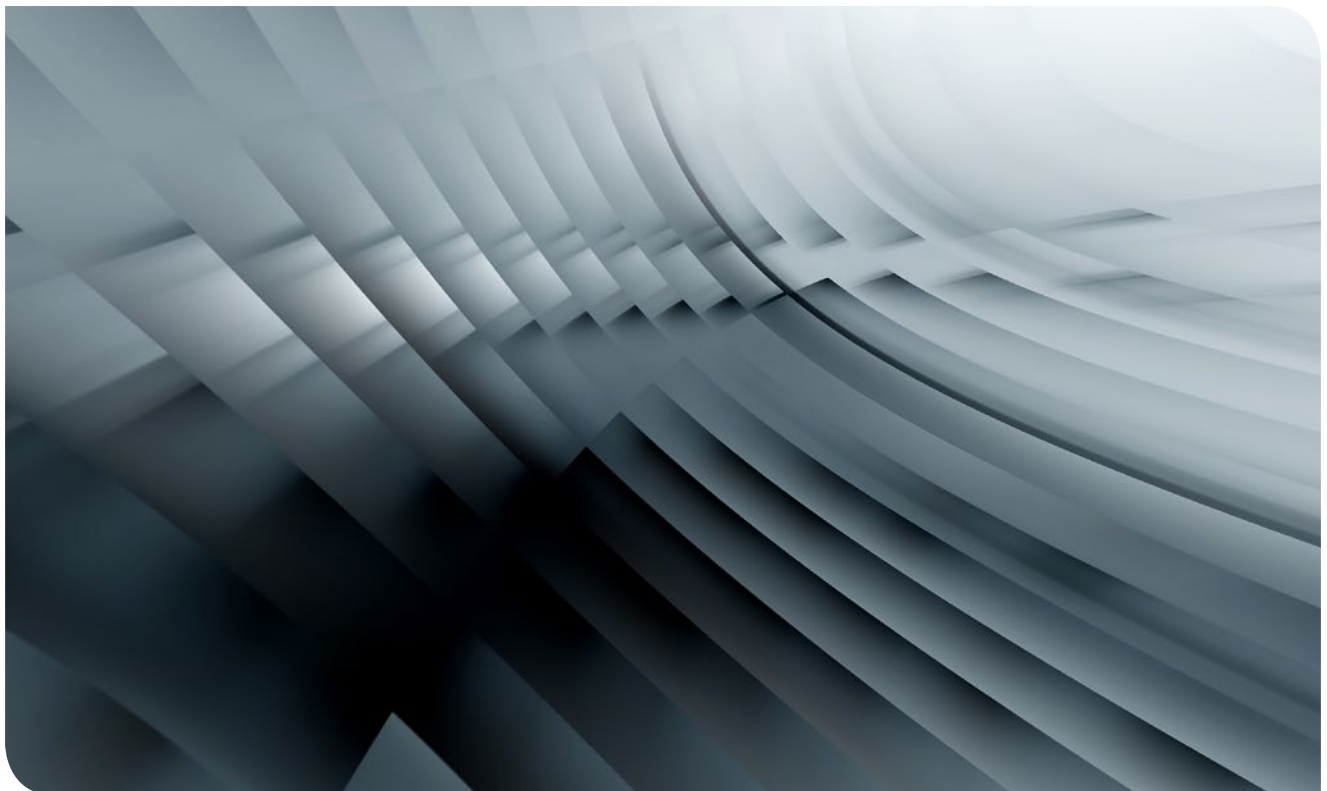
The SEC continues doggedly to bring and resolve FCPA cases against companies and individuals alike. One area of interest has been the extent to which the SEC relies upon the accounting provisions of the FCPA to obtain a settlement from a company, even where substantive FCPA violations are not pursued, perhaps due to a lack of evidence or an absence of jurisdictional nexus.

For more information, see: *SEC Continues to Leverage Accounting Provisions of the FCPA to Pursue Aggressive Theories of FCPA Liability*.

### *Looking Forward*

2018 was a busy year for FCPA-related activity. Enforcement by the DOJ and SEC remained robust, coordination between U.S. authorities and several overseas enforcement agencies remained a key feature of FCPA actions, and the DOJ was active in announcing new policies or enhancing existing policies that will directly or indirectly impact FCPA enforcement. These developments, all of which are covered in this update, make for a more complex and challenging environment for multinational companies to operate. It also raises the stakes for companies conducting internal investigations, considering voluntary disclosures, and interacting with government enforcement agencies around the world.

Please reach out to any of our contributors or your regular Allen & Overy contact for more information from our global network of experts.





# Continued Increase in International Cooperation in FCPA Enforcement

As the FCPA applies to activities that may occur abroad, the activities are often subject to jurisdiction by U.S. and multiple foreign anti-corruption authorities. In fact, five of the ten largest FCPA penalties involved multi-jurisdictional enforcement that resulted in global settlements in which both U.S. and foreign authorities recovered monetary penalties. In 2017, the U.S. Securities and Exchange Commission and the U.S. Department of Justice, the U.S. authorities primarily responsible for the FCPA's enforcement, publicly recognized the cooperation of 22 countries in press releases announcing FCPA resolutions.<sup>1</sup>

Although coordination among foreign countries in corruption investigations is not a novel practice, cross-border coordinated enforcement actions have become more frequent. Since 2016, global settlements of FCPA enforcement actions brought by U.S. and foreign authorities have generated approximately USD10bn in total penalties: USD5.4bn in 2016, USD2.2bn in 2017, and USD2.4bn in 2018.

This article examines the trend of international cooperation and its impact on FCPA enforcement. This article will address (1) the U.S. authorities' stated commitment to collaborating with foreign counterparts in enforcement actions; (2) examples of such collaboration in recent enforcement actions brought concurrently or consecutively by U.S. and foreign authorities; and (3) potential measures for multinational corporations to consider in light of the increase in cooperation.

## *The trend toward international cooperation*

### **A. International coordination as a U.S. policy**

Recently, the U.S. government agencies responsible for enforcing the FCPA have committed to coordinating with foreign authorities in enforcement actions. In November 2017, for example, SEC Enforcement Co-Director Steven Peikin announced that "cooperation and coordination among regulators and law enforcement worldwide is on a sharply upward trajectory, particularly in matters involving

corruption."<sup>2</sup> The SEC publicly acknowledged assistance from 19 jurisdictions in FCPA matters it resolved in its 2017 fiscal year.<sup>3</sup> Then-U.S. Attorney General Jeff Sessions announced the Trump Administration's commitment to "strongly enforce" the FCPA and stated that the DOJ intends to work closely with law enforcement authorities both in the U.S. and abroad to do so. Deputy Attorney General Rod Rosenstein echoed the DOJ's commitment to "enhancing international coordination" when he emphasized the additional resources the DOJ has and continues to allocate to facilitate information sharing in joint and parallel proceedings involving cross-border investigations.<sup>4</sup>

The DOJ has also announced a policy of discouraging duplicative penalties by multiple enforcement authorities for similar conduct; in practice, this is referred to as "non-piling on."<sup>5</sup> The policy states that the DOJ should "endeavor, as appropriate, to coordinate with and consider the amount of fines, penalties, and/or forfeiture paid to other federal, state, local, or foreign enforcement authorities that are seeking to resolve a case with a company for the same misconduct."

1 Evan Epstein, *FCPA, International Cooperation, Global Settlements and Focus on Latin America*, Medium (May 29, 2018), <https://medium.com/@evan.epstein/fcpa-international-cooperation-global-settlements-and-latin-america-focus-649d77ba4780>.

2 Steven R. Peikin, Co-Director Enforcement Division, SEC, *Reflections on the Past, Present, and Future of the SEC's Enforcement of the Foreign Corrupt Practices Act* (Nov. 9, 2017).

3 *Id.*

4 Rod Rosenstein, Deputy Att'y Gen., U.S. Department of Justice, *Remarks to the New York City Bar White Collar Crime Institute* (May 9, 2018).

5 Dep't of Justice, *Policy on Coordination of Corporate Resolution Penalties* (May 9, 2018).

## B. Recent enforcement actions with international coordination

The SEC and the DOJ collaborate with foreign authorities through parallel enforcement actions conducted concurrently or consecutively in response to another country's investigation. The U.S. and foreign authorities then coordinate a global settlement in which the total monetary penalty is divided amongst the countries involved and penalties accorded to foreign regulators are accorded credit by domestic regulators.

2016 was the first year in which the DOJ and SEC settled cases jointly with foreign regulators, and this trend continued in 2017 and 2018.

### *A Closer Look at FCPA Coordinated Settlements with Foreign Regulators*

#### 1. Petrobras (Brazil)

Petróleo Brasileiro S.A. (Petrobras) is a state-owned and controlled oil and gas company in which the Brazilian government owned a majority of the shares.<sup>6</sup> In September 2018, Petrobras paid USD1.78bn in penalties and disgorgement to the SEC, the DOJ, and Brazilian authorities<sup>7</sup> for USD2bn in improper payments its senior executives received from private companies and subsequently passed onto politicians and political parties from 2004 through 2012.<sup>8</sup> The SEC and the DOJ discounted their recovery by the USD682.5m penalty prescribed by the Ministério Público Federal in Brazil. Therefore, the SEC and the DOJ each recovered USD85.3m, which is about 10% of the USD853.2m penalty the DOJ calculated in its non-prosecution agreement.<sup>9</sup> The SEC also offset its penalty by the settlement owed in the

shareholder class action against Petrobras.<sup>10</sup>

#### 2. Société Générale (France)

In June 2018, Société Générale paid USD586m total in penalties to the DOJ and French authorities for USD90m in bribes its employees paid Libyan government officials from 2005 through 2011.<sup>11</sup> In its deferred prosecution agreement, the DOJ discounted its penalty to account for the USD293m penalty imposed by the French Parquet National Financier.<sup>12</sup> This was the first enforcement action in which U.S. and French authorities coordinated penalties.

#### 3. Keppel Offshore (Brazil and Singapore)

Keppel Offshore & Marine LTD, a Singapore-based shipyard and shipping vessel operations company, agreed to pay USD422m in penalties to the DOJ and authorities in Brazil and Singapore. From 2001 through 2014, Keppel Offshore's subsidiaries paid Brazilian officials USD50m in bribes, which resulted in USD350m in profits. Keppel Offshore entered into a deferred prosecution agreement in December 2017 in which the DOJ allocated the USD422m total penalty between the Brazilian Ministério Público Federal (USD211m), the Attorney General's Chambers in Singapore (USD105m), and the DOJ (USD106m). Keppel Offshore's U.S. subsidiary entered into a plea agreement that included a USD472m criminal penalty to the DOJ. A senior member of Keppel Offshore's Singapore legal department entered a separate guilty plea.<sup>13</sup>

6 In the Matter of Petróleo Brasileiro S.A., Admin. Proceeding File No. 3-18843 (Sept. 27, 2018) ¶ 6 (hereinafter the **Petrobras SEC Order**).

7 See Richard L. Cassin, "Petrobras reaches \$1.78 billion FCPA resolution," FCPA Blog (Sept. 27, 2018), <http://www.fcpablog.com/blog/2018/9/27/petrobras-reaches-178-billion-fcpa-resolution.html>.

8 Petrobras SEC Order ¶¶ 2, 16, 25.

9 Letter from U.S. Department of Justice to Petrobras (Sept. 26, 2017), available at <https://www.justice.gov/opa/press-release/file/1096706/download>.

10 Petrobras SEC Order at 9.

11 U.S. v. Société Générale S.A., 18-CR-253 (DLJ) (E.D.N.Y. June 4, 2018) ¶ 20.

12 *Id.*

13 Press Release, DOJ, Keppel Offshore & Marine Ltd. and U.S. Based Subsidiary Agree to Pay \$422 Million in Global Penalties to Resolve Foreign Bribery Case (Dec. 22, 2017), available at <https://www.justice.gov/opa/pr/keppel-offshore-marine-ltd-and-us-based-subsidiary-agree-pay-422-million-global-penalties>.

#### 4. SBM Offshore (Netherlands and Brazil)

SBM Offshore N.V. (SBM), a Netherlands-based offshore drilling equipment manufacturer, has paid a total of USD475m in penalties to the DOJ, the Dutch Public Prosecutor's Office, and Brazil's Ministério Público Federal. SBM executives bribed officials in Brazil, Angola, Equatorial Guinea, Kazakhstan and Iraq with over USD180m, and these bribes resulted in approximately USD2.8bn in profits. In November 2017, the DOJ ordered SBM to pay USD238m as part of its deferred prosecution agreement. At that time, SBM had already disgorged USD200m and paid a USD40m fine to the Dutch Public Prosecutor's Office. The DOJ accounted for the Dutch penalties and potential fines from Brazilian authorities in setting its penalty.<sup>14</sup>

#### 5. Telia (Sweden)

Swedish telecommunications service provider Telia agreed to pay USD965m in penalties to the SEC, the DOJ, Dutch, and Swedish authorities in September 2017. From 2007 through 2010, employees at Telia's subsidiaries bribed high-ranking government officials in Uzbekistan more than USD331m to gain access to the Uzbek telecommunications market.<sup>15</sup> The DOJ entered into a deferred prosecution agreement with Telia in which it stipulated that Telia should pay USD548m.<sup>16</sup> As part of that total, the DOJ offset its USD274m criminal penalty to account for the penalties imposed by the Dutch Public Prosecution Service.<sup>17</sup> The SEC ordered Telia to disgorge USD457m in illegally gained profits, but reduced the disgorgement total to USD208m to offset the DOJ penalty and USD40m forfeiture.<sup>18</sup>

#### *Increased focus on anti-corruption enforcement outside the United States*

While the United States is still the world leader in terms of enforcing anti-corruption laws against conduct that occurs beyond its borders, other countries are strengthening their anti-corruption laws and enforcement efforts.

Multiple countries are emboldening their enforcement authorities. Countries such as Switzerland and the Netherlands have bolstered their enforcement activity by bringing more and larger corruption investigations. For example, Swiss and Dutch authorities took active roles in the investigations of Telia, Odebrecht S.A., and VimpelCom.<sup>19</sup>

The Dutch Public Prosecution Service also brought an independent anti-corruption enforcement matter against the Dutch bank ING Group in September 2018: ING agreed to pay a fine of USD782 million and disgorge USD115 million to settle charges that the bank used laundered funds to bribe the daughter of an Uzbekistan official for telecommunications access.<sup>20</sup> Other foreign enforcement authorities, including Brazil, Peru, and South Korea, are investigating their own governments for misconduct. Argentinian authorities are currently investigating "the bribery notebooks" of a former government chauffeur who documented driving officials around to deliver cash bribes.<sup>21</sup>

Countries outside of the U.S. are actively enhancing their anti-corruption laws and enforcement authority by encouraging corporate cooperation with investigation, such as adopting U.S.-style deferred prosecution agreements in France and the United Kingdom.

14 Press Release, DOJ, SBM Offshore N.V. And United States-Based Subsidiary Resolve Foreign Corrupt Practices Act Case Involving Bribes in Five Countries (Nov. 29, 2017), available at <https://www.justice.gov/opa/pr/sbm-offshore-nv-and-united-states-based-subsidiary-resolve-foreign-corrupt-practices-act-case>.

15 In the Matter of Telia Company AB, Admin. Proceeding File No. 3-18195 (Sept. 21, 2017) ¶¶ 2, 15.

16 Letter from U.S. Dep't of Justice to Telia Company AB (Sept. 21, 2017) at 7-9, available at <https://www.justice.gov/criminal-fraud/file/998601/download>.

17 *Id.*

18 In the Matter of Telia Company AB, Admin. Proceeding File No. 3-18195 (Sept. 21, 2017) at 8.

19 See William Garrett and Kristen Savelle, FCPA Enforcement in Q3 Show Results of International Collaboration, *The Wall Street J.* (Oct. 24, 2017, 2:13 PM), <https://blogs.wsj.com/riskandcompliance/2017/10/24/fcpa-enforcement-in-q3-showed-results-of-intl-collaboration/> (hereinafter **Garrett and Savelle**).

20 Press Release, Openbaar Ministerie, ING pays 775 million due to serious shortcomings in money laundering prevention (Sept. 4, 2018), available at <https://www.om.nl/actueel/nieuwsberichten/@103952/ing-pays-775-million/>.

21 Los cuadernos de las coimas: uno por uno, todos los registros del chofer Oscar Centeno, *La Nacion* (Aug. 5, 2018, 10:37 AM), <https://www.lanacion.com.ar/2159363-cuadernos>.

Other foreign authorities are mirroring the U.S.'s non-piling on policy and recognizing companies' settlements with the U.S. to reduce their penalties: Israel reduced its penalty against Teva Pharmaceuticals to USD22m<sup>22</sup> and the Dutch Public Prosecution Service reduced its penalty against Telia Company at USD274m<sup>23</sup> to account for penalties owed to U.S. authorities.

### *Lessons for multinational corporations*

This increase in international cooperation and foreign regulator enforcement has implications for corporations operating on a global scale.

#### **Prevention as the best medicine**

Having a robust, global compliance program designed to address the company's specific risk profile will be the best chance to avoid expensive and protracted investigations from multiple regulators. Consider whether your company's compliance program is sufficiently resourced and tailored to your company's specific risk.

#### **Corporate records**

The barriers to U.S. regulators obtaining evidence from abroad are becoming lower, while foreign protections to sharing documents and information are often increasing. Taking care to consider where documents are created, maintained, and stored may become particularly important if confronted with an investigation with global reach.

#### **Managing an investigation with multiple regulators**

Where multiple regulators are investigating simultaneously or where multiple regulators may have jurisdiction over the same conduct, corporations should keep in mind cross-border concerns and take a proactive approach to managing regulators' expectations. Anticipate that documents and information shared with one country may become available to another country's authorities. Each jurisdiction is likely to impose different expectations and obligations with respect to retaining privilege, data protection, and employee rights with respect to data collection, conducting interviews, and potential disciplinary action.

Retaining counsel with expertise in each relevant jurisdiction will assist in ensuring the respective obligations are satisfied while positioning the company favorably in each jurisdiction.

<sup>22</sup> Shoshanna Solomon, Teva to pay NIS 75 million to Israel authorities to settle foreign bribes claims, The Times of Israel (Jan. 15, 2018).

<sup>23</sup> Press Release, Openbaar Ministerie, International fight against corruption: Telia Company pays \$274 million to the Netherlands (Sept. 21, 2017), available at <https://www.om.nl/vaste-onderdelen/zoeken/@100345/international-fight/>.

# The DOJ's Corporate Enforcement Policy in 2018

In November 2017, the U.S. Deputy Attorney General, Rod Rosenstein, announced the Department of Justice's new FCPA Corporate Enforcement Policy<sup>1</sup> that creates a presumption of declination for companies that voluntarily self-disclose, fully cooperate with the Department's investigation, and timely and appropriately remediate, including restitution and disgorgement of ill-gotten gains. This article will describe the Policy as adopted, two subsequent expansions to the application of the Policy, and recent declinations issued pursuant to the Policy.

## *Overview of the Corporate Enforcement Policy*

### **Presumption for Declination and Potential Reduction in Penalty Calculations**

The Policy offers a presumption of declination for companies that voluntarily self-disclose, fully cooperate with the Department's investigation, and timely and appropriately remediate, which may include disgorgement of any ill-gotten profits.<sup>2</sup> Under the preceding Pilot Program,<sup>3</sup> such companies were only "considered" for declination.

The presumption does not apply where there are aggravating circumstances or the company is a criminal recidivist.<sup>4</sup> Examples of aggravating circumstances include the pervasiveness of the misconduct at the company, the involvement of executive management, and whether the company received significant profits from the violations. Recidivism is not expressly limited to FCPA-related conduct, nor does it include civil conduct.

If a criminal resolution is warranted, but the company has self-disclosed, cooperated, and remediated, the Department will accord a 50% reduction in the penalty for non-recidivists and generally will not require a monitor if the company has implemented an effective compliance program at the time of resolution.

### **Timely Self-Reporting**

Consistent with the Pilot Program, self-disclosure must be both timely and complete. Companies that do not self-disclose are treated the same as under the Pilot Program – up to a 25% penalty reduction if they fully cooperate and remediate – and DOJ's definitions of "voluntary self-disclosure," "full cooperation" and "timely and appropriately remediation" are largely unchanged.

### **Full Cooperation**

To obtain the benefits of the Policy, companies must fully cooperate with the Department.<sup>5</sup> Full cooperation means timely disclosure of all facts relevant to the wrongdoing and timely updates on the company's investigation, including facts related to involvement by the company's officers, employees, agents, and third parties. The Department requires companies to provide it with a consistent flow of information.<sup>6</sup>

In the Department's view, this means that a company should be prepared to provide details of what it knows about the wrongdoing and the investigative steps it has taken to date. This includes a clear explanation of who is conducting the investigation. It should also disclose to whom the independent investigation will report – whether it be the audit committee, management, the general counsel, or someone else, and which individuals, if any, are "walled off" from the investigation or are represented by counsel.

<sup>1</sup> Dep't of Justice, FCPA Corporate Enforcement Policy, § 9-47.110.

<sup>2</sup> *Id.*

<sup>3</sup> Press Release, DOJ, Criminal Division Launches New FCPA Pilot Program (Apr. 5, 2016), available at <https://www.justice.gov/archives/opa/blog/criminal-division-launches-new-fcpa-pilot-program>.

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> John P. Cronan, Principal Deputy Assistant Att'y Gen., U.S. Dep't of Justice, Remarks at the Latin Lawyer/Global Investigations Review Anti-Corruption and Investigations Conference (Oct. 18, 2018).

A company and its advisors should also be prepared to address the nature, scope, and status of the investigation they are undertaking, as well as what investigative steps they plan to undertake, including what countries, locations, and conduct are being looked at. The Department also expects the company to explain what steps it is taking to preserve and collect potentially relevant evidence, including electronic devices and communications. Cooperation may also require that the company provide the Department with a list of individuals who have already been interviewed, those who it may interview in the future, and those who have already been told about the allegations – including any third party.

On November 29, 2018, Deputy Attorney General Rod J. Rosenstein explained the degree of cooperation the Department expects from companies.<sup>7</sup> Absent extraordinary circumstances, the Department will not issue a corporate resolution that protects individuals from criminal liability. Under the Policy, companies seeking cooperation credit in a criminal case must identify every individual who was substantially involved in, or responsible for the criminal conduct. However, in response to concerns raised by companies regarding the inefficiency of identifying every employee involved regardless of relative culpability, the Department clarified this requirement. Rather than delay investigations to collect information about individuals with little involvement, companies must identify those individuals who play significant roles in criminal conduct – in other words – who authorized it, and what did they know?<sup>8</sup>

### Remediation

To determine whether remediation credit is warranted and evaluate whether a monitorship is necessary, the DOJ will consider whether the company has implemented an effective compliance and ethics program. The Policy specifies some of the “hallmarks” of an effective compliance and ethics program against which the company’s remediation efforts will be evaluated. These hallmarks include the company’s

culture of compliance, resources dedicated to compliance, the expertise, authority, independence, and compensation of the compliance function, the effectiveness of the company’s risk assessment and how the compliance program has been tailored based on that assessment, and auditing of the program to ensure its effectiveness. This is a much more high-level description of how the Department evaluates corporate compliance programs than the DOJ Fraud Section’s detailed February 2017 guidance. A company monitor will also ordinarily not be required.

### *Expansions of the policy*

Throughout the course of 2018, the Department has continued to expand the FCPA Corporate Enforcement Policy and the possibility of a declination for cooperating companies. The principles of the Policy have been adopted as guidance involving violations other than the FCPA, and in the FCPA context, the Policy will now be applied to the acquisitions context.

### Declinations Beyond the FCPA

In March 2018, John Cronan, the acting head of the DOJ’s Criminal Division, and Benjamin Singer, Chief of the Fraud Section’s Securities and Financial Fraud Unit, stated that the Policy may be used as nonbinding guidance in other criminal cases involving corporate defendants.<sup>9</sup> The DOJ’s Criminal Division will “embrace” a similar approach and principles where appropriate – rewarding companies that voluntarily self-disclose, cooperate, and remediate. The Department announced a declination in a case involving non-FCPA violations, relying on the same principles underlying the Policy. In that case, Barclays Foreign Exchange (**FX**) traders allegedly misappropriated confidential information provided to Barclays in connection with FX options and spot transactions, and allegedly deceived the customer about the nature of its trading.<sup>10</sup>

<sup>7</sup> Rod Rosenstein, Deputy Att’y Gen., U.S. Dep’t of Justice, Remarks to the New York City Bar White Collar Crime Institute (May 9, 2018).

<sup>8</sup> *Id.*

<sup>9</sup> DOJ Expands Leniency Beyond FCPA, Lets Barclays Off, Law360 (Mar. 1, 2018), available at: <https://www.law360.com/articles/1017798/dojexpands-leniency-beyond-fcpa-lets-barclays-off>.

<sup>10</sup> Letter from U.S. Dep’t of Justice to Barclays (Feb. 28, 2018), available at <https://www.justice.gov/criminal-fraud/file/1039791/download>.

The conduct gave rise to individual enforcement actions, but the Department declined to prosecute the company due to its timely and voluntarily self-disclosure, thorough and comprehensive internal investigation, and full cooperation. Barclays' cooperation included providing all known relevant facts about individuals involved in the misconduct. Barclays also implemented new compliance policies and procedures to reduce the likelihood of future fraud and market manipulation. Barclays agreed to full remediation, including paying full restitution to its customer and disgorgement of profits (USD12,896,011) from the misconduct.

### Mergers & Acquisitions

On September 27, 2018, Deputy Assistant Attorney General Matthew Miner announced that the Department will now apply the Policy to mergers and acquisitions that cover potential FCPA violations, in addition to other types of wrongdoing.<sup>11</sup> Acknowledging that deals move quickly, and that an acquiring company may have limited access to a target's data and records, Miner clarified that if an acquirer discovers evidence of misconduct during pre- or post-acquisition due diligence, the Department will consider whether the acquiring company helped to uncover the misconduct, self-reported, and whether it implemented internal controls to the acquired company post-acquisition. Accordingly, companies should keep the benefits of early disclosure and the Policy in mind where it uncovers wrongdoing in an acquired company.

### *The policy in practice: FCPA declinations in 2018*

In 2018, the Department issued three declinations to companies facing FCPA violation allegations. These three declinations highlight how companies can take advantage of the Policy to obtain a declination. Although the Department declined to prosecute the companies in each case, it pursued individual enforcement actions against the culpable individuals. As Miner noted in September 2018, the Unit "remain[s] steadfast in [its] commitment to holding those engaged in wrongdoing accountable."<sup>12</sup>

The three FCPA-related declinations discussed below are instructive as to how the Department's various new policies on corporate enforcement operate, recognizing when companies are subject to foreign regulatory enforcement for the same conduct (the so-called Non-Piling On Policy), and focus on ensuring that individuals are held accountable for wrongdoing. In two of the declinations, senior executives were implicated in connection with the improper conduct, yet the DOJ nevertheless declined under the Policy.

### The Dun & Bradstreet Corporation

In April 2018, the Department publicly released its declination letter to The Dun & Bradstreet Corporation relating to its FCPA investigation into bribery committed by employees of the Company's subsidiaries in China.<sup>13</sup> The two Chinese subsidiaries used third party agents to make unlawful payments to obtain important data to Dun & Bradstreet's business as a provider of business financial information.<sup>14</sup> One subsidiary made unlawful payments to Chinese government officials in exchange for non-public financial statement information on Chinese entities. The second subsidiary made improper payments to third parties to acquire non-public personal data that was used in its products and also made improper payments to obtain specific business. Dun & Bradstreet falsely recorded these

11 Deputy Assistant Attorney General Matthew S. Miner of the Justice Department's Criminal Division Delivers Remarks at the 5th Annual GIR New York Live Event, New York, NY, Thursday, September 27, 2018 <https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-justice-department-s-criminal-division>

12 Ibid.

13 Letter from U.S. Dep't of Justice to The Dun & Bradstreet Corp. (Apr. 23, 2018), available at <https://www.justice.gov/criminal-fraud/file/1055401/download>.

14 Press Release, SEC, SEC Charges Dun & Bradstreet With FCPA Violations (Apr. 6, 2018), available at <https://www.sec.gov/enforce/34-83088-s>

improper payments as legitimate business expenses. Despite red flags discovered during pre-acquisition due diligence efforts, Dun & Bradstreet failed to take appropriate action to stop the improper payments or to stop the false entries into the subsidiary's books and records, which continued for several years post-acquisition.

The Dun & Bradstreet declination is useful in identifying how the Department considers full cooperation and remediation. There, Dun & Bradstreet identified all eleven individuals involved in or responsible for the misconduct, provided the Department all facts relating to that misconduct, making current and former employees available for interviews, and translated foreign language documents to English. To remediate, Dun & Bradstreet took steps to enhance its compliance program and its internal accounting controls, terminated the employment of all individuals involved in the misconduct, disciplined other employees by reducing compensation, lowering performance reviews, and issuing formal reprimands; and disgorged to the SEC USD9.2m. These factors demonstrate the extensive cooperation and remediation the Department requires for a company to benefit from the Policy.

Although the Department declined to prosecute, the SEC required Dun & Bradstreet to disgorge over USD6m in profits, in addition to a USD2m penalty, finding that Dun & Bradstreet civilly violated the FCPA's books and records and internal controls provisions.<sup>15</sup> Specifically, Dun & Bradstreet failed to identify and address red flags identified as part of pre-acquisition diligence, failed to conduct post-acquisition diligence, and failed to maintain a system to prevent and detect improper payments made over the course of several years.

### **Guralp Systems Ltd. (Guralp)**

In August 2018, the Department announced that it declined to charge Guralp for possible violations of the FCPA and U.S. money laundering statutes.<sup>16</sup> The violations stemmed from Guralp's payments to Heon-Cheol Chi, director of the Earthquake Research Center at the Korea Institute of Geoscience and Mineral Resources.

Not only did Guralp voluntarily disclose the misconduct to the Department, but it also made "significant remedial efforts," and substantially cooperated with the Department's investigation. Guralp cooperated with the Department by voluntarily producing relevant documents and information to the Department and by assisting with the prosecution of Chi for violating the U.S. money laundering statute. Citing Guralp's voluntary disclosure of the misconduct and cooperation, the Department recognized Guralp's role in assisting in its prosecution (and conviction) of Chi for violating the U.S. money laundering statute.

As an example of the Department's consideration of the "piling on" factor, Guralp was the subject of an ongoing investigation by the UK's Serious Fraud Office relating to the same conduct. Guralp, a UK company with its principal place of business in the UK, "committed to accepting responsibility for that conduct with the SFO." The Department factored the parallel investigation in its consideration to decline prosecution. Moreover, in August 2018, the UK Serious Fraud Office also announced charges against Dr Cansun Guralp, the founder of Guralp, and Andrew Bell, the Managing Director of Guralp.<sup>17</sup>

<sup>15</sup> In the Matter of The Dun & Bradstreet Corp. Proceeding File No. 3-18446 (Apr. 23, 2018).

<sup>16</sup> Letter from U.S. Dep't of Justice to Guralp Systems Ltd. (Aug. 20, 2018), available at <https://www.justice.gov/criminal-fraud/page/file/1088621/download>.

<sup>17</sup> Marieke Breijer, *SFO Charges Two in Guralp Systems Limited Investigation*, Global Investigations Review. (Aug. 17, 2018) <https://globalinvestigationsreview.com/article/1173236/sfo-charges-two-in-guralp-systems-limited-investigation>.



### **Insurance Corporation of Barbados Limited (ICBL)**

Also in August 2018, the Department announced that it had closed its inquiry of ICBL, a Barbadian insurance company, where the Department's investigation had found that ICBL, through its employees and agents, paid USD36,000 in bribes to a Barbadian government official in exchange for insurance contracts worth USD686,827, resulting in net profits of USD94,000.<sup>18</sup>

Specifically, high-level employees of ICBL took part in a scheme to pay bribes to Donville Inniss, a member of the Parliament of Barbados, who also served as the Minister of Industry, International Business, Commerce, and Small Business Development of Barbados. These high-level employees also took part in a scheme to launder the bribe payments into the United States through a U.S. bank account in the name of a New York dental company, owned by a friend of Inniss. Despite the high-level involvement of senior officers in the company, the Department decided to close its investigation, citing a number of factors it considered. On August 6, 2018, the Department filed charges against Donville Inniss in the Eastern District of New York. Although it did not list the specific individuals involved, the indictment described the bribery scheme and the involvement of company executives in furtherance of the scheme.<sup>19</sup>

First, ICBL timely and voluntarily self-disclosed the misconduct described above, and conducted its own thorough and comprehensive investigation. Second, ICBL cooperated with the Department in the inquiry, producing all relevant known facts about the misconduct and agreeing to continue to cooperate in the Department's ongoing investigations and/or prosecutions. Third, ICBL terminated all executives and employees involved in the misconduct,

and agreed to disgorge roughly USD94,000 in profits.<sup>20</sup> The Department noted that its ability to identify and charge the culpable individuals also influenced its decision.

### **Polycom, Inc. (Polycom)**

On December 20, 2018, the Department announced it had declined to prosecute Polycom for violations of the FCPA, consistent with the FCPA Corporate Enforcement Policy, despite the bribery committed by the employees of a Polycom subsidiary in China, and the company's subsidiaries in China knowing and willfully causing false books and records at Polycom.

Based on the SEC administrative order announced days later on December 26, 2018, we know this matter concerned activity between 2006 and at least July 2014 in which Polycom's Vice President of China at Polycom's China subsidiary, along with senior managers, provided significant discounts to Polycom's distributors and/or resellers, knowing and intending that the distributors and/or resellers would use the discounts to make payments to officials at Chinese government agencies and government-owned enterprises in exchange for those officials' assistance in obtaining orders for Polycom's products. Interestingly, this case involved employees and managers at the China subsidiary recording payments in a parallel deal-tracking and email system located in China, but outside of Polycom's company-approved systems. These senior managers at Polycom's Chinese subsidiary also instructed their sales personnel not to use their Polycom email addresses when discussing sales opportunities with Polycom's distributors.

<sup>18</sup> Letter from U.S. Dep't of Justice to Insurance Corporation of Barbados Ltd. (Aug. 23, 2018), available at <https://www.justice.gov/criminal-fraud/page/file/1089626/download>.

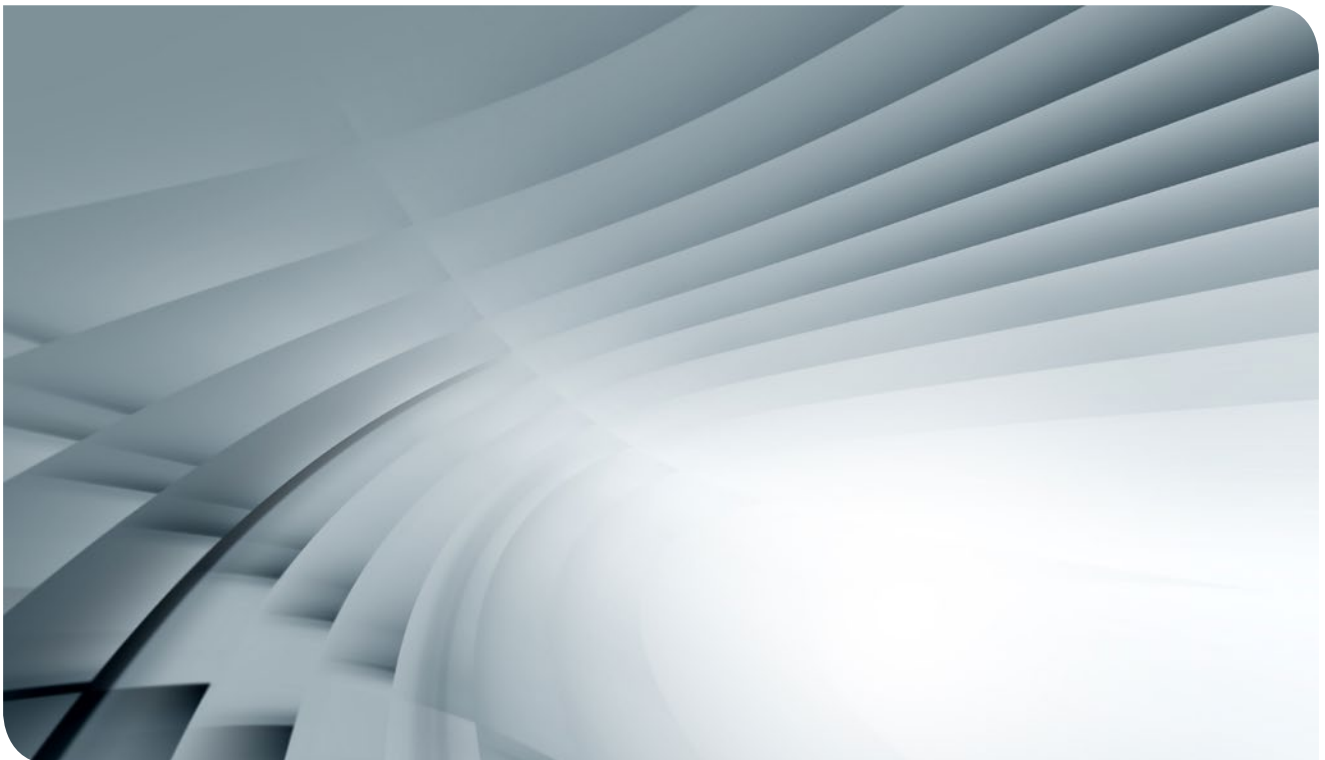
<sup>19</sup> Press Release, DOJ, Former Member of Barbados Parliament and Minister of Industry Indicted for Money Laundering (Aug. 6, 2018), available at <https://www.justice.gov/usao-edny/pr/former-member-barbados-parliament-and-minister-industry-indicted-money-laundering>

<sup>20</sup> Letter from U.S. Dep't of Justice to Insurance Corporation of Barbados Ltd. (Aug. 23, 2018), available at <https://www.justice.gov/criminal-fraud/page/file/1089626/download>.

The Department based its decision to decline prosecution based on a number of factors, including Polycom's thorough investigation and full cooperation which included providing the Department with all facts relating to the misconduct and making employees available for interviews and assisting with the Department's efforts to interview a former employee, translating foreign language documents to English, and identifying unrelated misconduct to the Department for investigation and potential prosecution, and Polycom's remediation, including steps taken to enhance its compliance program and its internal accounting controls, terminating the employment of eight individuals involved in the misconduct, disciplining another 18 employees and terminating Polycom's relationship with one of its distributors.

### *Takeaways*

In each of the declinations summarized above, the Department looked to whether the company promptly and voluntarily disclosed the misconduct and whether it conducted a comprehensive internal investigation. But what the declinations also show is that the Department expects significant cooperation and remediation if a company wants to benefit from the Policy. Even where senior executives are highly involved in the alleged misconduct, a company may still avoid prosecution. Indeed, even if the company loses the presumption of a declination under the Policy, the Department may still decline to prosecute. A company can benefit if it provides detailed information about the wrongdoing, the investigation, and the culpable individuals, and if it takes steps to correct the wrongdoing and to prevent further harm, including terminating employees and third party relationships.



# A Sea Change Underway? Negotiating Corporate Monitorships and Self-Reporting Undertakings in FCPA Settlements

Recent guidance from the DOJ regarding when and whether to impose a compliance monitor as an element of a corporate resolution provides evidence of a sea change underway in the use of such monitors, providing both instruction to prosecutors and arguments for companies aimed at reducing the frequency and intrusiveness of such monitors. In light of this guidance, companies navigating an FCPA investigation should commit to remediating any control weaknesses identified by the investigation as soon as possible, and should use DOJ's most recent guidance to avoid entirely or to narrow the scope of corporate monitor or self-reporting undertakings in FCPA settlements.

## *October 2018 DOJ guidance on corporate monitors – the Benczkowski Memorandum*

On October 11, 2018, the DOJ released new guidance on corporate monitors in a memorandum from Assistant Attorney General Brian A. Benczkowski titled “Selection of Monitors in Criminal Division Matters.”<sup>1</sup> The Benczkowski Memorandum supersedes prior guidance from 2009<sup>2</sup> and supplements the Morford Memorandum of 2008, which advised DOJ prosecutors negotiating corporate settlements to be mindful of both the costs and benefits of a monitor.<sup>3</sup> The Morford Memorandum also established nine principles to guide the selection, scope, and duration of a corporate monitorship. The most relevant of those are as follows:

**Principle 3:** A monitor's primary responsibility should be to assess and monitor a company's compliance with those terms of a settlement that are specifically designed to address and reduce the risk of recurrence of the company's misconduct, including, in most cases, evaluating (and where

appropriate proposing) internal controls and corporate ethics and compliance programs.

**Principle 4:** In carrying out his or her duties, a monitor will often need to understand the full scope of the company's misconduct covered by the settlement, but the monitor's responsibilities should be no broader than necessary to address and reduce the risk of recurrence of the company's misconduct.

**Principle 8:** The duration of a monitorship should be tailored to the problems that have been found to exist and the types of remedial measures needed to satisfy the monitor's mandate.<sup>4</sup>

The Benczkowski Memorandum provides guidance to prosecutors on the “principles for determining whether a monitor is needed in individual cases.”<sup>5</sup> That is, while the Morford Memorandum guided DOJ attorneys on the selection, scope, and duration of monitorships, the Benczkowski Memorandum directs prosecutors to assess whether a monitor is even necessary in the first place. The

1 Memorandum from Brian A. Benczkowski, U.S. Department of Justice, Selection of Monitors in Criminal Division Matters (2018), available at <https://www.justice.gov/opa/speech/file/1100531/download>.

2 Memorandum from Lanny Breuer, U.S. Department of Justice, Selection of Monitors in Criminal Division Matters (2009), available at <https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2012/11/14/response3-supp-appx-3.pdf>.

3 Memorandum from Craig S. Morford, U.S. Department of Justice, Selection and Use of Monitors in Deferred Prosecution Agreements and Non-prosecution Agreements with Corporations (2008), available at <https://www.justice.gov/sites/default/files/dag/legacy/2008/03/20/morford-useofmonitorsmemo-03072008.pdf>.

4 *Id.* at 5-8.

5 The Benczkowski Memorandum also provides guidance on subjects that are not addressed in this article, including the DOJ approval process for monitorship agreements, the terms of monitorship agreements, DOJ's Standing Committee and the selection process for monitors, retention of DOJ records regarding monitor selection, and departures from DOJ policy and procedure.

Memorandum acknowledges the potential benefits of monitorships, but cautions that “the imposition of a monitor will not be necessary in many corporate criminal resolutions” and advises that “the scope of any monitorship should be appropriately tailored to address the specific issues and concerns that created the need for the monitor.”<sup>6</sup> The Memorandum directs DOJ prosecutors to consider the following factors when evaluating the potential benefits of a corporate monitor:

- whether the underlying misconduct involved the manipulation of corporate books and records or the exploitation of an inadequate compliance program or internal control systems;
- whether the misconduct at issue was pervasive across the company or approved or facilitated by senior management;
- whether the company has made significant investments in, and improvements to, its corporate compliance program and internal control systems; and
- whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future.<sup>7</sup>

The Benczkowski Memorandum also notes that where misconduct occurred under different corporate leadership or within a compliance environment that no longer exists at a company, DOJ prosecutors should consider whether the leadership and/or compliance changes are adequate safeguards to prevent recurrence.<sup>8</sup> Prosecutors also should assess the adequacy of a company’s remedial measures such as the termination of business relationships with employees, management, or third party agents responsible for the misconduct.<sup>9</sup>

In assessing the potential costs of a monitor, the Benczkowski Memorandum advises that prosecutors “should consider not only the projected monetary costs to the business organization, but also whether the proposed scope of a monitor’s role is appropriately tailored to avoid unnecessary burdens to the business’s operations.”<sup>10</sup> The Memorandum concludes that a monitor should be imposed only where “there is a demonstrated need for, and clear benefit to be derived from, a monitorship relative to the projected costs and burdens” and advises that a monitor likely will not be necessary where “a corporation’s compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution.”<sup>11</sup>

### *What does this new guidance mean for companies facing an FCPA investigation?*

The DOJ is recognizing that monitorships are extraordinarily burdensome to companies, and that where needed, they should be imposed only within a tailored scope designed to address the identified problems at the company in question.

The frequency of corporate monitorships recently demonstrates the effect of this sea change in DOJ policy, even prior to the DOJ’s release of the Benczkowski Memorandum. In an October 12, 2018 speech at New York University School of Law, Assistant Attorney General Benczkowski noted that, over the past five years, approximately one in three corporate resolutions included a monitor provision.<sup>12</sup> As recently as 2016, nine of the fifteen FCPA resolutions published by the DOJ, or 60%, resulted in

<sup>6</sup> Benczkowski Memorandum, at 1-2.

<sup>7</sup> *Id.* at 2.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> Assistant Attorney General Brian A. Benczkowski Delivers Remarks at NYU School of Law Program on Corporate Compliance and Enforcement Conference on Achieving Effective Compliance (Oct. 12, 2018), available at <https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-nyuschool-law-program>.

a monitorship.<sup>13</sup> 2018, however, told a different story – there were six corporate FCPA resolutions with the DOJ and only one resulted in a monitor.<sup>14</sup> The DOJ has not announced any FCPA resolutions since the release of the Benczkowski Memorandum, but the guidance contained in the Memorandum suggests that this downward trend should continue into 2019 and beyond.

As to the scope of corporate monitorships, it remains to be seen what the “appropriately tailored” guidance contained in the Benczkowski Memorandum will mean in practice. DOJ resolutions historically often contained broadly worded monitor provisions. For example, as recently as April 2018, the DOJ deferred prosecution agreements established corporate monitors whose mandate was to evaluate “the effectiveness of the internal accounting controls, record-keeping, and financial reporting policies and procedures of the Company as they relate to the Company’s current and ongoing compliance with the FCPA and other applicable anti-corruption laws”<sup>15</sup> – a broad mandate across all business lines, all geographies, and all types of potentially corrupt conduct. Some DOJ monitor requirements have been more narrowly tailored, requiring monitors to employ a “risk-based approach” that would appear to achieve the same tailoring directed in the Benczkowski Memorandum. For example, the Panasonic Avionics DPA quoted above also contained the following directive:

*The Monitor’s reviews should use a risk-based approach, and thus, the Monitor is not expected to conduct a comprehensive review of all business lines, all business activities, or all markets. In carrying out*

*the Mandate, the Monitor should consider, for instance, risks presented by: (a) the countries and industries in which the Company operates; (b) current and future business opportunities and transactions; (c) current and potential business partners, including third parties and joint ventures, and the business rationale for such relationships; (d) the Company’s gift, travel and entertainment interactions with foreign officials; and (e) the Company’s involvement with foreign officials, including the amount of foreign government regulation and oversight of the Company, such as licensing and permitting, and the Company’s exposure to customs and immigration issues in conducting its business affairs.*<sup>16</sup>

The broad, blunder-buss monitor mandate should be the rare occurrence in light of the Benczkowski Memorandum, and those monitorships that are required should look to risk-based approaches to narrow the scope of the monitor’s review.

### *Will the SEC follow suit?*

By its terms, the Benczkowski Memorandum’s application is limited to the DOJ’s Criminal Division attorneys.<sup>17</sup> So what about the SEC? There are at least three signs that point to the SEC following the DOJ’s example.

First, because the DOJ and the SEC have concurrent jurisdiction over FCPA enforcement, they often jointly investigate potential violations and often coordinate the resolution of those matters. For example, the DOJ and the SEC regularly coordinate on monetary sanctions to avoid penalizing a company twice,<sup>18</sup> and on the imposition of a

<sup>13</sup> United States Department of Justice, Related Enforcement Actions: 2016, available at <https://www.justice.gov/criminal-fraud/case/related-enforcement-actions/2016>.

<sup>14</sup> United States Department of Justice, Related Enforcement Actions: 2018, available at <https://www.justice.gov/criminal-fraud/case/related-enforcement-actions/2018>; see *United States v. Panasonic Avionics Corp.*, Case No. 18-CR-00118-RBW (D.D.C. Apr. 30, 2018), ECF No. 2-1 (Deferred Prosecution Agreement), available at <https://www.justice.gov/opa/press-release/file/1058466/download>.

<sup>15</sup> See *Panasonic Avionics Corp.*, Case No. 18-CR-00118-RBW (D.D.C. Apr. 30, 2018), ECF No. 2-1 (Deferred Prosecution Agreement), at D-1; see also *United States v. Sociedad Quimica y Minera de Chile, S.A.*, Case No. 17-CR-00013-TSC (D.D.C. Jan. 13, 2017), ECF No. 2 (Deferred Prosecution Agreement), at D-4.

<sup>16</sup> *Panasonic Avionics Corp.*, Case No. 18-CR-00118-RBW (D.D.C. Apr. 30, 2018), ECF No. 2-1 (Deferred Prosecution Agreement), at D-3-4.

<sup>17</sup> Benczkowski Memorandum, at n.1.

<sup>18</sup> See, eg, *In the Matter of Credit Suisse Group, AG*, Exchange Act Release No. 83593, at 15 (July 5, 2018), available at <https://www.sec.gov/litigation/admin/2018/34-83593.pdf> (“Respondent acknowledges that the Commission is not imposing a civil penalty based upon the imposition of a USD47m criminal fine as part of Credit Suisse’s settlement with the United States Department of Justice.”). In May 2018, Deputy Attorney General Rod Rosenstein announced a new DOJ policy on coordinating corporate resolutions that directs DOJ attorneys to “endeavor, as appropriate, to coordinate with and consider the amount of fines, penalties, and/or forfeiture paid to other federal, state, local, or foreign enforcement authorities that are seeking to resolve a case with a company for the same misconduct.” *Justice Manual*, Department of Justice (2018), § 1-12.100, Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct, available at <https://www.justice.gov/jm/jm-1-12000-coordination-parallel-criminal-civil-regulatory-and-administrative-proceedings>.

single corporate monitor that reports to both agencies.<sup>19</sup> In light of this coordination, it seems likely that the SEC will approach corporate monitorships in a manner consistent with the Benczkowski Memorandum.

Second, the only guidance the SEC has provided on its use of monitors in FCPA settlements was co-published with the DOJ.<sup>20</sup> In 2012, the DOJ and the SEC published a joint resource guide to provide companies with insight into how both agencies approach FCPA enforcement.<sup>21</sup> Notably, the resource guide contains a list of “Factors DOJ and SEC Consider When Determining Whether a Compliance Monitor Is Appropriate.”<sup>22</sup> Since the only guidance provided by the SEC was published jointly with the DOJ and suggests that both agencies use the same factors to determine whether to impose a monitor, it seems likely that the SEC will follow the DOJ’s new guidance going forward.

Finally, a survey of SEC FCPA resolutions over the last five years suggests that like the DOJ, the SEC is also limiting its use of monitorships. In 2018, the SEC sanctioned only one corporate defendant with a monitor despite twelve corporate FCPA resolutions over the course of the year.<sup>23</sup> This trend suggests a more restrained approach to monitorships by the SEC in line with the Benczkowski Memorandum.

### *Practical tips for companies negotiating an FCPA settlement*

Companies facing an FCPA investigation should start remedial measures as soon as possible, with an eye towards having a full remediation plan executed by the time of resolution, in order to avoid or limit the scope of a monitor. And they should use the Benczkowski Memorandum in negotiations regarding the existence or scope of a monitor.

While a company has no control over most of the drivers of an FCPA settlement, it can control its response to the problem through remediation. The Benczkowski Memorandum recognizes that “[w]here a corporation’s compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will likely not be necessary.”<sup>24</sup> Companies should therefore commit as early as possible to remediating any control deficiencies that contributed to the misconduct at issue in the investigation. Remediation of the type necessary to avoid a monitor takes time, and aspirational, untested programs will be much less useful in negotiations or in keeping the company out of further difficulties than fully built solutions. While the attributes of an effective compliance program are beyond the scope of this article, companies should look to the DOJ’s FCPA Corporate Enforcement Policy<sup>25</sup> and Evaluation of Corporate Compliance Programs<sup>26</sup> to guide their remedial efforts.

19 *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, by the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission (**FCPA Resource Guide**) at 72, available at <https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf>.

20 *Id.* at 4.

21 See “SEC and Justice Department Release FCPA Guide,” Nov. 14, 2012, available at <https://www.sec.gov/news/press-release/2012-2012-225.htm>.

22 FCPA Resource Guide, at 71.

23 *In the Matter of Stryker Corp.*, Exchange Act Release No. 84308, at 9 (Sept. 28, 2018), available at <https://www.sec.gov/litigation/admin/2018/34-84308.pdf>.

24 Benczkowski Memorandum, at 2.

25 *Justice Manual*, Department of Justice (2018), § 9-47.120, FCPA Corporate Enforcement Policy, available at <https://www.justice.gov/criminal-fraud/file/838416/download>.

26 Evaluation of Corporate Compliance Programs (February 2017), Department of Justice, Fraud Section, available at <https://www.justice.gov/criminal-fraud/page/file/937501/download>.

Where a monitor will be required, companies should rely on the Benczkowski Memorandum to narrow the scope of their obligations as much as possible. A monitor's typical mandate is to reduce the risk of recurrence by evaluating a company's ongoing compliance with the FCPA and other anti-corruption laws.<sup>27</sup> Where a monitor is not required, the DOJ and the SEC both frequently include self-reporting undertakings in their corporate FCPA resolutions. A standard self-reporting undertaking might require a company to report to the DOJ or the SEC on the "status of Respondent's remediation and implementation of compliance measures"<sup>28</sup> or "its [FCPA] and anti-corruption-related remediation efforts to date."<sup>29</sup> In addition, companies ordered to self-report typically are required to disclose credible evidence of corrupt payments or false books and records.<sup>30</sup> The language of monitor and self-reporting provisions often is broader than the underlying misconduct that prompted the FCPA resolution, and, in that respect, is inconsistent with DOJ guidance contained in the Morford Memorandum and the Benczkowski Memorandum. For example, a pharmaceutical company that made improper payments to doctors at state-owned hospitals in South America might have a monitor that is authorized to review its M&A due diligence practices in Eastern Europe or its gifts and entertainment practices in China.

The SEC has agreed previously to narrow the scope of a self-reporting undertaking to align with the scope of the company's underlying misconduct. In a settlement with Kinross Gold Corporation, a Canadian mining company with operations in North America, South America, West Africa and Russia, the SEC's administrative order described internal control failures that led to questionable payments to vendors and third party consultants in West Africa.<sup>31</sup> Despite Kinross Gold's operations in multiple regions around the world, the administrative order's self-reporting undertaking was expressly limited to the company's operations in West Africa.<sup>32</sup>

Whether a company is negotiating a monitorship or a self-reporting undertaking, the new DOJ guidance released in the Benczkowski Memorandum signals a more nuanced approach to such provisions. At the very least, companies should be able to use this guidance to narrow the scope of a monitorship or self-reporting undertaking so that their obligations are tailored to the particular facts and circumstances of their case and no broader than necessary to reduce the risk of recurrence.

27 See *Panasonic Aviation and Sociedad Quimica y Minera de Chile* deferred prosecution agreements, *supra* note 15.

28 *In the Matter of General Cable Corp.*, Exchange Act Release No. 79703, at 12 (Dec. 29, 2016), available at <https://www.sec.gov/litigation/admin/2016/34-79703.pdf>; see also *Legg Mason, Inc. Non-Prosecution Agreement* (June 4, 2018), available at <https://www.justice.gov/opa/press-release/file/1068036/download>, at C-1.

29 *In the Matter of Sanofi*, Exchange Act Release No. 84017, at 7 (Sept. 4, 2018), available at <https://www.sec.gov/litigation/admin/2018/34-84017.pdf>.

30 *Id.* at 8; see also *In the Matter of JPMorgan Chase & Co.*, Exchange Act Release No. 79335, at 24 (Nov. 17, 2016), available at <https://www.sec.gov/litigation/admin/2016/34-79335.pdf>.

31 *In the Matter of Kinross Gold Corp.*, Exchange Act Release No. 82946, at 3-7 (March 26, 2018), available at <https://www.sec.gov/litigation/admin/2018/34-82946.pdf>.

32 *Id.* at 9.

# U.S. Appeals Court Narrows FCPA's Extraterritorial Reach But Beware – Enforcement Risk Remains

In a rare case of jurisdictional interpretation of the FCPA, 2018 saw the U.S. Court of Appeals for the Second Circuit narrow the circumstances in which a non-U.S. person or company may be prosecuted under the statute. In *United States v. Hoskins*, the Court ruled that the general criminal statutes regarding conspiracy and complicity cannot be used to extend the FCPA's jurisdiction to a non-U.S. person.

Relying on the FCPA's text and legislative history, the Court found that the statute was cautiously designed to limit the FCPA's extraterritorial reach. Further, the Court relied upon a 2016 U.S. Supreme Court case on extraterritoriality in declining to extend the FCPA's reach abroad, as U.S. law "governs domestically, but does not rule the world." This follows a series of recent Supreme Court cases relying upon the presumption against extraterritoriality to reject claims brought against foreign nationals for conduct occurring abroad in connection with other federal statutes.

- The DOJ and SEC have jurisdiction under the FCPA only over the following persons and conduct:
- U.S. citizens, U.S. nationals, U.S. residents, and U.S. companies (**domestic concerns**), regardless of whether the conduct is domestic or abroad;
- U.S. and non-U.S. companies with securities listed on a U.S. exchange and that have periodic reporting obligations to the SEC (**issuers**), regardless of whether the conduct is domestic or abroad;
- Agents, employees, officers, directors, and shareholders of U.S. companies or issuers, when they act on the company's behalf, regardless of whether the conduct is domestic or abroad; and
- Foreign persons (foreign nationals and companies) who violate the FCPA while present in the United States.

The Court dismissed the government's argument that non-U.S. persons who do not act while in the United States could be prosecuted if they met the requirements for accessorial liability, i.e. conspiring to violate the FCPA, or aiding and abetting a FCPA violation.

It also rejected the prosecutorial practice of asserting jurisdiction over foreign conduct by non-U.S. persons for conspiring with, or helping, a person otherwise within the FCPA's reach to violate the statute.

However, in our view *Hoskins* is unlikely to alter the pattern of FCPA enforcement against non-U.S. companies as it does not foreclose prosecution of non-U.S. persons who act as agents of U.S. companies or issuers, regardless of where the conduct occurs. Furthermore, in light of the increased enforcement by non-U.S. regulators of anti-corruption laws and cooperation among global anti-corruption enforcement agencies, multinational companies should continue efforts to prevent, detect, and remediate potential bribery-related conduct wherever it occurs.

## *Foreign Corrupt Practices Act*

The FCPA, which prohibits making improper payments to foreign public officials for a business benefit or advantage, has been a top enforcement priority of the DOJ and SEC. Since the FCPA's enactment, the SEC and DOJ have collectively brought over 540 FCPA actions. Approximately 180 of those enforcement actions were targeted at foreign companies and nationals, including in circumstances where little or no relevant conduct occurred in the United States.

The jurisdictional reach of the FCPA has not been without controversy. One of the more controversial jurisdictional theories advocated by U.S. prosecutors is that accessorial liability may be applied over a non-U.S. person who would not otherwise be subject to the FCPA.



In 2012, for example, a Japanese company, Marubeni Corporation, paid the DOJ over USD54 million in criminal penalties to resolve FCPA charges in circumstances where there was no jurisdiction absent accessorial liability. The allegations related to bribes paid by a joint venture in Nigeria, which was created for the purpose of bidding on and, if successful, designing and building a liquefied natural gas plant. The relevant conduct did not occur in the United States, but one of the joint venture partners was a U.S. company. The DOJ asserted jurisdiction over Marubeni and the Japanese sales agent through whom bribes were funnelled, on the basis that they had aided and conspired to violate the FCPA with a domestic concern. The DOJ's enforcement action against Marubeni resulted in a deferred prosecution agreement, in which Marubeni agreed to pay criminal penalties and to hire an independent monitor.

Because such cases are often resolved by settlement, the jurisdictional theories pursued by the enforcement agencies are rarely subject to judicial scrutiny.

### *U.S. v Hoskins*

In *Hoskins*, the DOJ alleged that Lawrence Hoskins, a citizen of the United Kingdom, employed by a British subsidiary of a French parent company, was allegedly involved in a scheme to pay bribes to Indonesian public officials for the U.S. subsidiary to win a USD118 million government contract in Indonesia. It was alleged that Hoskins approved the selection of and payments to third party consultants retained to pay the bribes. Hoskins was not an employee of the U.S. subsidiary and never travelled to the U.S. while the bribery scheme was ongoing—his closest geographic connection was that he called and emailed U.S.-based co-conspirators while they were in the United States.

The charges against Hoskins included that he acted as an agent of the U.S. company in effectuating the bribery scheme and that independent of his agency relationship, he conspired with the U.S. company, its employees, and foreign persons to violate the FCPA, and aided and abetted their

violations of the FCPA. These charges rely on independent criminal statutes for aiding and abetting the commission of illegal acts by another, and conspiring with another to commit an offense.

The narrow question on appeal was whether Hoskins could be charged for conspiring to violate the FCPA or aiding and abetting others' alleged FCPA violations where there was no jurisdictional nexus over his actions. The Court affirmed the district court's decision to dismiss those claims, relying in the first instance on the text of the statute, which "defined precisely" the categories of persons who may be charged for violating its provisions and states clearly the extent of its extraterritorial application. The Court left intact the possibility that Hoskins may still be convicted for violating the FCPA if the government can prove that he acted as an agent of the American company.

In addition to considering the text of the statute, the Court examined the statute's legislative history and found that Congress's choice to define precisely the persons covered by the FCPA was in contrast to an earlier draft that primarily relied upon conspiracy and complicity theories of liability. Further, the Court found that Congress narrowly circumscribed the FCPA's application to foreign nationals acting within the United States out of concern to take a "delicate touch where extraterritorial conduct and foreign nationals were concerned."

The Court also relied upon the presumption against extraterritorial application. Even if it could be argued that the text and legislative history were not clear that the FCPA's reach over foreign nationals was limited, the Court rejected the government's position as it would "transform the FCPA into a law that purports to rule the world." The Court found that the extraterritorial application of the ancillary offenses of aiding and abetting and conspiracy should be coterminous with the underlying criminal statute.

The Court's rejection of expansive interpretations of the conspiracy and complicity statutes as applied to the FCPA was at least in part due to a recognition of those laws' potential for overreach, noting that the conspiracy and complicity statutes are "among the broadest and most shapeless of American law, and may ensnare persons with only a tenuous connection to a bribery scheme."

Lastly, the Court's ruling is narrow and leaves open the possibility that *Hoskins* could be found liable under the FCPA if he acted as an agent of the U.S. company. The Court found that such an interpretation is squarely within the confines of the statute, consistent with legislative history, and there is no extraterritorial application that arises if *Hoskins* were an agent of the U.S. company acting entirely abroad.

In a concurring opinion, Circuit Judge Gerard E. Lynch noted that leaving intact the agency theory of jurisdiction while eliminating the reliance on accessory liability claims creates a perverse result – a foreign national who is an agent of a U.S. company may be found liable under the FCPA, but a foreign national who is the mastermind of the bribery scheme or directs a U.S. person to pay a bribe in a foreign jurisdiction may not be if none of the foreign national's actions occur in the U.S.

### *Implications*

*Hoskins* is unlikely to have a meaningful impact on continued FCPA enforcement against non-U.S. companies and persons.

First, the decision applies narrowly to accessorial liability and the majority of FCPA actions against foreign companies do not rely on accessorial liability as the sole basis for jurisdiction. Typically such cases fall into two categories: (1) actions against non-U.S. companies in overseas joint ventures with a domestic concern or issuer; and (2) actions against non-resident non-U.S. nationals that oversaw or overlooked improper conduct by a U.S. subsidiary, business partner or agent.

Second, the decision leaves intact the FCPA's defined scope of liability for foreign nationals who: (1) act on American soil; (2) are officers, directors, employees or shareholders of U.S. companies; or (3) are agents of U.S. companies.

Third, *Hoskins* does not offer any protection against the growing trend of anti-corruption enforcement by non-U.S. regulators. Foreign regulators are no longer content to allow the U.S. alone to collect large penalties in anti-corruption investigations. In addition, the DOJ and SEC regularly coordinate enforcement efforts with its counterparts in the United Kingdom, France, Germany, Switzerland, the Netherlands, Brazil, and others. In the past 18 months, the DOJ has announced its first coordinated settlements with authorities in France and Singapore. This trend of non-U.S. enforcement and cooperation between regulators is only likely to increase.

In short, although *Hoskins* limits U.S. jurisdiction when relying solely on statutes other than the FCPA, this decision does not alter the corruption risk calculus for companies operating in high risk markets. U.S. and non-U.S. companies should continue to take efforts to detect, prevent, and remediate bribery-related conduct.

# SEC Continues to Leverage Accounting Provisions of the FCPA to Pursue Aggressive Theories of FCPA Liability

In 2018, the SEC continued its practice from recent years of seeking to leverage the accounting provisions of the FCPA to bring enforcement actions predicated upon aggressive theories of FCPA liability that on the face of the publicly available settlement documents bear little to no connection to foreign bribery.

In this article, we will look at two enforcement actions from 2018 in which the SEC did not directly allege specific corrupt payments but instead relied on an apparent breakdown of internal controls or the inadequacies of compliance policies and procedures: Elbit Imaging Ltd<sup>1</sup> (**Elbit**), Kinross Gold Corporation<sup>2</sup> (**Kinross**). We will also look at a third case from 2018, Centrais Eletricas Brasileiras S.A.<sup>3</sup> (**Eletrobras**), which appears to introduce a variation on the themes emerging from Kinross and Elbit.

## *The FCPA's Accounting Provisions*

The FCPA's "accounting provisions" comprised the books-and-records provision and the internal controls provision. The books-and-records provision requires issuers to make and keep accurate books, records and accounts that, in reasonable details, accurately and fairly reflect the issuer's transactions and disposition of assets. The internal controls provision requires issuers to devise and maintain reasonable internal accounting controls aimed at preventing and detecting potential violations of the FCPA. The accounting provisions apply to Issuers and those acting on their behalf.

The accounting provisions are frequently used by regulators, in part because there is no requirement that a false record or deficient control be linked to a bribe. A payment that does not constitute a false record or a deficient control does not have to be linked to a bribe to a foreign government official

under the FCPA's anti-bribery provisions to result in a prosecution under the accounting provisions.

## *Historic practice*

It was historically common for SEC enforcement actions alleging stand-alone books and records and internal controls violations (i.e. without an accompanying FCPA anti-bribery provision violation) to link those violations to language in the SEC order that mentioned a "bribe" or the term "improper payments".<sup>4</sup> The end result of this practice was that the SEC would make a clear link between the *possibility* of improper payments having been made to foreign government officials and the violation of the FCPA's accounting provisions.

From around 2012, however, the SEC began bringing cases that rather than suggesting a link between the possibility of improper payments having been made to foreign government officials and a violation of the FCPA's accounting provisions, instead began mentioning the creation of "heightened" or "significant" risks of bribery as a result of a violation of the FCPA's accounting provisions.<sup>5</sup> That is, SEC orders no longer contained an outright suggestion of bribery or improper payments that was clearly associated with the violation of the accounting provisions.

1 See In the Matter of Elbit Imaging Ltd., Exchange Act Release No. 82849 (March 9, 2018) <https://www.sec.gov/litigation/admin/2018/34-82849.pdf>

2 See In the Matter of Kinross Gold Corporation, Exchange Act Release No. 82946 (March 26, 2018) <https://www.sec.gov/litigation/admin/2018/34-82946.pdf>

3 See In the Matter of Centrais Eletricas Brasileiras S.A., Exchange Act Release No. 84973 (December 26, 2018) <https://www.sec.gov/litigation/admin/2018/34-84973.pdf>

4 See, for example, In the Matter of Diageo plc, Exchange Act Release No. 64978 (July 27, 2011) <https://www.sec.gov/litigation/admin/2011/34-64978.pdf>

5 See, for example, In the Matter of, BHP Billiton Ltd. And BHP Billiton plc, Exchange Act Release No. 74998 (May 20, 2015) <https://www.sec.gov/litigation/admin/2015/34-74998.pdf> and *Securities and Exchange Commission v. Oracle Corp.*, Civil Action No. CV-12-4310 CRB (N.D.Cal. August 16, 2012) <https://www.sec.gov/litigation/complaints/2012/comp-pr2012-158.pdf>

### *SEC's use of the accounting provisions today*

We have now seen a further step in the evolution of the SEC's use of the accounting provisions with a number of very recent settlements finding violations of the books-and-records and internal controls provisions based only on findings that there is "no evidence to suggest" that due diligence was done on third parties, that "there is no documentation or other evidence showing" any services rendered by consultants or third parties, and that an anti-bribery and corruption compliance program was not implemented correctly, or if one was implemented it was not maintained. This most recent series of cases contain no allegations or mention of bribery or risks of bribery.

In the rest of this article, we will look at three examples of such cases brought by the SEC in 2018.

### *Kinross Gold Corporation*

#### **Background**

In 2010, Kinross conducted pre-acquisition FCPA due diligence on two mines it would acquire the same year – one in Mauritania and the other in Ghana. That due diligence found anti-corruption compliance and accounting deficiencies, though nothing in the SEC order suggests those issues resulted in bribes being paid to foreign government officials. Kinross also conducted three post-acquisition FCPA audits in each of the three years after acquiring the two mines. Those audits made findings consistent with the pre-acquisition due diligence. The audits found inadequate internal controls for FCPA compliance purposes, inconsistent adherence to the accounting controls that did exist, and a lack of a meaningful procurement process.

In spite of the pre-closing diligence and the subsequent FCPA audits, Kinross: (i) took three years after acquiring the two mines in 2010 to implement any internal controls or compliance program; (ii) did not remediate the anti-corruption compliance and accounting deficiencies discovered by its own due diligence; and (iii) failed to apply its own internal accounting controls (including bidding procedures and conducting due diligence) when they were eventually implemented in 2013.

It was also noted by the SEC that local management at these two mines either did not respond to the three audits, or said they would respond to the audits and yet did not follow up on each occasion. Senior management is repeatedly mentioned in the SEC order as having (i) "failed to take immediate action" in response to audit findings and finance department concerns; (ii) "fail[ed] to follow through on its commitments" to implement needed remediation; and (iii) "failed to maintain ... internal accounting controls."

As a result of the conduct described above, the SEC brought claims of civil violations of the books and records and internal accounting controls provisions of the FCPA and Kinross was ordered to pay USD950,000 and report on its efforts to improve internal accounting controls for one year.

#### **No bribery alleged in SEC order**

The SEC order does not allege that any of the compliance failures or inadequate accounting controls resulted in bribes to foreign government officials or otherwise resulted in any "improper payments".

Instead, what the SEC has focused on here is numerous internal control failures, without tying those failures to actual or potential bribery of foreign government officials. Those internal control failures included (1) the failing of senior management in not doing what they said they were going to do and responding to internal audit reports that identified internal control failures; (2) failure to implement appropriate internal controls and FCPA compliance program at the

acquisition targets<sup>6</sup>; and (3) failing to follow and maintain internal controls once they were established at the subsidiaries, particularly those regarding the conduct of procurement processes and due diligence on third parties.

What we appear to have with Kinross is FCPA liability being attributed to the parent company based on the inactions of a foreign subsidiary (particularly inactions of senior management) in not implementing appropriate internal controls. Even when those internal controls were implemented, Kinross failed to maintain those internal controls. There is, however, no evidence in the publicly available documents of the *actions* or *inactions* of the foreign subsidiary resulting in bribery of foreign government officials or improper payments.

## *Elbit Imaging Ltd*

### **Background**

Between 2007 and 2012, Elbit and its subsidiary, Plaza Centers NV (**Plaza**), directly and indirectly paid approximately USD27m to third party offshore consultants and sales agents for their apparent services in relation to a real estate development project in Romania and the sale of a large portfolio of real estate assets in the United States.

According to the SEC: (i) there was no evidence to suggest that Elbit or Plaza conducted any due diligence on the consultants and sales agents; (ii) payments were authorized by Plaza's senior management to the consultants and agents even though there was no evidence that the consultants and sales agents had actually provided the contracted services; (iii) payments to the consultants and sales agents were not recorded in a manner that accurately and fairly reflected the nature of the payments in their books and records; and (iv) Elbit failed to devise and maintain internal accounting

controls sufficient to provide reasonable assurances that company funds would only be used as authorised for legitimate corporate purposes.

### **“No evidence” of due diligence conducted or services provided**

Elbit was charged with a violation of the books and records and internal controls provisions based on a finding that “there is no evidence to suggest” that due diligence was done on the consultants and sales agents and that “there is no documentation or other evidence showing” any services rendered by the consultants. The SEC does not make a finding in the publicly available documents that links the lack of evidence of due diligence and lack of evidence of services being provided by the consultants, with a bribe to a foreign government official. Rather, the SEC order vaguely states that “Plaza characterized the payments to the consultants in its books and records as legitimate business expenses for services rendered, when some or all of the funds *may* [emphasis added] have been used to make corrupt payments to Romanian government officials or were embezzled”.

This resolution is a reminder that the SEC will use the civil accounting provisions of the FCPA to bring enforcement actions in situations such as this, even where the evidence might not sustain a charge under the FCPA's anti-bribery provisions. Critically, the Elbit order suggests that failure to conduct due diligence on third parties and failure to keep sufficient records in the presence of red flags are sufficient findings to support an administrative action for violation of the accounting provisions of the FCPA. Again, as opposed to FCPA liability for the actions of a foreign subsidiary, in the case of Elbit, we seem to have liability created for the inactions of a foreign subsidiary.

<sup>6</sup> This is a case that is very similar in many respects to the 2011 Watts Water Technologies case brought by the SEC for violations of the FCPA's accounting provisions. See In the Matter of Watts Water Technologies, Inc. and Leesen Chang, Exchange Act Release No. 65555 (October 13, 2011), <https://www.sec.gov/litigation/admin/2011/34-65555.pdf>. In that case, Watts Water Technologies was found to have violated the FCPA, in part, because of waiting three years to implement Watts Waters FCPA compliance program at a newly acquired Chinese subsidiary. In the three years between closing of the acquisition and implementation of the FCPA compliance program, improper payments were reportedly made by the Chinese subsidiary.

For companies, this settlement highlights several important practical considerations relating to managing third party risk: (1) conducting appropriate risk-based due diligence; (2) making sure you adopt a process to determine whether third parties are being engaged for genuine and needed services; (3) determining whether the contemplated compensation is commensurate with the services to be provided; (4) ensuring that there is sufficient documentation or other evidence that the contracted services were provided; and (5) approving only those invoices for payment based on proof or reliable confirmation of services.

### *Centrais Eletricas Brasileiras S.A.*

#### **Background**

The third case we will look at in this article introduces a variation on the themes of Kinross and Elbit. In the Eletrobras case, according to the publicly available documents relating to the matter Eletrobras appears to have been the victim of a bribery scheme coordinated and run by other companies and now-former Eletrobras executives. And yet the SEC has used the accounting provisions to charge Eletrobras.

Eletrobras, Brazil's state-owned power company and issuer, was charged with violations of the FCPA's accounting provisions based on what appears to be self-dealing by a number of now-former executives. That self-dealing appears to have been of no benefit to Eletrobras or its shareholders.

According to the SEC order, former officers of Eletronuclear, Eletrobras' majority-owned nuclear power generation subsidiary, "used their influence at Eletronuclear" to engage in an illicit bid-rigging and bribery scheme involving the construction of a nuclear power plant (**UTN Angra III**). "The officers also misused their official positions in authorizing unnecessary contractors and inflating the cost of Eletronuclear' infrastructure project." In return, the construction companies involved in the scheme paid the former Eletronuclear officers approximately USD9m.

According to the SEC, Eletronuclear paid invoices related to the inflated contracts in the ordinary course of its business because Eletrobras had failed to devise and maintain a sufficient system of internal accounting controls from 2009 through 2015. The corruption scheme at Eletronuclear "caused misstatements in Eletrobras's books and records because Eletronuclear recorded payments made to UTN Angra III contractors, a percentage of which was used for bribes, as money legitimately spent to acquire and improve assets."

#### **Specific instances of anti-bribery and corruption compliance system weaknesses; no benefits attributed to Eletrobras**

Eletrobras' anti-corruption policies or procedures and accounting controls relied, in part, on "general or boilerplate prohibitions that did not apply to all employees or were ignored." For example, Eletrobras adopted a code of ethics in 2005 but it applied only to the holding company and made no mention of the subsidiaries and special purpose entities.

Further, in 2009, Eletrobras began anti-corruption training for a small number of its workforce. It also approved a code of conduct in 2010 that required all employees, including employees at its subsidiaries, to observe Eletrobras' ethical principles that prohibited, in part, support or contribution to political parties or campaigns for elective office. Nonetheless the SEC order does identify payments made to Brazilian political parties and government officials in violation of the prohibition in the code of conduct, but the payments were made on behalf of the Brazilian construction companies and only partly funded out of the sham invoices and inflated contract prices paid by Eletronuclear. There is no allegation that Eletrobras received an improper benefit as a result of these payments.<sup>7</sup>

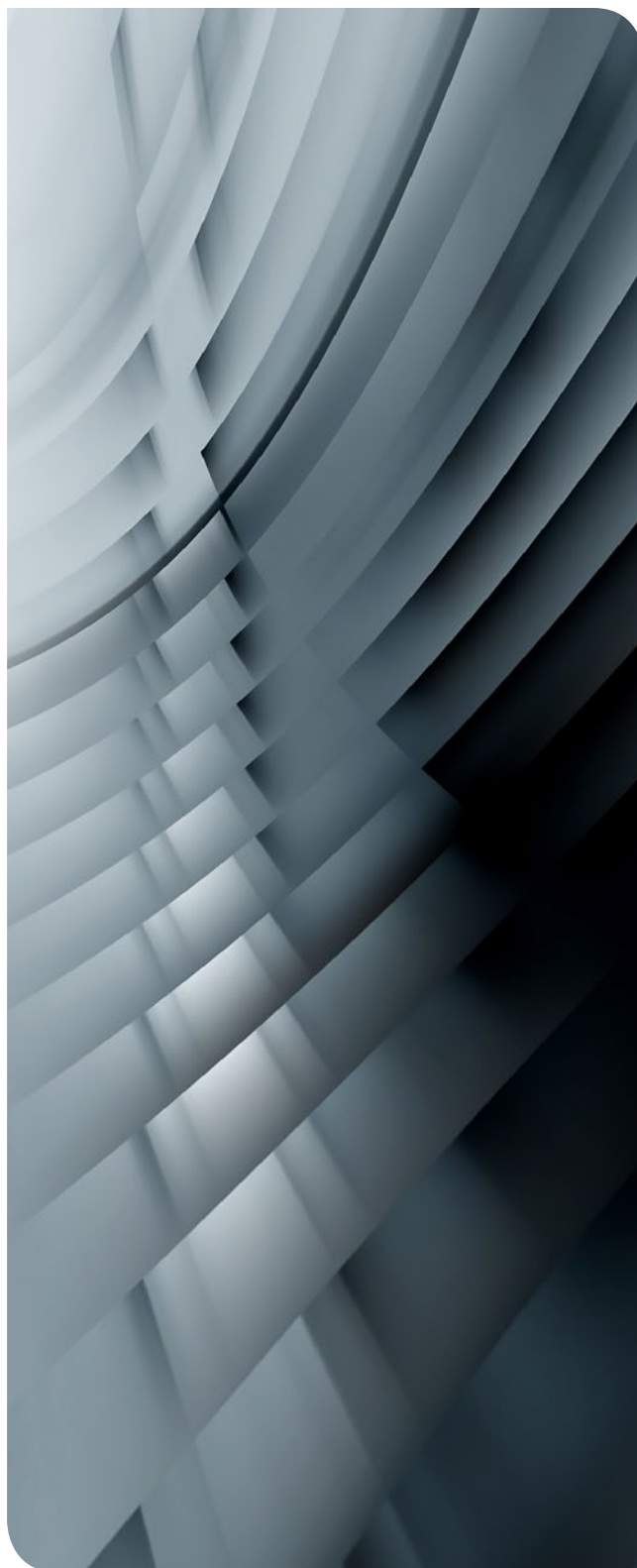
<sup>7</sup> This may also explain why there was no disgorgement ordered as there was no benefit to Eletrobras alleged.

### *Practical Considerations for Issuers Arising Out of these Cases*

The apparent ease with which the SEC has been able to find a violation of the FCPA's books and records and internal controls provisions in recent years demonstrates the potency of the provisions.

These cases also demonstrate the degree to which the SEC will inquire into the minutiae of the anti-bribery and corruption compliance program of a company under investigation for potential violations of the FCPA. For example, errors and oversights in compliance related documentation and failure to maintain or store compliance documentation (e.g. due diligence records), even without corrupt intent, now looks enough to violate the FCPA.

These enforcement actions also serve as a reminder of the importance of designing and implementing an appropriate risk-based anti-bribery and corruption compliance program. Perhaps more importantly, they also remind companies to make sure that their compliance program is regularly reviewed, tested and enhanced in an effort to avoid a compliance program that is out-dated or ill-designed to combat the bribery risks facing the company.



# Practical Steps for Managing FCPA Risk in M&A: Lessons from FCPA Enforcement Actions in 2018

Several FCPA enforcement actions in 2018 highlighted the FCPA risks and common pitfalls associated with companies engaging in corporate activity in high risk jurisdictions and industries.

In this article, we will review two FCPA enforcement actions brought by the SEC which illustrate the challenges and risks associated with: (i) acquiring targets that have been engaged in violations of anti-corruption laws, (ii) ensuring appropriate responses to “red flags” identified during due diligence, and (iii) timely post-closing integration of the target company into the acquiring company’s systems, policies and procedures. The cases discussed in this article reinforce the benefits of an acquiring company having in place a comprehensive due diligence policy and procedure, understanding a target’s potential liability and FCPA risk exposures, taking steps to minimize the identified risk, and integrating the acquired target into your compliance program and policies as soon as practicable post-closing.

## *Dun & Bradstreet Corporation*

### Background

The conduct underlying the Dun & Bradstreet Corporation (**D&B**) FCPA enforcement action<sup>1</sup> concerned two Chinese subsidiaries of D&B who used third party agents to make unlawful payments to obtain data vital to D&B’s business as a provider of business financial information. One subsidiary, part of a joint venture (**HDDB**) with a Chinese company (**Huaxia**), acquired non-public financial statement information on Chinese entities, in violation of Chinese law, by making unlawful payments to Chinese government officials. The second subsidiary (**Roadway**) made improper payments to third parties to acquire non-public personal data in violation of Chinese law that was used in its products and also made improper payments to obtain specific business. These improper payments were falsely recorded as legitimate business expenses.

### The HDDB joint venture

In 2006, D&B’s President of the Asia Pacific region was considering a number of partners to merge with or acquire, ultimately focusing on Huaxia as a joint venture partner. Among other factors, Huaxia was considered attractive to joint venture with as a result of its “government connections.”

D&B had conducted due diligence in anticipation of the joint venture. The due diligence revealed that Huaxia “used its government connections to source financial statement information directly from provincial offices of the Chinese State Administration of Industry and Commerce, [other government agencies], lawyers, and other individuals, rather than publicly available sources” and that it sometimes made payments to Chinese government officials via third party agents to obtain restricted data. According to the SEC order, D&B’s due diligence procedures failed to follow up on the information contained in the due diligence report even though D&B China management was aware of the commercial use restrictions in China on the financial statement information. Instead, D&B provided a short FCPA training session to Huaxia executives and then requested that they complete an anti-bribery questionnaire and certification.

The joint venture between D&B China and Huaxia was completed in November 2006 and resulted in the formation of HDDB. For at least two years after the closing of the deal, HDDB did not fully integrate or consolidate the operations and data acquisition practices of the two predecessor entities, allowing them to continue to operate much as they had. Legacy D&B China continued its normal business operations in Shanghai and legacy Huaxia continued its normal business operations in Beijing. However, a D&B Greater China manager stopped the practice of Huaxia employees directly making improper

<sup>1</sup> See In the Matter of The Dun & Bradstreet Corporation, Exchange Act Release No. 83088 (April 23, 2018) <https://www.sec.gov/litigation/admin/2018/34-83088.pdf>.



payments to AIC officials and implemented the practice of using third party agents to obtain the data.

### Roadway subsidiary

In 2009, D&B acquired a 90% stake in Roadway, a direct marketing services company in China. Businesses used Roadway's services to market directly to businesses or consumers through various media, including direct mail, telemarketing and email.

A key risk identified by D&B in its pre-acquisition due diligence of Roadway related to certain February 2009 amendments to Chinese criminal laws concerning citizens' data privacy. The amendments provided criminal sanctions for entities and individuals who illegally obtain citizens' personal information, through theft or other means, from Chinese government entities or organizations. D&B knew that Roadway had obtained a significant amount of its data from independent vendors, thus it needed to ensure that Roadway had legally obtained its pre-existing data and that Roadway would employ legal means of acquiring data post-acquisition.

However, during negotiations, Roadway said that they could not warrant that no improper payments would be made to obtain citizen data. D&B did not conduct further due diligence to verify whether sales representatives were in fact making improper kickbacks of a portion of commissions in order to secure business, or to determine whether any clients were state-owned or state-controlled entities. Subsequent internal audit reviews after the acquisition failed to detect the improper payments. Improper payments continued to be made post-closing of the transaction.

In 2012, a television news show in China revealed that Roadway sales representatives had made payments to secure information on over 150 million Chinese citizens, and that this information was then sold by Roadway to companies for marketing purposes. This led to a police raid and criminal prosecution of Roadway and five then-current or former employees of Roadway for illegally obtaining private information on Chinese citizens.

### Outcome

The exposure of this issue on Chinese television in 2012 resulted in D&B commencing investigations that led to disclosures being made to the DOJ and SEC. D&B took significant remedial measures, including: shuttering the Roadway subsidiary; discontinuing illicit practices at HDBC; terminating employees who were involved in the misconduct; doubling the size of audit and corporate compliance teams; hiring legal and compliance employees in China; developing and implementing FCPA compliance procedures, including the expansion and implementation of new due diligence and contracting requirements for vendors and suppliers; and taking action against senior executives who had oversight responsibility for ensuring FCPA compliance and adequate training was in place at HDBC and the Roadway subsidiary.

### *Beam, Inc.*

#### Background

From 2006 through 2012, Beam's Indian subsidiary, Beam India, used third party sales promoters and distributors to make improper payments to government employees to increase sales orders, process license and label registrations, and facilitate the distribution of Beam's distilled spirit products. The SEC order stated that the Indian subsidiary reimbursed the third parties for the improper payments through the use of fabricated or inflated invoices, and then falsely recorded the expenses at the subsidiary level. The expenses were then consolidated into Beam's books and records. The SEC's order also found that during this period Beam failed to devise and maintain a sufficient system of internal accounting controls.<sup>2</sup>

<sup>2</sup> See In the Matter of Beam Inc., n/k/a Beam Suntory Inc., Exchange Act Release No. 3944 (July 2, 2018) <https://www.sec.gov/litigation/admin/2018/34-83575.pdf>

### **Beam acquires Indian entity that becomes Beam India; existing management retained**

Beam acquired Beam India in 2006. According to the SEC order, prior to its acquisition by Beam, the Indian entity that subsequently became Beam India regularly made direct and indirect payments to Indian government officials in connection with inspections of the bottling facilities, distribution of its products, label registration and warehouse license applications and renewals, and advantageous product placement and promotion in both government and retail stores. It also made payments to government officials responsible for ordering alcoholic products for distribution in government run retail channels in order to secure and increase sales of spirit products. The Indian management also maintained a second set of financial records that tracked the payments and disguised the schemes in the entity's books and records to make it appear that the illicit payments were legitimate business expenses. There is no suggestion in the SEC order that Beam was aware of these historic issues as a result of the conduct of FCPA due diligence.

When Beam acquired the assets of the Indian entity, it also retained existing management of the entity who knew of and orchestrated the bribe schemes. Those retained managers continued the schemes at Beam India without interruption from the 2006 acquisition through 2012.

After Beam acquired Beam India in 2006, it provided Beam India management with its Code of Conduct manuals and additional compliance training. Beam also instituted annual internal audits starting in 2008.

### **Multiple compliance reviews, audits and investigations by various professional services firms**

Beginning in 2010, Beam engaged a variety of global accounting firms, Indian law firms and U.S. law firms to conduct compliance reviews of Beam India. The first of these reviews in 2010 was conducted by an accounting firm which interviewed Beam India executives and conducted limited transaction testing. That review resulted in a report that stated certain Beam India executives believed that "promoters are likely making grease payments" to

government officials in India and, as a result, recommended that Beam follow up and "conduct and document due diligence to confirm activities undertaken" by third parties, "investigate red flags," "discuss legal considerations of third party actions taken on Beam's behalf," and "consider need to further review" the government-facing businesses. Further reviews by Indian law firms and U.S. law firms involving additional interviews of Beam executives followed, all of which confirmed previously identified issues or identified new issues. Beam did not follow a number of the recommendations provided by both the Indian law firm and the U.S. law firm to follow up on identified issues.

It would only be in 2012, when additional issues were raised internally through an internal whistleblower making allegations that a manager had used false invoices from third parties to generate cash to pay bribes to government officials, that investigations were commenced and disclosures made to the SEC.

### **Outcome**

The SEC order focuses on the failures of Beam to timely remediate deficiencies at its acquired subsidiary in a challenging jurisdiction. The SEC order notes that "red flags" existed from 2010 as a result of advice from a global auditing firm, a U.S. law firm and an Indian law firm to take additional investigative steps, which it did not immediately do.

### *Observations from the D&B and Beam cases*

In respect of HDHC and Roadway, the SEC order emphasizes that D&B did not take steps to respond to the information it obtained during due diligence. Between 2006 and 2012, D&B did not act on information discovered during the Huaxia due diligence, and D&B did not take any steps to investigate further when it was told by Roadway that it could not warrant not making improper payments to obtain citizen data.

In respect of Beam India, the SEC order shows that Beam failed to follow up on "red flags" identified in the post-

closing integration period. While a failure to conduct audits and identify risks can create or exacerbate exposure in itself, the SEC order shows the potential repercussions of identifying red flags through post-closing audits and reviews and then failing to adequately remediate those red flags.

### *What conclusions can we draw from the D&B and Beam cases?*

- U.S. enforcers will bring FCPA charges for the pre- and post-acquisition conduct of a target *and* the conduct of an acquiring company when conducting pre- and post-acquisition assessments of a target.
- Buyers are much better off if they understand the scope of potential liability before the acquisition and take steps to reduce their risk including, potentially, modification of the transaction terms to account for increased risk.
- Post-acquisition reviews are critical to identifying issues that were not identified in pre-acquisition due diligence, particularly if there was limited opportunity for pre-acquisition due diligence beforehand. Such reviews should be thorough and done as quickly as possible.
- Issues identified should be remediated as quickly as possible. If the issues are significant, consider whether there is value in disclosing them to the relevant enforcement agencies.
- Pre-acquisition due diligence and post-acquisition reviews, identification of issues and compliance program implementation should take on heightened urgency where there are recent or known issues.
- For sellers, it is also important to assess the risk profile of the target and the level of interest and exposure of the potential buyer(s). If the seller will be expected to sign anti-corruption-related representations and warranties (or include a closing condition or indemnities), seller due diligence may be appropriate. Sellers may also need to prepare for corruption-related due diligence questions and requests from the buyer. The extent to which sellers can feasibly push back on these depends on the respective leverage of the buyer and seller in the transaction.
- Obtain as much publicly available information as necessary. Engaging a third party due diligence provider can streamline information gathering.
- Work with your financial/tax due diligence advisers to look for relevant information in the accounts of the target (for example, cash payments, gift and hospitality accounts, miscellaneous or poorly described accounts, large payments to agents and payments to individuals). Include anti-corruption questions in the due diligence requests.
- Use the information you find to strategize on next steps, whether it is further due diligence, discussions with the seller or tailored provisions in the transaction documents. Where possible, continue to conduct due diligence following signing and before closing.
- Develop a detailed plan for post-acquisition review and integration. Engaging and instructing service providers prior to closing will facilitate the review following the acquisition. This step takes on heightened importance if pre-acquisition due diligence is limited due to the nature of the transaction (for example, where the transaction is hostile or subject to a competitive tender process which may limit due diligence and leverage in negotiating transaction terms).
- Implement the post-acquisition review as soon as possible after closing.

### *What are some practical actions for planning for and conducting due diligence?*

- For buyers, understand the risk profile of the target as much as possible before starting pre-acquisition due diligence and then develop an initial plan for due diligence. Modify the due diligence plan to respond to information as it becomes known.

# Overview of the SEC's Whistleblower Program in 2018

## *Record-breaking whistleblower awards in 2018*

The U.S. Securities and Exchange Commission's whistleblower program (**Program**) enjoyed a record-breaking year in 2018, with the SEC ordering its largest whistleblower awards to date. The Program rewards those who submit tips related to violations of U.S. federal securities laws, including the FCPA. In March 2018, the Program saw three individuals receive awards totaling USD83m. Over the course of 2018, 13 individuals received a combined total of USD168m in the form of rewards for whistleblower information. These figures are indicative of an upward trend in both the number and size of awards made under the Program. By comparison, since the inception of the Program, the SEC has awarded approximately USD326 million to 59 individuals.

## *Increasing number of whistleblower tips*

The SEC received over 5,200 whistleblower tips in FY 2018, the highest increase in tips since the Program's commencement in 2010. In six years, the number of whistleblower tips received by the SEC has grown by approximately 76%. Of the tips received, 202 were FCPA-related tips from whistleblowers in 2018 which amounted to almost 4% of all tips received by the SEC for that year. The 2018 figure represents a marginal decline in the number of FCPA-related tips from the 210 in 2017. It is one of only two categories of tips that saw a decline in the number of tips received in comparison to 2017.

Outside of the United States, the SEC received the highest number of whistleblower tips (including FCPA-related tips) this past fiscal year from individuals in Canada, the United Kingdom and Australia. From the APAC region approximately 175 tips were received by the SEC with 45 coming from Australia, 40 from China and 26 from India. This figure puts it ahead of both the Americas and Africa from which 46 and 28 tips originated. The top foreign jurisdictions for those two regions were Brazil with 19 tips

and South Africa with 14. Meanwhile in Europe, individuals from the United Kingdom provided 85 tips to the SEC, with the next highest being Germany which submitted 29 tips, followed by Spain and Russia. In total, 263 tips were received by the SEC from individuals in Europe.

## *Proposed whistleblower rule amendments*

Proposed whistleblower rule amendments intended to increase efficiencies in the claims review process and provide additional tools in award determinations have been introduced, and are currently being considered. The proposed amendments will allow the SEC to prevent individuals from submitting whistleblower applications when they previously submitted false information, or made frivolous award claims, to the SEC. Additionally, the proposal will allow the SEC to order awards based on deferred prosecution agreements and non-prosecution agreements.

## *Who is a "whistleblower"?*

A recent Supreme Court ruling will also require rule amendments to provide that an employee must report possible securities law violations to the SEC to qualify for protection against retaliation.<sup>1</sup>

On February 21, 2018, the U.S. Supreme Court unanimously held in *Digital Realty Trust, Inc. v. Somers* that the anti-retaliation provision of the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111-203) covers only those who report an alleged violation of the federal securities laws to the SEC. The Court's decision reversed a Ninth Circuit ruling that Dodd-Frank's anti-retaliation provision also covers employees who report such issues internally without reporting them to the SEC.

The holding in *Digital Realty* has been interpreted by some as suggesting a future where potential whistleblower's bypass internal reporting channels and go directly to the SEC to ensure they are protected.

<sup>1</sup> *Digital Realty Trust, Inc. v. Somers* 138 S. Ct. 767 (2018).

# FCPA-related Policy Developments in 2018

In 2018, the United States Department of Justice made a number of changes to aspects of its enforcement policy – particularly FCPA enforcement policy – relating to corporate entities. Many of these changes reflect an incremental expansion of the FCPA Corporate Enforcement Policy that was announced in late 2017 and address some of the key aspects of corporate enforcement: voluntary disclosure, cooperation, monitors, and international coordination. The practical effect of these changes will depend in large part on how they are applied over time, but as a general matter the changes that have been introduced seem intended to reduce the burden of corporate investigations and some of the more stringent requirements of previous policies to qualify for cooperation credit.

This article looks at each of these policy announcements and initiatives in turn, beginning with a brief reminder of the FCPA Corporate Enforcement Policy announced in late 2017.

## *FCPA Corporate Enforcement Policy*

In November 2017, the DOJ announced a revised FCPA Corporate Enforcement Policy.<sup>1</sup> The FCPA Corporate Enforcement Policy was an outgrowth of the Pilot Program that had been initiated under the previous administration in 2016 and formally incorporated into the U.S. Attorneys' Manual (which was renamed the Justice Manual in September 2018<sup>2</sup>).

The FCPA Corporate Enforcement Policy offers the possibility of corporate declinations from prosecution as an incentive for self-disclosure and cooperation by companies during FCPA investigations. According to the policy, there will be a presumption of corporate declination if three prerequisites are met: full and timely voluntary self-disclosure to the DOJ; full cooperation (including as to all facts relevant to the culpability of individual employees); and timely and appropriate remediation (including implementation of an effective compliance and ethics program and appropriate discipline of employees).<sup>3</sup>

In March 2018, DOJ announced that it would begin using its FCPA Policy as “nonbinding guidance” in all Criminal Division corporate matters, not just those involving violations of the FCPA.

## *“No piling on” policy*

In May 2018, the DOJ announced its “Policy on Coordination of Corporation Resolution Penalties,” also known as the “no piling on” policy.<sup>4</sup> In describing the new policy, Deputy Attorney General Rod Rosenstein stated that “[i]t is important for us to be aggressive in pursuing wrongdoers. But we should discourage disproportionate enforcement of laws by multiple authorities. In football, the term ‘piling on’ refers to a player jumping on a pile of other players after the opponent is already tackled. Our new policy discourages “piling on” by instructing Department components to appropriately coordinate with one another and with other enforcement agencies in imposing multiple penalties on a company in relation to investigations of the same misconduct.”<sup>5</sup>

1 Department of Justice, 9-47.120 – FCPA Corporate Enforcement Policy, (Apr. 5, 2016) <https://www.justice.gov/criminal-fraud/file/838416/download>

2 <https://www.justice.gov/opa/pr/departments-justice-announces-rollout-updated-united-states-attorneys-manual>

3 <https://www.justice.gov/criminal-fraud/file/838416/download>

4 Memorandum from Rod J. Rosenstein, Deputy Attorney Gen., to Heads of Department Components, United States Attorneys (May 9, 2018) <https://www.justice.gov/opa/speech/file/1061186/download>

5 Deputy Attorney General Rod Rosenstein Delivers Remarks to the New York City Bar White Collar Crime Institute, New York, NY, Wednesday, May 9, 2018 (<https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar>)

The policy encourages DOJ prosecutors to “consider the totality of fines, penalties, and/or forfeiture imposed by all Department components as well as other law enforcement agencies and regulators (both in the United States and in other countries) in an effort to achieve an equitable result.”<sup>6</sup> In essence, the policy requires DOJ prosecutors to coordinate and not unduly “pile on” penalties, including with regard to penalties that will be imposed by foreign law enforcement for the same conduct being investigated by the DOJ.

### *Extension of the FCPA Corporate Enforcement Policy to M&A*

In a further incremental expansion of the DOJ’s application of its FCPA Corporate Enforcement Policy, a July 25, 2018 speech before ACI’s Global Forum on Anti-Corruption Compliance in High Risk Markets, Deputy Assistant Attorney General Matthew S. Miner announced that the DOJ will “look to” the principles of the FCPA Corporate Enforcement Policy in evaluating “other types of potential wrongdoing, not just FCPA violations” that are uncovered in connection with mergers and acquisitions.<sup>7</sup> As a result, when an acquiring company identifies misconduct through pre-transaction due diligence or post-transaction integration, and then self-reports the relevant conduct, DOJ is now more likely to decline to prosecute if the company fully cooperates, remediates in a complete and timely fashion, and disgorges any ill-gotten gains.

Miner acknowledged that in the area of FCPA risk and M&A transactions the DOJ could do better to avoid the uncertainty and inconsistency created by current policy statements. In particular, the 2012 Resource Guide states under the heading “M&A Risk-Based FCPA Due Diligence and Disclosure” that “DOJ ... will give meaningful credit to

companies who undertake these actions, and, in appropriate circumstances, DOJ ... *may* [emphasis added] consequently decline to bring enforcement actions.”<sup>8</sup> This appears inconsistent with the FCPA Corporate Enforcement Policy which offers a presumption of corporate declination if three prerequisites are met. Miner said he understood that acquiring companies want greater clarity as to how DOJ will exercise its discretion to decline prosecution following the discovery of an FCPA issue related to M&A activity. He added that his understanding was that the phrase “*may ... decline*” is a significant sticking point for corporate management in deciding how to proceed in the M&A context. Miner went on to say that the DOJ “intends to apply the principles contained in the FCPA Corporate Enforcement Policy to successor companies that uncover wrongdoing in connection with mergers and acquisitions and thereafter disclose that wrongdoing and provide cooperation, consistent with the terms of the Policy.”

Above all, Miner’s comments appear designed to encourage companies with robust compliance and due diligence programs to enter high risk markets and industries. He described the benefits of having an acquiring company with robust compliance systems entering a high risk market or industry and being in a position to “right the ship” by applying strong compliance practices to an acquired company which does not have the same compliance standards. That is, the specter of FCPA enforcement activity should not be a factor that impedes corporate transactions by good corporate actors.

Two months later, at a Global Investigations Review (GIR) Live event, Miner expanded his comments to make clear that they apply to “other types of potential wrongdoing, not just FCPA violations,” unearthed in connection with merger and acquisition activity that is disclosed to DOJ.<sup>9</sup>

6 Memorandum from Rod J. Rosenstein, Deputy Attorney Gen., to Heads of Dep’t Components, United States Attorneys (May 9, 2018) <https://www.justice.gov/opa/speech/file/1061186/download>

7 Deputy Assistant Attorney General Matthew S. Miner Remarks at the American Conference Institute 9th Global Forum on Anti-Corruption Compliance in High Risk Markets, Wednesday, July 25, 2018, <https://www.justice.gov/opa/pr/deputy-assistant-attorney-general-matthew-s-miner-remarks-american-conference-institute-9th>

8 United States Department of Justice and United States Securities & Exchange Commission, A Resource Guide to the U.S. Foreign Corrupt Practices Act (November, 2012) at 29, <https://www.justice.gov/criminal-fraud/fcpa-guidance>

9 Deputy Assistant Attorney General Matthew S. Miner of the Justice Department’s Criminal Division Delivers Remarks at the 5th Annual GIR New York Live Event, New York, NY, Thursday, September 27, 2018 <https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-justice-department-s-criminal-division>

### *Additional guidance regarding selection of monitors in Criminal Division matters*

In October 2018, Assistant Attorney General Brian Benczkowski issued a memorandum on the “Selection of Monitors in Criminal Division Matters”<sup>10</sup> (**Benczkowski Memo**) which had the stated purpose of establishing standards, policy, and procedures for the selection of monitors in matters being handled by Criminal Division attorneys. The memorandum supplements existing guidance provided by the memorandum entitled, “Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations,” issued by then-Acting Deputy Attorney General, Craig S. Morford (**Morford Memorandum**).

The Benczkowski Memo states that prosecutors should consider both “potential benefits” to imposing a monitor as well as “potential costs”. It formalizes many of the DOJ’s long-standing practices with respect to the evaluation of the appropriateness of imposing a monitor as part of a corporate disposition based on a number of factors, such as a company’s corporate compliance program at the time of a resolution, the financial costs of a monitor to a company, and any unnecessary burdens to a company’s operations.

Of particular interest to companies, the Benczkowski Memo emphasizes that a company’s remediation efforts in responding to FCPA or other issues being investigated, including reviewing and enhancing compliance policies and programs, may negate the need to impose an independent monitor. The Benczkowski Memo states that “[i]n general, the Criminal Division should favor the imposition of a monitor only where there is a demonstrated need for, and clear benefit to be derived from, a monitorship relative to the projected costs and burdens. Where a corporation’s compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will likely not be necessary.” This appears to be another example of the DOJ looking to

incentivize companies to respond to potential corporate wrongdoing with root-cause analyses and assessments of the adequacy of a company’s existing compliance program and policies.

On a related point, one day after issuing the Benczkowski Memo, Assistant Attorney General Benczkowski delivered remarks at a conference in New York where he discussed the importance of assessing compliance in every corporate enforcement matter before the Criminal Division.<sup>11</sup> Previously, the Criminal Division had hired a single compliance counsel who was housed in the Fraud Section and assisted prosecutors, but Benczkowski stated that there were inherent limitations in having the locus of the DOJ’s compliance expertise consolidated in a single person in a single litigating section. Going forward, the DOJ intends to build upon compliance capacity, expertise and knowledge across every section in the Criminal Division that requires it, starting with the Fraud Section and the Money Laundering and Asset Recovery Section, where the bulk of the Criminal Division’s corporate enforcement activity takes place. The DOJ intends to accomplish this through a combination of hiring and the development of targeted training programs, so that attorneys will be able to bring compliance expertise to the table, not just experience as prosecutors and in the courtroom.

### *“China Initiative” announced promising to investigate and prosecute Chinese companies*

We have separately addressed this initiative in this update, but in brief, on November 1, 2018, then-Attorney General Jeff Sessions announced the United States Department of Justice’s “China Initiative” with the objective of countering perceived national security threats to the United States from China. The initiative promises to investigate and prosecute Chinese companies aggressively for alleged trade secret theft, espionage, FCPA offenses and other violations of U.S. law.

<sup>10</sup> Memorandum from Brian A. Benczkowski, Assistant Attorney Gen. (Oct. 11, 2018) <https://www.justice.gov/opa/speech/file/1100531/download>

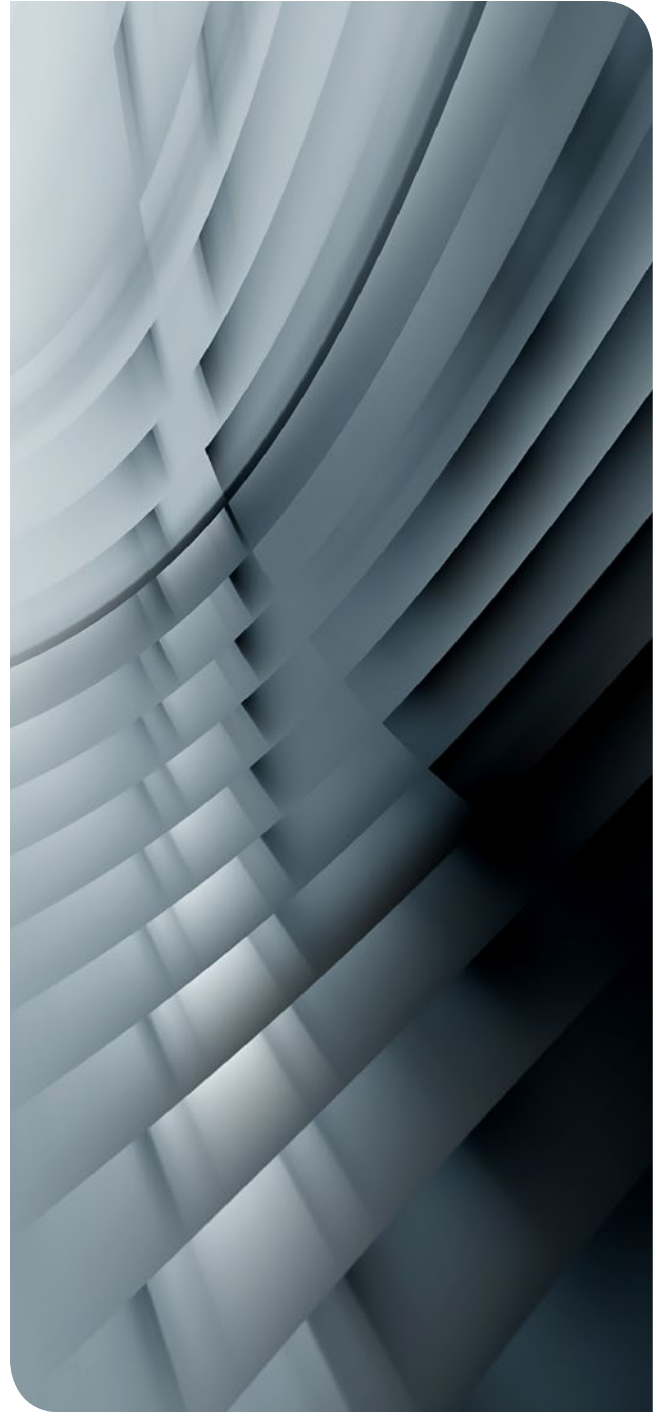
<sup>11</sup> Assistant Attorney General Brian A. Benczkowski Delivers Remarks at NYU School of Law Program on Corporate Compliance and Enforcement Conference on Achieving Effective Compliance, New York, NY, Friday, October 12, 2018, <https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-nyu-school-law-program>

### *Standards for receiving cooperation credit*

Most recently, Deputy Attorney General Rod Rosenstein in November 2018 announced a modest change to the “Memorandum on Individual Accountability” (referred to as the Yates Memorandum) and incorporation of the memorandum into the Justice Manual.<sup>12</sup> Specifically, in order for a corporation to receive full credit for cooperating with the DOJ in an investigation, it now does not need to provide information on “all” individuals involved in the misconduct at issue, but instead only information on “all individuals substantially involved in or responsible for the misconduct at issue, regardless of their position, status or seniority, and provide to the Department [of Justice] all relevant facts relating to that misconduct.”<sup>13</sup>

The revised policy also allows for cooperation credit in criminal cases even where a company “is unable to identify all relevant individuals or provide complete factual information despite its good faith efforts to cooperate fully” if it can explain the restrictions it is facing to the prosecutor.

Apart from these changes, the policy continues to prioritize individual accountability for wrongdoing. Rosenstein explained in the speech that “the most effective deterrent to corporate criminal misconduct is identifying and punishing the people who committed the crimes.”



12 Deputy Attorney Gen. Rod J. Rosenstein Delivers Remarks at the Am. Conference Inst. 35th Int'l Conference on Foreign Corrupt Practices Act, Department of Justice (Nov. 29, 2018) <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0>

13 Department of Justice, Justice Manual, 9-28.700, The Value of Cooperation, <https://www.justice.gov/jm/9-28000-principles-federal-prosecution-business-organizations#9-28.700>



# “China Initiative” Announced by DOJ to Investigate and Prosecute Chinese Companies

Against the background of rising trade tensions between the United States and the People’s Republic of China (**China**), on November 1, 2018, then-Attorney General Jeff Sessions announced the U.S. Department of Justice’s “China Initiative” (the **Initiative**).<sup>1</sup> The Initiative is essentially a DOJ enforcement program with the promise of devoting additional resources, and strategic focus, to a number of pre-existing federal enforcement tools with the stated goal of aggressively investigating and prosecuting Chinese companies for alleged trade secret theft, economic espionage, FCPA offenses and other violation of U.S. law. The Initiative reflects the DOJ’s strategic priority of countering perceived Chinese national security threats and which reinforces President Donald Trump’s overall national security strategy.

The enforcement activities anticipated by the Initiative are being coordinated and led by DOJ’s National Security Division, supported by other senior officials from DOJ and the Federal Bureau of Investigation, along with a working group of U.S. attorneys from five different judicial districts.

Among the various strategies announced to carry out the initiative, the Attorney General said that the DOJ will “identify FCPA cases involving Chinese companies that compete with American businesses”. Assistant Attorney General for Criminal Division Brian Benzckowski said in relation to the announcement of the Initiative: “Every day, the Chinese engage in efforts to steal American trade secrets and commit other illegal acts intended to enrich their economy at the expense of American businesses. We know that Chinese companies and individuals also have bribed government officials in other countries in order to win contracts. The Criminal Division is committed to fully enforcing the Foreign Corrupt Practices Act. Bringing these offenders to justice will help create a level playing field for American companies in foreign markets.”

Emphasizing that the Initiative is more than just an FCPA-focused program, the other stated strategies of the Initiative designed to help counter perceived Chinese national security threats, include:

- Identifying priority trade secret theft cases, ensuring that investigations are adequately resourced; and working to bring them to fruition in a timely manner and according to the facts and applicable law;
- Developing an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;
- Educating colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;
- Applying the Foreign Agents Registration Act to unregistered agents seeking to advance China’s political agenda, bringing enforcement actions when appropriate;
- Equipping the nation’s U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;

<sup>1</sup> Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage, Washington, DC, Thursday, November 1, 2018

- Implementing the Foreign Investment Risk Review Modernization Act (**FIRMA**) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);
- Identifying opportunities to better address supply chain threats, especially ones impacting the telecommunications sector, prior to the transition to 5G networks;
- Increasing efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and
- Evaluating whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.

The Initiative is an interesting development because it seems to suggest that the DOJ will focus on the nationality of individuals and companies, rather than wrongful conduct, including when pursuing FCPA enforcement actions. FCPA enforcement against Chinese companies has been quite limited to date.

At the same time, if the FCPA is seen as being used to achieve political objectives, the Chinese government may counter with steps to frustrate DOJ investigations. As we note below in discussing developments in China, in October 2018 China enacted the International Criminal Judicial Assistance Law that could frustrate DOJ investigations.



# In Brief

## *FCPA scrutiny continues for life sciences industry; SEC signals ongoing attention*

In announcing the Sanofi FCPA enforcement action in September 2018, SEC FCPA Unit Chief, Charles Cain stated: “[b]ribery in connection with pharmaceutical sales remains as a significant problem despite numerous prior enforcement actions involving the industry and life sciences more generally. While bribery risk can impact any industry, this matter illustrates that more work needs to be done to address the particular risks posed in the pharmaceutical industry.”

## *Polycom case an important reminder of the FCPA risks associated with non-company email and accounting systems*

The Polycom FCPA enforcement action involved the creation of an off-the-books accounting and recordation system for corrupt payments made by or on behalf of Polycom China. While Polycom had a customer relations management (CRM) database, Polycom China’s senior managers directed Polycom China’s sales personnel to enter details concerning sales opportunities into a separate, parallel sales management system outside of Polycom’s company-approved systems, which was orchestrated by Polycom’s Vice President of China. Polycom personnel outside China were unaware of the existence of this parallel system. Polycom China’s senior managers also directed Polycom China’s sales personnel to use non-Polycom email addresses when discussing deals with Polycom’s distributors.

## *Travel, Entertainment and Hospitality*

In September 2018, United Technologies Corporation agreed to pay USD13.9m to resolve charges that, among other improper conduct, it violated the FCPA as a result of improperly provided trips and gifts to various foreign

government officials from 2009 to 2015 in China, Kuwait, South Korea, Pakistan, Thailand, and Indonesia through its Pratt & Whitney division and Otis subsidiary in order to obtain business.<sup>1</sup> As described in the SEC order, UTC policies required the Legal Department to review and approve all leisure travel and entertainment as gifts to a foreign government official. Nonetheless, employees frequently circumvented this requirement by submitting travel for foreign government officials for approval without disclosing the leisure and entertainment component. On occasion, the travel was included as a cost component in the contract with the end customer and was therefore not submitted for appropriate approval.

It has been some time since a FCPA enforcement action focused entirely or in large part on improper travel, hospitality, entertainment and gifting practices. The case is an important reminder that companies with global operations must implement policies, procedures and internal accounting controls that prevent bribery and motivate employees to perform ethically.

## *Financial hardship being taken into account*

In two FCPA enforcement actions in 2018 we saw the DOJ and SEC take into account the financial condition of a company and its ability to pay. The SEC’s order against Vantage Drilling International notes that “in determining the disgorgement amount and not to impose a penalty, the commission has considered Vantage’s current financial condition and its ability to maintain necessary cash reserves to fund its operations and meet liabilities.”<sup>2</sup> The DOJ’s enforcement action against Transport Logistics International reflected a similar concern as to whether a criminal fine would substantially jeopardize the continued viability of the company.<sup>3</sup>

1 See In the Matter of United Technologies Corporation, Exchange Act Release No. 84087 (September 12, 2018) <https://www.sec.gov/litigation/admin/2018/34-84087.pdf>

2 See In the Matter of Vantage Drilling International, Exchange Act Release No. 84617 (November 19, 2018) <https://www.sec.gov/litigation/admin/2018/34-84617.pdf>

3 See, <https://www.justice.gov/opa/press-release/file/1043221/download>

### *FCPA enforcement against individuals, and the continued rise of related AML enforcement*

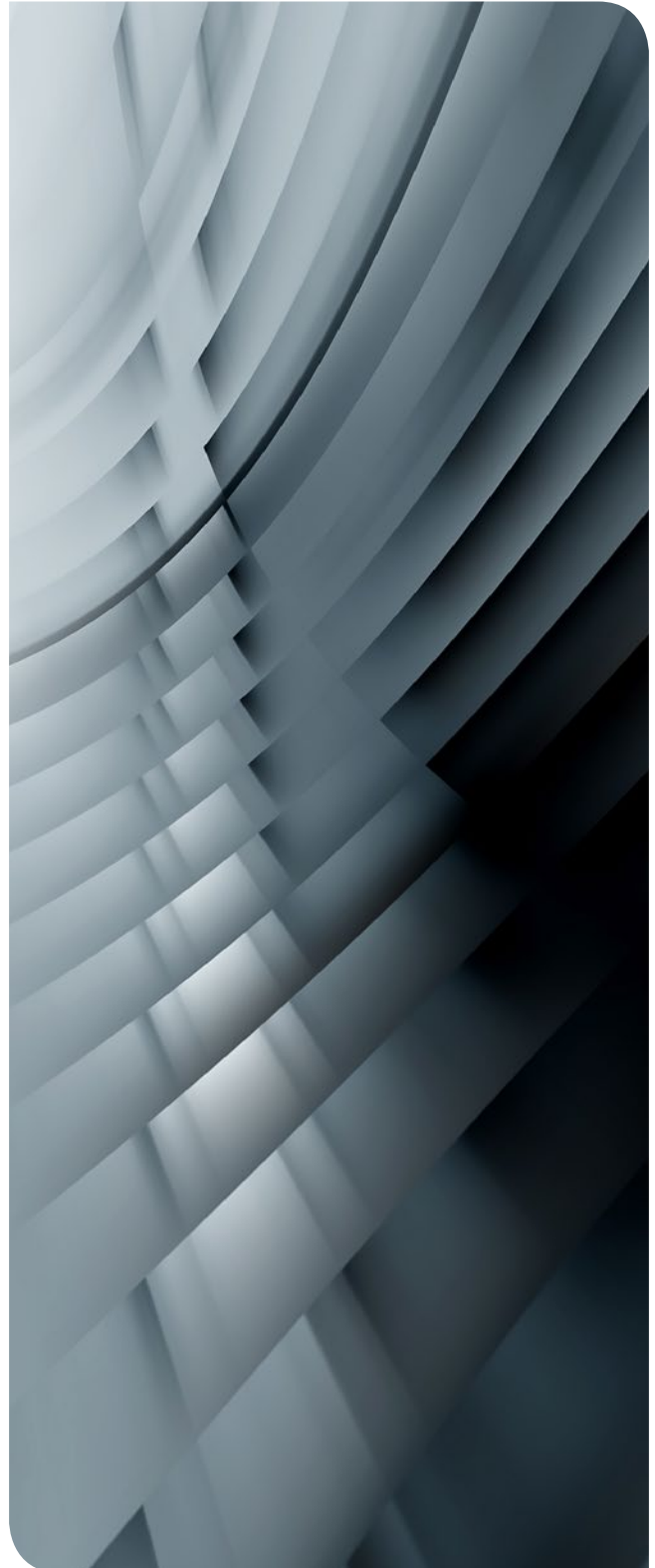
Enforcement against individuals in 2018 for alleged FCPA violations was down from the highs of 2017 but continued to reflect the focus of both the DOJ and SEC on holding individual wrongdoers accountable for their conduct. The DOJ was more active than the SEC, bringing charges against nine individuals versus two by the SEC.<sup>4</sup> Interestingly, only one of the individual enforcement actions brought in 2018 was related to a corporate enforcement action; in prior years this was more often the case. The DOJ also secured guilty pleas against six individuals, and secured two convictions in jury trials for FCPA offenses.

It also needs to be noted that the true extent of FCPA enforcement against individuals cannot be understood by only looking at FCPA-specific charges against individuals. DOJ continued its trend of recent years of bringing non-FCPA criminal charges against individuals—including foreign government officials—under money laundering, wire fraud and Travel Act statutes. These type of charges are largely a result of DOJ pursuing the foreign government official recipients of bribe payments, given that the “demand” side of foreign bribery is not caught by the FCPA. Foreign government officials can be caught by criminal offenses associated with the receipt of those bribes, such as money laundering. The extraterritorial jurisdictional reach of U.S. anti-money laundering statutes is even greater than that of the FCPA.

### *OECD reports on lack of enforcement against bribe takers*

On December 11, 2018, the Organisation for Economic Cooperation and Development (OECD) Working Group on Bribery released a report called “Foreign Bribery Enforcement: What Happens to the Public Officials on the Receiving End?” The report concluded that “[p]ublic officials accepting bribes from OECD-based companies run little risk of being punished” and that there is a lack of international cooperation on the “demand side” of foreign bribery.

<sup>4</sup> Based on publicly filed charging instruments.



Part 2:  
*Anti-corruption*  
*Developments around*  
*the World*

# *Australia*



# Australia's Adoption of New Foreign Bribery Laws and DPA Scheme Stalls in Parliament

In December 2017 the Australian government introduced the *Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2017 (Bill)* into the Senate. The Bill introduced a number of significant changes to the foreign bribery offenses set out in the *Criminal Code Act 1995*. Over a year later, and the Bill is still under legislative consideration in Australia's federal parliament.

We have covered each of the proposed changes in detail in other publications, but each of those pending amendments are briefly discussed below along with several other reforms to Australia's foreign bribery and corporate accountability regime.

## *Failure to prevent bribery offense*

The introduction of a new strict liability corporate offense of "failure to prevent bribery of foreign public officials" is the most significant change in the proposed legislation. Under this "failure to prevent" offense, the Bill imposes criminal liability on a company when a person "associated" with the company pays a bribe intending to obtain or retain business or a business advantage for the entity. The Bill defines associated person broadly to include any person who performs services for or on behalf of the entity, and includes employees, agents (including those operating overseas), and subsidiaries. The offense applies to Australian incorporated corporations as well as foreign corporations operating in Australia.

This new offense will be an "absolute liability" offense that provides for a defense only if the relevant company can demonstrate that it had implemented "adequate procedures" to prevent bribery by associated persons. No guidance has yet been published to explain what "adequate procedures" a company must implement to establish this defense, but we expect such guidance to be released when the proposed changes are enacted and for that guidance to largely reflect the wealth of already available public material – particularly from UK and U.S. authorities – that provides guidance as to the key elements of an anti-bribery and corruption compliance program.

As in a number of other common law jurisdictions that are covered in this update, the overriding purpose of this proposal is to assist in reducing the existing legislative barriers to Australian prosecutors pursuing companies implicated in overseas bribery of public officials – something that to this day has not been possible as

demonstrated by Australia's to-date absent track record of foreign bribery prosecutions.

## *Broadening of the Existing Foreign Bribery Offense*

The Bill also broadens the current existing foreign bribery offense and lowers the bar that must be established for the commission of the offense. It does so by:

- introducing a concept of "improperly influencing" a foreign public official to obtain or retain business or a business advantage. This removes the former requirement that the business advantage not be "legitimately due" to a foreign public official. The existing regime that required the business advantage not be "legitimately due" is inconsistent with the foreign bribery offenses of other countries and has proven challenging for Australian prosecutors, particularly when a payment to a foreign public official is disguised as a "legitimate" business transaction;
- extending the scope of the offense of foreign bribery to include bribery to obtain a personal advantage;
- removing the requirement that the foreign official be influenced in the exercise of their official duties; and
- extending the definition of "foreign public official" to include a candidate for public office.

Importantly, there is no proposal at this stage to remove or amend the facilitation payment defense, which allows payments of minor value to expedite routine government actions.

### *New Deferred Prosecution Agreement Regime*

As a means of encouraging greater self-reporting by companies, the Bill also introduces a Deferred Prosecution Agreement (DPA) regime in Australia. DPAs are a voluntary, negotiated settlement between a prosecutor (in this case, the CDPP) and a defendant, which are designed to encourage greater self-reporting by companies and improve cooperation with ongoing investigations. Importantly, a company will not be prosecuted in relation to matters that were the subject of a DPA where the company fulfills its obligations under the agreement. Under the current proposals, DPAs will only be available to companies (not individuals) and will be available for a range of serious corporate crime offenses including foreign bribery, fraud, false accounting, money laundering and others.

Perfectly timed with the DPA proposal – and also issued in December 2017 – the AFP and CDPP released joint self-reporting guidelines for foreign bribery and related offending by corporations (the **Guidelines**). The Guidelines address the principles and process that the AFP and the CDPP will apply when a corporation self-reports conduct which is believed to be in contravention of the foreign bribery offenses or associated crimes. The AFP must receive a company's self-report before they themselves choose to commence an investigation, or before receiving a referral from a domestic or international agency. The Guidelines seek to incentivize self-reporting by companies by giving them greater clarity on how a report will be handled by the AFP and CDPP and will set expectations for the forthcoming DPA regime.

### *Additional Legal Reforms*

The Bill sits alongside a number of other legislative reforms that have been introduced in recent years in Australia.

### *New Books and Records Offenses*

Before these legislative reforms were introduced, in early 2016, the Australian Government introduced new offenses prohibiting an individual or company from, intentionally or recklessly, making, altering, destroying or concealing an accounting document. The accounting offenses were

intended to address some of the deficiencies in Australia's books and records provisions in the *Corporations Act* which was not adapted to the foreign bribery context. The new books and records offenses introduced in March 2016 have sought to align Australian laws more closely with foreign bribery regulations and enforcement in other jurisdictions such as the United States, where a large proportion of enforcement actions under the FCPA have focused on "books and records" violations, even in the absence of anti-bribery findings.

### *Whistleblower Reforms*

Finally, in December 2017, the Australian Government also introduced the *Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2017 (Whistleblower Bill)* to strengthen whistleblower protections. The Whistleblower Bill proposed the following key reforms:

- introducing new requirements for public and large proprietary companies to implement a clear and accessible internal whistleblower policy;
- allowing anonymous whistleblowing disclosures and making it an offense to disclose a whistleblower's identity or any information that is likely to identify the whistleblower; and
- introducing a reverse onus of proof to make it easier for a whistleblower to seek compensation for loss, damage or injury suffered as a result of whistleblower retaliation.

On December 6, 2018, an amended *Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2017* was published by the Government responding to a number of issues raised during the Parliamentary review process. The Whistleblower Bill will return to the Parliament in early February 2019 for further consideration.

### *What Lies Ahead?*

There is every indication that the Bill will pass in 2019, along with the Whistleblower Bill. With the Australian Government's intensified focus on foreign bribery and domestic corruption, Australian companies and foreign companies operating in Australia can expect to face greater scrutiny.



# Lifting of Suppression Orders Reveals Details of Australia’s Largest Foreign Bribery Case

On November 27, 2018, a former employee of a Reserve Bank of Australia (**RBA**) subsidiary, Securrency International Pty Ltd (**Securrency**), pleaded guilty to conspiring to bribe foreign public officials. As a result of the former employee – Christian Boillot – being the last accused to have their case dealt with, suppression orders that were sought and granted in 2011 by the co-accused in the case to protect their fair trials were lifted, permitting the publication of details of the judgments and sentences from Australia’s first foreign bribery prosecution after seven years of suppression orders around the case being in place.

## *Background*

Securrency produces polymer substrate, upon which Note Printing Australia Pty Ltd (**NPA**) prints banknotes. Securrency and NPA were both subsidiaries of the RBA (Australia’s central bank equivalent to the U.S. Federal Reserve). The RBA sold its 50% stake in polymer banknote maker Securrency. It still owns and controls NPA.

In 2009, the Australian Federal Police (**AFP**) commenced an investigation into allegations of bribery of foreign public officials by Securrency and NPA and several employees and agents of the companies to obtain banknote contracts in Malaysia, Nepal, Indonesia and Vietnam. The alleged conduct occurred from the late 1990s through to the early 2000s.

In July 2011, the Commonwealth Director of Public Prosecutions (**CDPP**) commenced criminal prosecutions against Securrency and NPA, together with several executives, alleging that they engaged in a conspiracy to bribe foreign public officials in several countries in order to secure valuable and profitable banknote printing contracts for central banks around the world, facilitated by various third party agents and intermediaries.

## *Securrency and NPA*

In October 2011, Securrency and NPA each pleaded guilty to three charges of conspiracy to commit foreign bribery. Securrency’s offending occurred in Indonesia, Malaysia and Vietnam. NPA’s offending occurred in Indonesia, Malaysia and Nepal. In July 2012, Securrency was sentenced to fines totalling AUD480,000 and NPA was sentenced to fines totalling AUD450,000. These sentences in 2012 were the first in Australia to enforce its foreign bribery offenses under Division 70 of the Criminal Code Act (1995). The fines would have been more substantial were it not for both companies pleading guilty and undertaking to cooperate with the authorities in relation to the prosecutions of their employees and agents.<sup>1</sup>

Interestingly, the Court noted in sentencing that (at [57]) “the fact that Securrency and Note Printing were both subsidiaries of Australia’s central bank (which plays an important role in relation to national monetary policy, financial stability and the issuing of banknotes), means that their actions had the capacity to harm the reputation of the Reserve Bank itself, and of broader Australian interests. That does make the offending more serious than if they had been commercial entities with no such connection.”

<sup>1</sup> See, *CDPP v Note Printing Australia Limited & Anor* (Ruling on agreed facts document related to the companies’ sentence) [2012] VSC 304 (17 July 2012) (see, <http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VSC/2012/304.html>), and *CDPP v Note Printing Australia Limited & Anor* (Sentence) [2012] VSC 302 (17 July 2012) (see, <http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VSC/2012/302.html>).

Securrency and NPA cooperated in a proceeds of crime application pursuant to the *Proceeds of Crime Act 2002* (Cth) that was brought as a result of the successful company prosecutions. The companies paid a combined total of AUD21,666,482 in pecuniary penalty orders. The pecuniary penalties against NPA and Securrency are the largest ever ordered in Australia.

### *John Ellery*

On July 18, 2012, John Ellery, the former Chief Financial Officer and company secretary of Securrency, pleaded guilty to a charge of false accounting in relation to a payment of commission made to the Malaysian agent and falsely described as marketing and other expenses.<sup>2</sup> Mr Ellery cooperated with authorities, pleaded guilty at the earliest opportunity and his remorse was considered genuine. He was sentenced to six months' imprisonment, with the term suspended for a period of two years. Were it not for his plea of guilty, he would have been sentenced to one year's imprisonment with a non-parole period of nine months.

### *Radius Christanto*

On September 30, 2013, Radius Christanto, the Indonesian agent for Securrency, pleaded guilty to conspiracy to bribe foreign public officials in Indonesia. He was sentenced to two year's imprisonment, and was released to be of good behavior for two years. The sentencing judge took into account 42 days' imprisonment that Mr Christanto served in Singapore prior to his extradition to Australia, his early plea of guilty and associated remorse and extensive cooperation that he undertook to provide to Australian authorities.<sup>3</sup> Had Mr Christanto not pleaded guilty or offered future cooperation, he would have been sentenced to five years imprisonment, with a minimum non-parole period of three years' and four months.

In sentencing Mr Christanto, the Court made some interesting observations around the cultural context in

which the bribes were paid in Indonesia (at [31]) “[y]our original agreement with Securrency and its employees, and most of your activities in relation to the promotion of polymer banknotes, occurred prior to the introduction of the foreign bribery provisions. What had previously been legal suddenly became illegal on 17 December 1999. Your actions also occurred in a cultural context, in your own country, in which the payment of bribes in order to secure business was a commonplace occurrence. I accept that you were not aware that your activities after December 1999 might involve a breach of Australian law. Although ignorance of the law is not a defense, in sentencing you I have borne in mind the rather unusual circumstances of your offending.” It is unlikely that this unusual reference to cultural context will be relevant today given the number of jurisdictions enacting anti-bribery and corruption laws and increasing enforcement in this area that is discussed throughout this update.

### *Myles Curtis*

On October 10, 2017, Myles Curtis, Securrency's former Chief Executive Officer and general manager, pleaded guilty to conspiracy to bribe foreign public officials in Indonesia and Malaysia, and to false accounting for a payment of commission made to the Malaysian agent and falsely described as marketing and other expenses. On the conspiracy to bribe foreign public officials charge, Mr Curtis was sentenced to two years and six months' imprisonment, but released to be of good behavior for two years and six months.<sup>4</sup>

On the false accounting charge, Mr Curtis was sentenced to six month's imprisonment, wholly suspended for one year. Were it not for his plea of guilty, he would have been sentenced to three years' imprisonment with a non-parole period of two years on the conspiracy charge, and one year imprisonment with a six-month non-parole period on the false accounting charge.

2 *CDPP v Ellery* [2012] VSC 349 (20 August 2012) (<http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/vic/VSC/2012/349.html>).

3 *CDPP v Radius Christanto* [2013] VSC 521 (<http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VSC/2013/521.html>).

4 *CDPP v Curtis* [2017] VSC 613 (17 October 2017) (<http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VSC/2017/613.html>).

### *Clifford Gerathy*

On May 30, 2018, Clifford Gerathy, the former senior business development manager of Securrency, pleaded guilty to false accounting for the payment of commission made to the Malaysia agent and falsely described as marketing and other expenses. He was sentenced to three months' imprisonment, wholly suspended for six months.<sup>5</sup> If he had not pleaded guilty, he would have been sentenced to four months' immediate imprisonment.

### *Christian Boillot*

On November 27, 2018, Christian Boillot, a former banknote specialist of Securrency, pleaded guilty to conspiracy to bribe foreign public officials in Malaysia. He was sentenced to two and a half years' imprisonment, but released to be of good behavior for two years. Were it not for his plea of guilty, he would have been sentenced to three years' imprisonment with a minimum non-parole period of two years. Mr Boillot had been held in prison for 84 days in Germany and Australia following his arrest in 2011 and had remained in Australia on bail since September 2011.

In sentencing Mr Boillot, Justice Hollingworth of the Supreme Court of Victoria noted the significant adverse effects that the foreign bribery offenses have had on two whistleblowers, Mr Brian Hood and Mr James Shelton. Her Honor remarked that 'Mr Hood and Mr Shelton had both showed tremendous courage in raising their concerns about foreign bribery activities with appropriate people'. Her Honor further remarked that 'the various foreign bribery court proceedings have lasted for many years longer than anyone might have anticipated, without there having been any public acknowledgement of the very important role played by [Mr] Brian Hood and [Mr] James Shelton in exposing what happened within Securrency and NPA'.

### *Other controversies*

So prominent were some of the alleged overseas targets of the Securrency and NPA bribery scheme that the Commonwealth of Australia Department of Foreign Affairs and Trade (equivalent to the U.S. Department of State) successfully sought a suppression order on the identities of the foreign politicians and officials associated with the case. They included prominent figures with connections to overseas prime ministers and presidents, as well as the former Indonesian president Susilo Bambang Yudhoyono (even though there was no suggestion he was involved in the wrongdoing). Malaysian Ex prime minister Najib Razak was also implicated.

<sup>5</sup> *CDPP v Gerathy* [2018] VSC 289 (1 June 2018) ([http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VSC/2018/289.html?context=1;query=cdpp%20v%20gerathy;mask\\_path=au/cases/vic/VSC](http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VSC/2018/289.html?context=1;query=cdpp%20v%20gerathy;mask_path=au/cases/vic/VSC)).

# Proposed Establishment of a Commonwealth Integrity Commission

On December 13, 2018 the Australian Government announced its intention to create a Commonwealth Integrity Commission (CIC), a central body responsible for the prevention and investigation of corruption in the public sector. The announcement was accompanied by a detailed proposal that addresses many of the issues explored in the September 2017 Senate Committee Report on the same issue. However, the Government has also established an expert panel to consult further on the proposed legislation, indicating that any legislation is unlikely to be passed before the next Federal election.

The proposed Commission will have two divisions, a 'law enforcement integrity' division and a 'public sector integrity' division. Each division will have at its helm a deputy commissioner, with a Commonwealth Integrity Commissioner overseeing both.

## *Law Enforcement Integrity Division*

The proposed law enforcement division reconstitutes the existing Australian Commission for Law Enforcement Integrity (ACLEI) and will investigate "corruption issues"<sup>1</sup> in law enforcement agencies. The most significant change to this division is an expanded responsibility to investigate employees of several additional government agencies.<sup>2</sup> There is also a suggestion that the division will be given greater funding and resources than previously available to the ACLEI.

## *Public Integrity Division*

Of greater interest is the proposed public integrity division. This division will have a broad jurisdiction to investigate "corrupt conduct" by:

- parliamentarians, their departments and staff;
- statutory agencies and public service departments;
- Commonwealth companies;
- Commonwealth service providers and subcontractors engaged by them; and

- any person who receives and deals with Commonwealth funds "to the extent that their suspected corrupt conduct intersects with a public official's suspected corrupt conduct".

The definition of "corrupt conduct" will be limited to a set of existing criminal offenses, including abuse of public office, misuse of official information and non-impartial exercise of official functions. It is proposed that these offenses will be collected into a new, separate division of the Commonwealth Criminal Code (Code). The Government is also consulting on potential new offenses that could be added to the new division. The new offenses proposed are:

- repeated public sector corruption, which would apply where a person has committed three or more offenses falling within the new division of the Code;
- corrupt conduct by a senior official, which would apply where a person is a member of the Senior Executive Service (or equivalent) or an appointed agency head, and that person uses their position, influence, resources or knowledge as such to commit an offense;
- a failure to report public sector corruption, which will apply to senior public service officials at a public agency that:

<sup>1</sup> As that term is defined in s 7 of the *Law Enforcement Integrity Commissioner Act 2006* (Cth).

<sup>2</sup> Australian Securities and Investments Commission, Australian Prudential Regulatory Authority, the Australian Competition and Consumer Commission, the Australian Taxation Office and the remainder of the staff of the Department of Agriculture and Water Resources.

- have information that would lead a reasonable person to believe an employee of that agency has committed an offense within the new division of the Code; and
- do not take reasonable steps to arrange for the conduct to be reported to the appropriate authority.

Conduct not falling within the new division of the Code will be referred to either the Australian Federal Police (**AFP**) or the relevant agency. Limiting the investigative jurisdiction of the public integrity division to the investigation of particular criminal offenses will avoid the issues that arose from the ambiguous legislation that established the New South Wales Independent Commission Against Corruption (**NSW ICAC**).<sup>3</sup>

### *Investigative Powers*

The law enforcement division will have the same powers of the ACLEI, namely powers to:

- compel the production of documents;
- hold public or private hearings, and compel a person to give evidence at those hearings;
- make arrests, enter and search premises, and seize evidence; and
- undertake “controlled operations” and integrity testing.

The public integrity division will have only some of these powers but, notably, will be able to:

- compel the production of documents;
- hold private hearings and compel a person to give evidence at those hearings; and
- enter and search premises.

The power to compel a person to give evidence at a hearing is significant as it is not currently available to the AFP.

Indeed, the AFP’s inability to conduct compulsory examinations has, in at least one case, resulted in it enlisting the assistance of the Australian Crime Commission<sup>4</sup> to conduct an examination on the AFP’s behalf. This practice was recently condemned by the High Court of Australia.<sup>5</sup>

Having observed the practice of anti-corruption commissions established in several States, the Australian Government has proposed that the public integrity division will not have the power to conduct public hearings or make “findings” of corrupt conduct. The CIC will instead be an investigator that will refer matters to the Commonwealth Director of Public Prosecutions, who will decide whether to prosecute.

There has already been criticism of the proposal not to empower the public integrity division to conduct public hearings, with the suggestion that this would create one set of rules for law enforcement officers and another for politicians and public servants. However, it is not apparent that the power to hold public hearings has been used by the ACLEI to date. In the ACLEI’s 2013-14 Annual Report, the Integrity Commissioner noted that the ACLEI had conducted 111 hearings from January 2007 to 30 June 2014, all of which were held in private.<sup>6</sup> The Government has justified its approach on the basis that state-based integrity bodies, such as the NSW ICAC, “have proved to be ‘kangaroo courts’[,] falling victim to poor process and being little more than a forum for self-serving mud slinging and the pursuit of personal, corporate and political vendettas”.

<sup>3</sup> See, for example, *ICAC v Cunneen* [2015] HCA 14.

<sup>4</sup> Now called the Australian Criminal Intelligence Commission.

<sup>5</sup> *Tony Strickland (a pseudonym) v Commonwealth Director of Public Prosecutions* [2018] HCA 53.

<sup>6</sup> The ACLEI’s website states that 85 hearings have been held since that time, but does not indicate whether they were in public or private, or provide any other information in relation to investigations that

### *Other Features*

The CIC will not only be an investigator of criminal conduct. It will also:

- act as a public corruption data center, conducting analysis of corruption trends and supporting integrity strengthening efforts across government, including policy advice on proposed legislation;
- provide training and support to public agencies to assist with preventing or reducing corruption through improvements in agencies' internal controls.

It will undoubtedly interact with a number of existing agencies, including the Fraud and Anti-Corruption Centre, the Australian Public Service Commission and the Commonwealth Ombudsman, however the detail of its interaction and cooperation is still to be determined.

### *What To Expect*

Given the substantial political pressure to establish a national integrity commission, it can be expected that the Government's proposal represents a minimum set of likely features that a future CIC will have. The Government has estimated that the CIC should be given an annual budget of approximately AUD30m per year, which is over 2.5 times the current funding of the ACLEI. While sufficient for conducting investigations into the conduct of individuals and small corporations, the CIC may struggle in earlier years with achieving the resourcing required to conduct large-scale investigations into major corporates.

The public support that was generated by the high-profile hearings conducted by the NSW ICAC and the Royal Commission into Misconduct in the Financial Services Industry suggest that it is possible that this Government, or a Government established after the next election (if different), may amend the current proposal to give the public integrity division the power to hold public hearings. Those commissions have appeared to produce significant cultural change in their respective sectors. However, there have been a number of individuals whose conduct has been viewed by many as unfairly the subject of extreme public criticism arising from the intense media scrutiny accompanying those public hearings, particularly those whose conduct was ultimately not criticized in final or interim reports prepared by those commissions.

Nonetheless, the now complete political support for the establishment of a CIC will, together with other pending changes to anti-bribery and corporate crime legislation, lift the temperature for domestic and international companies, particularly those providing services to the Commonwealth.

# Brazil



# Brazil: Developments and Trends in Anti-bribery & Corruption

## *Introduction*

Brazil has been the stage for one of the largest white collar criminal investigations in Latin America. Initially focused on dismantling a money laundering scheme run from a car wash in Brasília, in “Operação Lava Jato” or “Operation Car Wash,” the Brazilian Federal Police unveiled during its investigation evidence of a much larger scheme involving the state-controlled oil company Petrobras. In this scheme, high-ranking executives of Petrobras allegedly received bribes in exchange for awarding large construction contracts. Operation Car Wash, which is still ongoing, has revealed the cover up of other related industries and jurisdictions, and exposed a far-reaching network of corruption and public agents involved.

Operation Car Wash has deeply affected the Brazilian heavy construction market, the oil and gas and offshore drilling industries, and how Brazilian companies generally operate. Changes in the political landscape also had an impact on public contractors and companies operating in other regulated markets. Companies in an array of sectors took measures ranging from enhancing and enforcing (or, in some instances, devising from scratch) internal anti-bribery and corruption controls, to ousting employees involved in corruption scandals. Operation Car Wash put to the test not only Brazilian anti-bribery and corruption laws, but also new investigation and enforcement tools and procedures available to the Brazilian Federal Police and federal prosecutors.

## *Cooperation with Foreign Authorities*

In Operation Car Wash, the Brazilian and Swiss authorities have worked closely to gather and exchange critical information on Swiss bank accounts held by individuals and entities under investigation in Brazil. Such accounts, as reported by Swiss financial institutions, were used for laundering money paid in exchange for the fraudulent award of construction contracts by Petrobras.

A number of large investigations against corporations triggered by Operation Car Wash became global investigations based on inside information provided by

participants in the scheme, prompting foreign authorities to take action.

Cooperation between Brazilian and foreign authorities resulted in significant financial penalties for those companies:

### **Embraer S.A.**

Brazilian and foreign authorities worked together in the investigations of bribery allegations concerning wrongful dealings by the Brazilian aircraft manufacturer Embraer S.A. in the Dominican Republic, India, Mozambique, and Saudi Arabia. The global investigation resulted in a payment of a total of USD205m to the DOJ, the SEC, and the Brazilian authorities.

### **Odebrecht S.A. and Braskem S.A.**

An estimated USD788m in bribes were paid by the Brazilian conglomerate Odebrecht S.A. and its subsidiary Braskem S.A. in more than ten countries (ending in a settlement of USD3.5bn payable to the DOJ, and credited to Swiss and Brazilian authorities).

### **Rolls-Royce PLC**

Bribes paid by the British engine manufacturer Rolls-Royce plc in eight countries (including Brazil, where a Petrobras long-term employee told Brazilian authorities he personally received approximately USD200,000 from Rolls-Royce, giving rise to an international investigation) from 1989 to 2013 ended in a global settlement of USD800m involving the DOJ, the Serious Fraud Office in the United Kingdom, and Brazilian authorities.

### **SBM Offshore N.V.**

Bribes in an aggregate amount of nearly USD16m paid in Angola, Brazil, Equatorial Guinea, Kazakhstan and Iraq by the Dutch oil drilling manufacturer SBM Offshore N.V. resulted in a global settlement of USD820 involving the DOJ, Brazilian, and Dutch authorities.

### **Keppel Offshore and Marine Ltd.**

Bribes of more than USD70m paid over the course of approximately 14 years by the Singaporean shipyard



operator Keppel Offshore and Marine Ltd. to Brazilian politicians and individuals affiliated with Petrobras resulted in a USD422m global settlement (involving American, Brazilian and Singaporean authorities).

These are also good examples of Brazil's anti-corruption law long-arm statute, and how Brazilian authorities may thereunder prosecute and effectively sanction companies for corrupt practices conducted abroad. While developing countries are usually more prone to taking the back seat in high profile cross-border investigations as providers of information to agencies and governmental authorities of more developed countries, Brazilian enforcement authorities have been acting as both providers (as in the Embraer and Odebrecht cases) and recipients (as in the Odebrecht, Rolls-Royce, SBM and Keppel cases), taking on relevant investigative duties, negotiating with companies and sometimes sharing in the monetary proceeds of settlements and convictions.

### *Internal Cooperation and Leniency Agreements*

In addition to pursuing closer ties with foreign entities, certain Brazilian authorities – namely the Attorney General of Brazil (**AGU**), the Ministry of Transparency and Comptroller General of Brazil (**CGU**), the Federal Audit Court (**TCU**) and the Federal Public Prosecutor's Office (**MPF**) – noticeably enhanced internal cooperation among themselves. This contributed to the strengthening of a novel and somewhat controversial tool in the anti-bribery and corruption enforcement practice in Brazil, the so-called “leniency agreements.” Similarly to Deferred Prosecution Agreements under U.S. law, Brazilian leniency agreements allow companies to voluntarily disclose relevant information with respect to wrongdoings in exchange for more “lenient” sanctions.

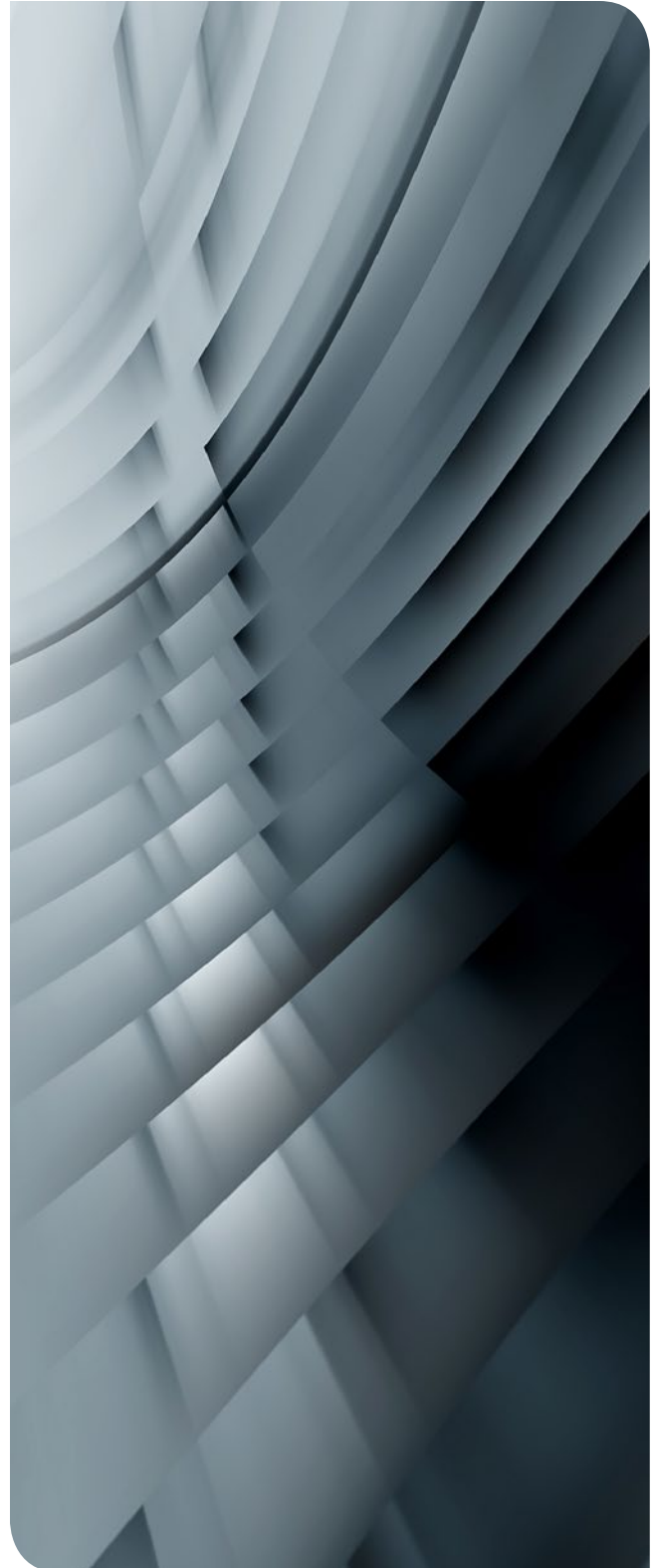
The SBM Offshore leniency agreement negotiations illustrate the challenges that Brazilian authorities have been facing in implementing leniency agreements. In July 2016, SBM Offshore entered into a leniency agreement with the AGU, the CGU, the MPF and Petrobras to settle allegations that SBM Offshore had bribed Petrobras officials. However, in a complex post-signing approval process required by Brazilian law, involving multiple reviewing bodies, the July 2016 leniency agreement was eventually rejected by a reviewing chamber within the MPF. It took the parties over two years to redesign the agreement, which ultimately was divided in two: one agreement among SBM Offshore, the AGU, the CGU and Petrobras (announced in July 2017, subject to review and approval by the TCU) and one agreement between SBM Offshore and the MPF only (announced in September 2018).

The difficulties faced by the parties to SBM Offshore leniency agreements and other proceedings in terms of sharing confidential information and settling conflicting interests called for urgent cooperation between the authorities. Efforts by the MPF and the TCU led to the signing of a “Technical Cooperation and Mutual Assistance Agreement” in June 2018, aiming at facilitating the exchange of information between the authorities and regulating audits and reviewing procedures. As a result, risks of conflicting reviews and approval decisions in respect of new leniency agreements can be credibly expected to decline, motivating companies to pursue leniency agreements as a safe means to settle allegations of bribery and related unlawful activities. In the wake of these developments, a number of other companies are said to be in talks with investigation and enforcement authorities to enter into leniency agreements regarding alleged wrongdoings.

### *Conclusion*

The unprecedented cooperation that the Brazilian authorities exhibited in Operation Car Wash is likely to continue in new investigations and may well serve as an example for other countries. As authorities and individuals in charge of conducting investigations and enforcement proceedings learn from their current practice and cooperation with foreign counterparts, anti-bribery and corruption probes are very likely to continue in the infrastructure industry, and to surge in other sectors of high public interest such as healthcare and financial services.

On another note, President-elect Jair Bolsonaro recently announced that he will appoint Judge Sergio Moro as Brazil's next Justice Minister, an appointment that Mr Moro publicly accepted. Mr Moro presided over many of the most important judicial proceedings in Operation Car Wash and is considered a strong voice against bribery and corrupt practices. Whether the next Brazilian government will interfere with ongoing and prospective investigations and enforcement practices, however, is yet to be seen.



# *Canada*



# Canadian Remediation Agreement Regime Takes Effect

In 2018, Canada introduced its form of a DPA regime known as the Remediation Agreement Regime (**RAR**). The RAR came into effect on September 19, 2018. A remediation agreement is defined in its implementing legislation as “an agreement, between an organization accused of having committed [certain economic] offence[s] and a prosecutor, to stay any proceedings related to that offence if the organization complies with the terms of the agreement.”

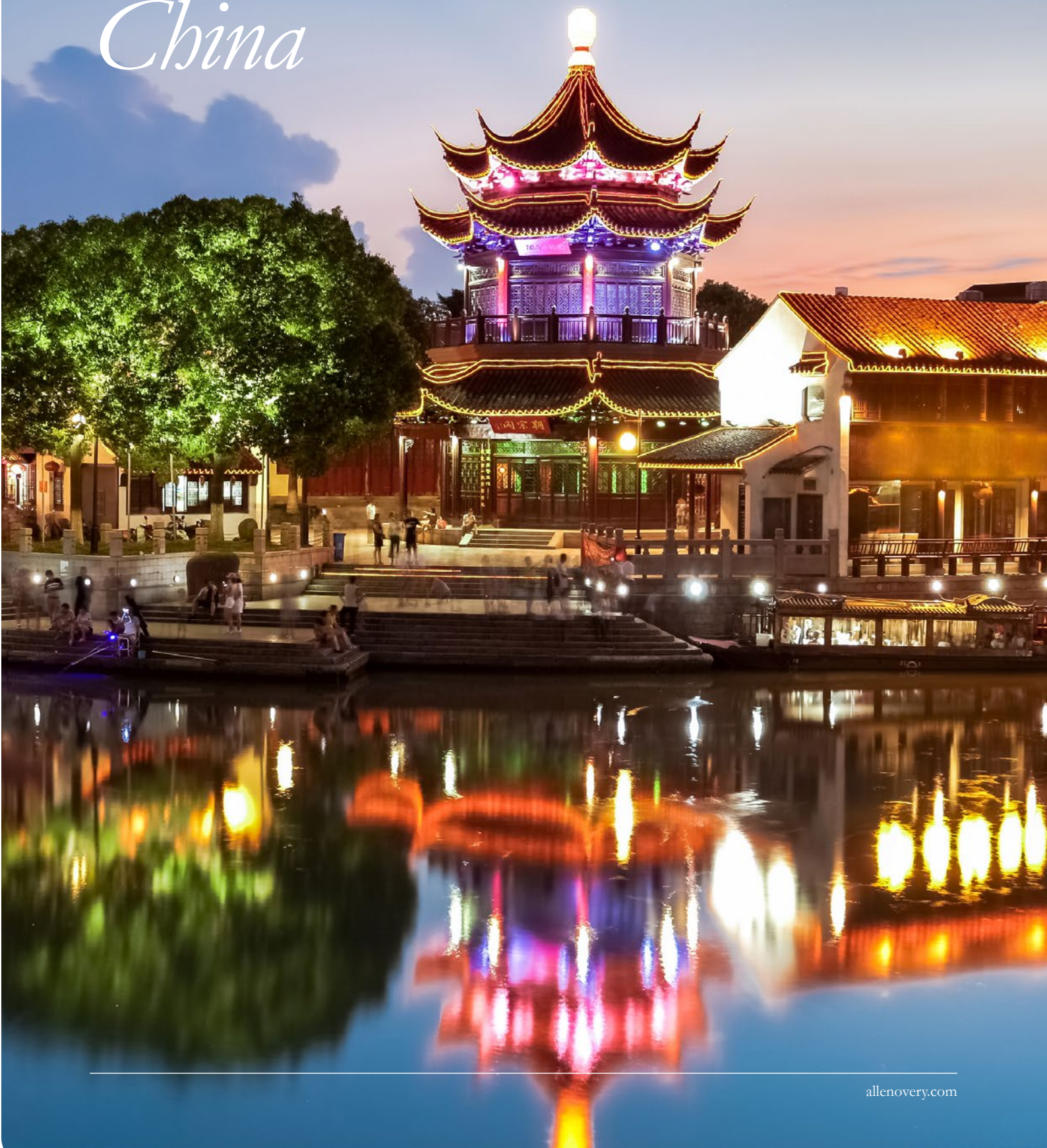
In order to be eligible for a remediation agreement, the prosecutor must believe that (a) there is a reasonable prospect for conviction, (b) the act or omission that forms the basis of the offense did not cause bodily harm or death, and (c) negotiating the agreement is in the public interest. The Canadian Attorney General must also consent to the negotiation of the agreement.

In considering whether a remediation agreement is warranted, the following factors set out in the implementing statute will be considered: (1) the circumstances in which the conduct was brought to the attention of authorities; (2) the nature and gravity of the act or omission; (3) the degree of

involvement of senior officials; (4) the disciplinary action taken by the organization; (5) whether the organization had made reparations; (6) whether the organization expressed a willingness to identify individuals involved in wrongdoing; (7) whether the organization was convicted of an offense or sanctioned by a regulatory body or previously entered into a remediation agreement; (8) whether the organization is alleged to have committed other offenses; and (9) any other factor that the prosecutor considers relevant. Anyone familiar with DPA's in other jurisdictions, such as the UK and U.S. will be familiar with similar factors. As with other jurisdictions, remediation agreements are not only available for foreign bribery offenses in Canada.



# China



# Changes to China's Anti-bribery Regulatory and Legislative Landscape

In May 2018, China's State Administration for Market Regulation (**SAMR**) announced the launch of a nationwide campaign to crack down on unfair competition and commercial bribery in the pharmaceutical, medical device and educational sectors. The announcement of the campaign followed on the heels of the introduction by the Chinese government of key amendments to its Anti-Unfair Competition Law (**AUCL**) and suggested that China is gearing up for tougher enforcement of its anti-bribery laws.

On May 17, 2018 China's newly-established SAMR announced the launch of a nationwide five-month campaign to crack down on unfair competition, with a focus on commercial bribery in the pharmaceutical, medical device and education sectors in the PRC. The campaign appeared designed to leverage off recent amendments to the PRC's AUCL, which has clarified the scope of the commercial bribery offense and increased the penalties for commercial bribery. The announcement came as Chairman Xi Jinping's government intensified its crackdown on corruption both at the local and national PRC government level. The SAMR's announcement signaled that China is gearing up its enforcement efforts and looking into those industries that are most prone to corruption risk.

## *China's New Regulatory Landscape*

The creation of the SAMR is the result of a sweeping government restructure in China, which has seen the SAMR assuming the role previously played by five separate government agencies, including the State Administration for Industry and Commerce (**SAIC**). The SAMR's focus on the pharmaceutical industry is particularly significant given the Chinese government's recent establishment of a new State Drug Administration (**SDA**) (under the purview of the SAMR) to oversee the regulation of drugs, medical devices and cosmetic products. Additionally, China has given the SAMR antitrust regulation powers, previously enforced by three separate Chinese agencies.<sup>1</sup>

With this restructuring, it appears that the Chinese government has nominated the SAMR as the key market regulator, tasked with overseeing everything from drug safety through to the management of intellectual property rights, anti-competitive behavior and corporate bribery. In the anti-bribery space, the SAMR's powers will extend to the bringing of civil actions against companies operating in China for bribery and unfair competitive behavior under the recently amended AUCL.

## *SAMR's Anti-Bribery Campaign*

The SAMR's announcement of an anti-bribery campaign stated that the agency will focus its five-month probe on the following three enforcement areas:

- commercial bribery in the pharmaceutical sector, the education industry and at state-owned enterprises (SOEs);
- infringement of trademarks and trade secrets; and
- false and misleading online advertizing.

Of particular note was the SAMR's focus on activities of the pharmaceutical and medical device industry, a sector which is traditionally prone to increased bribery risks. In its announcement, the new agency states that its campaign will center on the purchase and sale of medicines and medical equipment in the PRC, and the payment of bribes to both private counterparties and public officials. It will also target bribes paid to healthcare providers (HCPs) or government officials through third parties and agents.<sup>2</sup>

<sup>1</sup> The Anti-Monopoly Bureau of the Ministry of Commerce (**MOFCOM**), the Price Supervision/Inspection and Anti-Monopoly Bureau of the National Development and Reform Commission (**NDRC**) and the Anti-Monopoly and Anti-Unfair Competition Bureau of the SAIC.

<sup>2</sup> In China, HCPs who work in public hospitals are often presumed to be state functionaries, so any financial incentives to HCPs to prescribe certain medicines or to compile prescription data are deemed bribes under Chinese bribery laws.

### *China's Anti-Unfair Competition Law*

China's revised AUCL, which came into effect on January 1, 2018, prohibits individuals and entities from giving money or property to a business counterpart or public official, or using other means to obtain a business opportunity or competitive advantage. Private and public bribery is prohibited as well as bribery via a third party (an individual or entity). Companies should also note that employers will be held vicariously liable for their employees' acts of bribery.

The fines for commercial bribery under the AUCL range from RMB100,000 to 3 million (approximately USD15,000 – 466,000). Those found liable may also face confiscation of illegally obtained income and, in the case of serious offenses, the revocation of business licenses. Although the SAMR only has jurisdiction to bring civil enforcement proceedings, it can also refer cases to the Public Security Bureau or the Chinese Procuratorate for criminal prosecution under the Criminal Law of the People's Republic of China (**PRC Criminal Code**).

Additionally, failure to comply with the AUCL may also increase the risk of an investigation by the U.S. Department of Justice, the Securities and Exchange Commission or the UK's Serious Fraud Office for violations of U.S. or UK anti-bribery laws.

### *Key Takeaways for Companies Operating in the PRC*

Although the SAMR did not identify which specific companies it will focus its anti-graft campaign on, pharmaceutical and medical device companies with operations in China should expect increased regulatory scrutiny. In particular, pharmaceutical and medical device companies in China should:

- prepare for heightened dawn raid activity in China and ensure they have a protocol in place to react to dawn raids. Companies that already have such a protocol in place

should ensure it is up-to-date and that employees responsible for responding to a dawn raid are adequately trained;

- consider the need to conduct risk assessments to identify the most significant risks faced by their business and put in place controls to monitor and mitigate such risks. Specifically, internal controls around travel and entertainment, conference sponsorships for HCPs, meetings with doctors, as well as gifts and hospitality to government officials and hospital staff should be reviewed and tightly monitored for corruption red flags;<sup>3</sup>
- conduct anti-bribery due diligence on third parties, including downstream distributors and contract sales organizations. Depending on the risk profile of the third parties, fees paid to such entities should be reviewed and audited annually to ensure that distribution margins/commissions are not used to pay bribes;
- check that their anti-bribery and compliance policies are translated into Chinese and that all employees are educated about the implications of the AUCL; and
- ensure they have a panel of in-house or external legal counsel they can turn to in the eventuality of an inquiry by the SAMR. Legal counsel selected should have appropriate expertise and a good understanding of the local regulatory environment in China.

Finally, companies outside the pharmaceutical sector should also be aware of the risk of being caught up in the SAMR's anti-graft probe. Although one part of the probe is focused on commercial bribery in the pharmaceutical industry, the campaign extends to anti-competitive behavior generally, as well as violations of trademark laws and false advertising. Therefore, companies engaged in business dealings with Chinese SOEs or other government agencies and educational institutions could also find themselves the subject of inquiries by the SAMR.

<sup>3</sup> Pharmaceutical companies in China have recently been investigated for the provision of cash, gifts, travel and other forms of entertainment to healthcare professionals for improper gain or in exchange for fictitious patient data. In particular, pharma companies have used event planning and travel companies, local distributors or contract sales organisations to funnel bribes to doctors in exchange for drug prescriptions. In addition, recent investigations have identified that sales representatives are engaged in the practice of submitting false expense claims for meetings and meals with physicians and using the cash reimbursements to bribe HCPs.

# China's New Law on Judicial Assistance in Criminal Proceedings

On October 26, 2018 the PRC enacted a new law that could impact the process of obtaining assistance and evidence in criminal matters by foreign authorities in China. The new International Criminal Judicial Assistance Law (**ICJAL**) prevents individuals and entities within China from disclosing evidence obtained in China to assist in foreign criminal proceedings, unless they seek the approval of a “competent authority”.<sup>1</sup> In effect, this gives PRC authorities the power to monitor and block requests for assistance from other countries.

The ICJAL may present challenges for foreign authorities such as the UK Serious Fraud Office and the DOJ. In particular, the DOJ has actively conducted investigations in China in recent years, and announced on November 1, 2018 that it would seek to prioritize FCPA enforcement actions involving Chinese companies that are in direct competition with American businesses. The strained relationship between the U.S. and China brought on by recent events, combined with the enactment of this new law, make it unclear whether PRC authorities would provide assistance for such DOJ investigations.

## *Scope of the ICJAL*

The ICJAL only applies to the provision of assistance in criminal proceedings in foreign countries. Requests for assistance in relation to civil proceedings are therefore excluded from the scope of the ICJAL, including civil investigations conducted by the U.S. Securities and Exchange Commission.

The types of assistance encompassed by the new law includes the service of documents, collection of evidence, arrangements for witness testimony, seizure, freezing and confiscation of assets and unlawful gains, and the transfer of convicted persons.

## *Grounds for Refusal of Assistance*

PRC authorities can decide to postpone<sup>2</sup> or refuse assistance under the ICJAL. Assistance could be refused in the following circumstances:

- The conduct in the criminal proceeding does not constitute a crime under the PRC's laws;
- When receiving the request for assistance (**Request**), there is a parallel proceeding in the PRC or the proceeding has already ended, or the statute of limitations has passed;
- The proceeding is political in nature;
- The proceedings concern a military offense;
- The purpose of the Request is to investigate and prosecute based on race, ethnicity, religion, gender, political views, identity, or other reasons; or where the parties may be subject to unfair treatment based on these factors;
- The assistance sought is irrelevant to the proceeding; or
- Any other circumstances that warrant refusal.

The last provision is a catch-all provision that gives PRC authorities wide discretion to refuse assistance. “Other” circumstances that PRC authorities may cite could include refusal on the basis of harm to the judicial sovereignty and national security of the PRC.

1 Competent authorities include 5 PRC authorities: (i) the National Supervisory Commission; (ii) the Supreme People's Court; (iii) the Supreme People's Procuratorate; (iv) the Ministry of Public Security; and (v) the Ministry of State Security.

2 The new law is unclear on what grounds the authorities may postpone assistance. The ICJAL states that if the Request is obstructing an investigation, prosecution, judgment or enforcement of a proceeding in China, the authorities may postpone assistance but should inform the foreign country of their reasons for denial.



### *Practical Implications of the ICJAL*

The new law applies to requests for assistance from jurisdictions that have a mutual legal assistance treaty with China, as well as those that do not. For countries with such a treaty in place, the law may have little practical impact on the procedures to be followed, as similar procedures may already apply under the treaty. However, for countries that have not concluded such a treaty with China and have relied on informal practices, the new law may significantly impede progress with overseas criminal enforcement actions.

Interestingly, the ICJAL does not contain penalties for non-compliance.

### *Key Takeaways*

- **The ICJAL will likely not affect internal investigations** – internal investigations conducted by a company, including in relation to possible violations of the FCPA and UK Bribery Act, are unlikely to be affected. However, if a company voluntarily discloses the findings of an investigation to regulators in foreign countries, it should consider the need to submit the Request to one of the five relevant PRC authorities for further review and approval.
- **There may be tension between complying with Chinese and foreign laws** – recent DOJ enforcement actions suggest that the DOJ will apply a presumption in favor of a declination for companies that voluntarily self-disclose, cooperate with the DOJ and remediate misconduct. With the enactment of the new law, PRC subsidiaries of U.S. companies operating in China may have to choose between co operating with the DOJ and violating the ICJAL. This is not a new development. Companies operating in China that are subject to foreign government investigations usually have to balance compliance with the PRC’s state secrets and data privacy laws and disclosure of relevant materials to foreign regulators.
- **Civil proceedings are not affected under the new law** – as noted above, the ICJAL only applies to criminal proceedings and not civil proceedings. However, there are treaties and agreements the PRC has entered into that regulate assistance with civil cases.<sup>3</sup> The National People’s Congress may enact laws in the future specifically governing assistance in civil cases.

<sup>3</sup> Treaties and agreements include Convention on the Service Abroad of Judicial and Extra Judicial Documents in Civil or Commercial Matters; Convention on the Taking of Evidence Abroad in Civil or Commercial Matters; 35 existing treaties in the PRC. See [http://www.moj.gov.cn/organization/content/2014-12/17/jjzxwtdt\\_7237.html](http://www.moj.gov.cn/organization/content/2014-12/17/jjzxwtdt_7237.html).

# *Czech Republic*



# Criminal Liability of Companies in the Czech Republic

The concept of criminal liability of legal entities was introduced to the Czech legal system on January 1, 2012 and on December 1, 2016 a so-called large amendment to the Act on criminal liability of legal entities and proceedings against them (the **Act**) came into force.

The amendment significantly increased the number of crimes for which legal entities can be held liable (from 84 crimes to 270 crimes). The new crimes include, among others, infringement of competition rules, unauthorized operation of a lottery or other type of betting game, or machinations in insolvency proceedings. The absence of these crimes in the original Act had often been criticized by legal experts and the public.

Most importantly, the amendment softened the original concept of strict liability of a legal entity for acts committed by members of its statutory body (but also persons acting on behalf of the legal entity under a power of attorney), persons carrying out management or supervisory activities in respect of the legal entity (typically members of the supervisory board), or persons exercising a decisive influence on the management of the legal entity (e.g. majority shareholders). Under the amendment, the legal entity is able to discharge itself from liability for the acts of these persons if it has made all efforts that could reasonably be expected of it to prevent the commission of a crime.

As opposed to entities in the UK, until very recently Czech legal entities lacked thorough guidance from Czech regulators on the procedures to implement to fulfill the criteria for exempting themselves from Czech law criminal liability.

Detailed guidance was issued on August 14, 2018 by the Supreme State Prosecutor's Office (the **Guidance**). The Guidance requires legal entities to implement an effective compliance management system (**CMS**), which should represent a set of general principles, rules, recommendations and procedures to follow to prevent crimes from being committed by a legal entity's personnel, its statutory body members or persons carrying out its management or supervisory activities. When set up correctly, a CMS should be proportionate to the size of the legal entity, its international reach, risk profile and the sector in which it operates.

Although large Czech legal entities and those which are part of multinational corporations generally had created compliance programs in line with the UK and U.S. law requirements already, the Guidance now follows those standards and requires midsize and smaller Czech companies to duly implement them as well.

Each CMS should consist of three pillars – prevention, detection and reaction.

The Guidance requires each legal entity to (i) conduct a risk analysis, (ii) introduce and implement a code of ethics or another set of rules and principles of the CMS reflecting the findings of the risk analysis, (iii) perform an in-depth due diligence of its business partners, (iv) introduce regular training for its personnel, and (v) conduct a due diligence and follow-up regular screening of its employees. Tone from the top is also crucial for the prevention phase of the CMS. The detection requirement should comprise measures that will enable CMS violations to be identified, such as whistleblowing and internal investigation procedures that must be followed by corrective measures (including labor law implications), and an immediate revision of the CMS, if necessary. Continuous monitoring of the CMS's implementation throughout the entire organization and reporting identified misconducts to law enforcement authorities form an integral part of CMS's reaction measures.

The Guidance further lists several important decisions of lower Czech courts that are not public in the continental law system but which are useful for interpreting the Act.

Even though the Guidance is primarily addressed to state prosecutors who assess the criminal liability of legal entities, it provides a useful guidance for Czech companies in setting up their own compliance programs. Regulation of criminal liability of legal entities in the Czech Republic has thus moved one step closer to creating legal certainty and meeting international standards.

# *France*



# The French-style DPA – Round II

On February 23, 2018, the French public prosecutor of Nanterre executed Deferred Prosecution Agreements (known as **CJIP**) with two French companies to settle investigations into corruption offenses.

The first of this new type of settlement, introduced by the so-called “Sapin II” Law which was enacted on December 9, 2016, had already been entered into between a Swiss subsidiary of a major financial institution headquartered in the UK, represented by Allen & Overy Paris, and the National Financial Prosecutor’s Office, in relation to alleged laundering of tax evasion proceeds and illicit banking solicitation.

This time, however, the second and third French-style DPAs since Sapin II entered into force were executed by companies which had been placed under formal investigation (*mis en examen*) for active corruption of a French public official.

Although the CJIP is not considered to entail a criminal conviction nor would they appear on any criminal record, both companies had been targeted by judicial investigations (*information judiciaire*) and therefore had to accept the facts for which they had been placed under investigation in order to reach a settlement.

In addition, the negotiations ended up with both companies accepting:

- To pay a public fine of (i) EUR800,000 in 4 instalments due on a quarterly basis for the first company, and (ii) EUR2.71m split into twelve monthly payments for the second company;
- To indemnify the French State which had registered as a victim (*partie civile*) during the judicial investigations, in the amount of EUR30,000 for each company; and

- To be subject to monitoring by the new French Anti-Corruption Agency (**AFA**) for 18 months and two years respectively (i.e. less than the three-year maximum provided by Sapin II).

These are the first monitorships to be imposed since Sapin II entered into force. They involve monitoring compliance with all of the eight anti-corruption measures set out in Article 18 of Sapin II (e.g. risk mapping, code of conduct, internal whistleblowing mechanisms).

Allen & Overy witnessed Round I of the CJIP with a foreign institution and the fight against tax evasion. We have now seen Round II with smaller French companies in the energy sector and the fight against corruption.

Many rounds of enforcement are likely to follow. According to an interview of AFA’s deputy-director of inspections in 2018, six inspections were notified in 2017 and around a hundred inspections were scheduled for 2018. AFA has a duty to notify the public prosecutor of any potentially criminal conduct discovered. Who knows what these inspections will lead to.

# Settlements with Société Générale – Beginning of a New Era?

On June 4 2018, Société Générale (the **Bank**) announced that it had entered into settlements with the U.S. Department of Justice, the U.S. Commodity Futures Trading Commission (**CFTC**) and the French National Financial Prosecutor (Parquet National Financier, **PNF**), to conclude London Inter-bank Offered Rate (**Libor**) and Libya-related investigations.

These coordinated settlements are the first example of transatlantic cooperation between France and the U.S. since the enactment of the so-called “Sapin II” Law on December 9, 2016, introducing the first French style DPA (known as the **CJIP**).

These coordinated settlements might mark the beginning of a new era for white collar crime investigations against international companies that are headquartered, present or simply conducting activities in France, if cross border cooperation (particularly between U.S. and French authorities) becomes common practice.

The settlement between the Bank and the PNF is the fourth CJIP to be concluded in France. While the first CJIP concerned a foreign company and the laundering of tax evasion proceeds, the subsequent CJIPs have been executed with French companies suspected of corruption.

To conclude the preliminary investigation opened by the PNF on November 18, 2016 on the grounds of corruption of foreign public officials in relation to the Bank’s business relationships with the Libyan Investment Authority between 2007 and 2010, the Bank has agreed to (i) be subject to the AFA’s monitorship for two years and (ii) pay a public fine of EUR250,150,755 to the French Treasury.

As the same events were being investigated by the DOJ on the grounds of the FCPA, the PNF and the DOJ coordinated the settlements and agreed that the same amount (i.e. EUR250,150,755) would be paid by the Bank to the United States Treasury.

The agreement reached between the Bank and the DOJ also resolves investigations regarding alleged manipulation of the Libor. The CFTC investigated the same events, as well as alleged manipulation and false reporting in connection with the Euro Inter-bank Offered Rate (**Euribor**). The Bank has agreed to pay a fine of USD275m to the DOJ and a civil monetary penalty of USD475m to the CFTC.

Such coordinated settlements enable both the authorities and companies to cope with legal uncertainty resulting from lengthy criminal investigations and trial proceedings. Société Générale agreed to pay approximately USD1.3bn in total thereby putting an end to an investigation opened in France only a year and half beforehand.

However, the settlement with a company does not stop its directors from being prosecuted, as illustrated by the indictment of former Société Générale senior management in August 2017 in relation to the Libor.

# Increase in Corruption Investigations Against Prominent French Politicians and Businessmen

The French authorities have brought a number of enforcement cases against individuals and have not shied away from cases against high-profile politicians and businessmen. These cases focus on corruption and bribery outside of France in which the individuals were involved, as well as related domestic offenses.

A former French President was placed under formal investigation in March 2018 on grounds of corruption, illegal financing of an electoral campaign and receiving misused Libyan public funds in relation to the alleged funding of his presidential campaign by the late Libyan leader, Muammar Gaddafi in 2007.

Later in the same month, the same former French President was referred to trial on grounds of corruption and influence peddling in the so-called “tapping scandal”, named after the conversations tapped by investigators between him, his lawyer, and a former judge of the French Supreme Court.

A French businessman running extensive activities in Africa was placed under formal investigation in April for alleged corruption of a foreign public official, aiding and abetting the misuse of corporate funds, forgery and using forged documents, in relation to port concessions obtained by his group in Africa back in 2010. Other directors have also been placed under formal investigation.

A preliminary investigation into the Secretary General of the Elysée Palace was opened on June 4, after a criminal complaint had been filed by the anti-corruption association Anticor on June 1. The investigation targets alleged influence peddling (trafic d’influence) and the offense of directly or indirectly taking, receiving or keeping an interest in a company or an operation over which the suspect was supposed to ensure the supervision, administration, liquidation or payment (prise illégale d’intérêts). It appears to focus on the relationship between the Secretary General and an Italian-Swiss group which conducted a series of negotiations with the French State while he was in office at the Ministry of the Economy, between 2012 and 2016.



# *India*





# Significant Changes to India's Prevention of Corruption Act Target Bribe-payers, Corporate Liability, "Adequate Procedures" and Managerial Liability

In July 2018, India passed amendments to the *Prevention of Corruption Act 1988* (the **PCA**). The amendments contained in the *Prevention of Corruption (Amendment) Act 2018* (the **Amendments**) will have considerable impact on multinational corporations operating in India, including to criminalizing giving an "undue advantage" to a government official, establishing criminal liability for companies involved in bribery in India, and creating a specific offense penalizing corporate management.

## *Targeting bribe-payers*

Prior to the Amendments, while there were some indirect means to target bribe-payers under the PCA, the primary focus of the law had been on the demand side of corruption and the acceptance of bribes by public servants.

The Amendments introduced in July 2018 include a distinct offense dealing with the supply side of bribery, establishing an offense for giving or offering an "undue advantage" to another person with the intention of inducing or rewarding a public servant to improperly perform a public function. Whether the public servant accepts the offer, and the form the gratification takes (other than legal remuneration), is immaterial.

The Amendments also place limits on the immunity previously afforded bribe-payers. The unamended PCA provided bribe-givers with immunity if they reported a public servant having accepted a bribe or turned witness for the prosecution. The Amendments limit this protection to instances where the bribe-payer is "compelled" to provide the "undue advantage," or bribe, and requires reporting to law enforcement within seven days.

## *Corporate liability*

Significantly, the Amendments also introduced corporate liability. A commercial organization can be held liable "if any person associated with the commercial organization gives or promises to give any undue advantage to a public servant" with an intent to obtain or retain business or any advantage for that commercial organization. This provision covers all types of entities (including domestic and foreign companies) doing business in India, but does not include charitable organizations. Commercial organizations operating in India will therefore be vicariously liable for any bribes provided to public servants by persons associated with such organizations. The Amendments consider anyone "who performs services for or on behalf of the commercial organization" to be a person associated with such an organization. Consequently, commercial organizations can be held liable for the actions of their employees, external agents, contractors, consultants, subsidiaries, and other intermediaries.

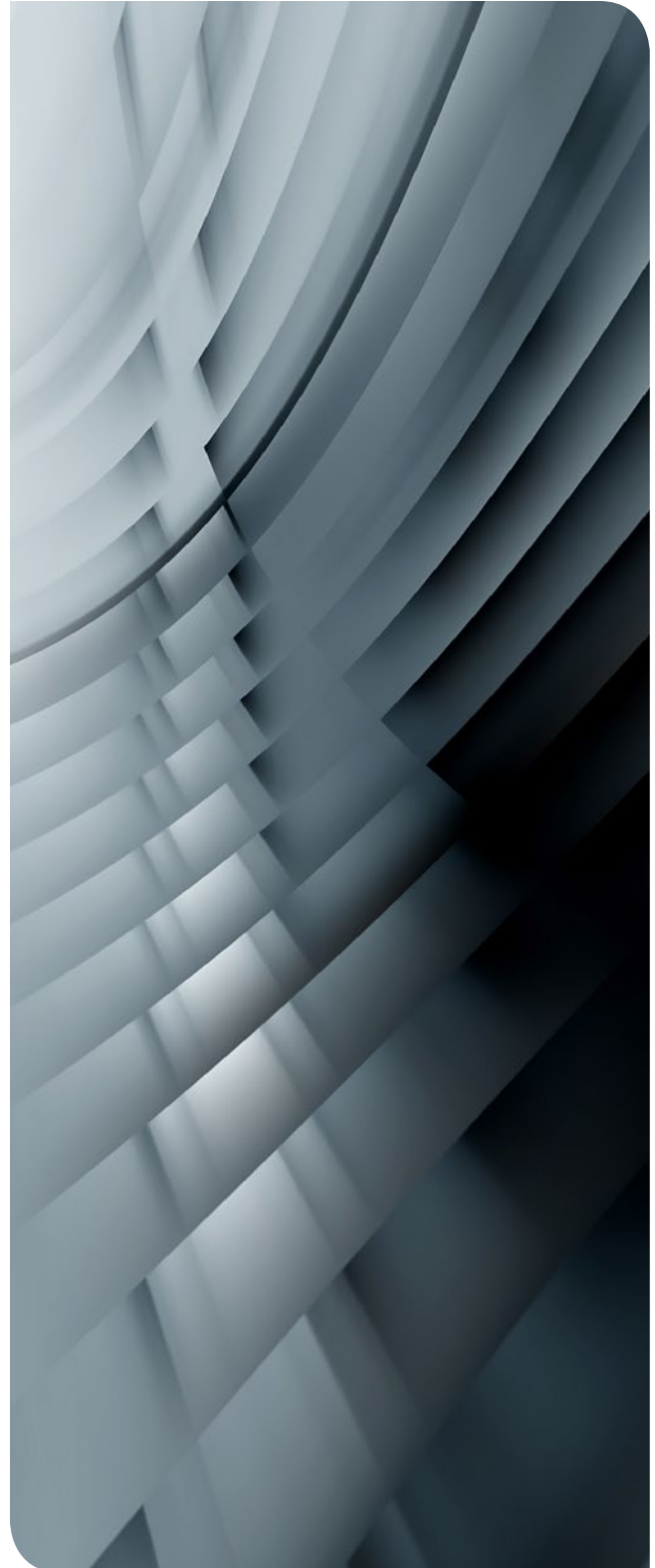
### *Adequate procedures*

Commercial organizations can avoid liability for a bribe provided by a person associated with them by demonstrating that the bribe was provided to the public servant despite the organization putting in place “adequate procedures designed to prevent” such wrongful conduct. While the 2018 Amendment does not delineate what are considered to be “adequate procedures”, it requires the Indian Government to prescribe guidelines in this regard.

Foreign parent companies should be mindful of the increased liability under the amended PCA. As parent entities may now be held liable in India for wrong-doing committed by their Indian subsidiaries, such parent companies should ensure that their Indian subsidiaries have adequate procedures to prevent bribe-giving to Indian public servants. Until such time as the Indian Government stipulates guidelines regarding the “adequate procedures”, commercial organizations doing business in India would do well to adhere to established international standards for compliance programs.

### *Managerial liability*

The Amendments also impose liability on directors, managers, secretaries and other officers of a commercial organization. Under new Section 10 of the PCA, managerial personnel of a commercial organization will be liable if the prosecution is able to establish that such personnel consented to or connived with the person committing the offense under the PCA. Managerial personnel can face imprisonment for up to seven years and/or fines if found guilty.



# *Indonesia*



# Indonesia's KPK Maintains Vigorous Pace of Anti-corruption Enforcement

Anti-corruption enforcement activity in Indonesia remained very active in 2018. Indonesia's Corruption Eradication Commission (*Komisi Pemberantasan Korupsi* or the **KPK**) was the primary enforcer, having a busy 2018 investigating bribery and corruption cases and maintaining its almost impeccable conviction rate.

- The KPK conducted 29 raids, the highest number of raids ever conducted by the KPK. Those raids resulted in 108 people being named suspects for criminal offenses.
- For the first time, the KPK indicted a corporation in a bribery case for bid-rigging. Among the penalties against the corporation that the KPK has requested, it has demanded that the company be prohibited from participating in public bidding for contracts over a period of time. The KPK is also currently considering charging three other corporations.
- The KPK has successfully pursued several high-profile individuals that had previously been deemed untouchable in the Indonesian media and political circles, including Setya Novanto, who was the former speaker of the Indonesian House of Representatives and Andi Narogong who was a former official of the Ministry of Home Affairs.

In total, the KPK is currently investigating 175 cases, comprising 152 bribery cases, 17 goods/services procurement fraud cases, and six money laundering cases.

One of the KPK's current high-profile cases relates to the Indonesian conglomerate, Lippo Group. The KPK has raided ten locations, including the home of Lippo Group Deputy Chairman, James Riyadi, as part of a bribery investigation linked to the group's USD21bn Meikarta real estate project. The Meikarta real estate project will comprise campuses for the automotive and electronics industries, as well as hotels, shopping malls, universities and housing. It has been described as the "Shenzhen of Indonesia," after China's booming manufacturing city. As part of its investigation, the KPK summoned Lippo Group Chief Executive Officer James Riyadi as a witness to be interviewed. The investigation is ongoing.



# Malaysia



# Malaysia Targets Corporations and Senior Management in Amendments to Anti-bribery Law

Against the backdrop of the ongoing investigations around the world into Malaysian sovereign wealth fund 1MDB, in April 2018, the Malaysian Parliament passed amendments to the *Malaysian Anti-Corruption Commission Act 2009* (the **MACC**). Following the trend of changes to anti-bribery and corruption legal regimes in jurisdictions across Asia in 2018, the amendments introduced a new statutory liability offense of corruption by a corporation if a person associated with the organization corruptly gives, offers or promises any gratification to any person with an intent to obtain or retain business or a business advantage for the said commercial organization. The MACC stipulates that persons considered to be “associated” with a commercial organization include directors, partners and employees of the commercial organization, as well as any person “who performs services for or on behalf of the commercial organization”. The MACC also states that a corporation shall be acquitted of a bribery charge if it proves that it “had in place adequate

procedures designed to prevent persons associated with the commercial organization from undertaking such conduct”. At the time of tabling these amendments, it was announced that this particular corporate liability provision of the MACC will start to be enforced two years after the amendments are enacted to allow companies time to adopt the necessary anti-corruption procedures.

In addition, the MACC also created personal liability for any director, controller, partner, officer or manager of a corporation for the same offense if the corporation is found liable. The only defense available to the relevant individual is if he or she can prove that the offense was committed without his or her consent, and that he or she had exercised “due diligence to prevent the commission of the offense as he ought to have exercised, having regard to the nature of his function in that capacity and to the circumstances”.



# *Netherlands*



# Potential Changes to Settlement of High-Profile Corruption Cases in the Netherlands

Although the Netherlands is generally considered low risk when it comes to bribery and corruption, the Dutch Public Prosecution Service (DPPS) has been involved in settling several of the most high-profile cases involving global corporations of the last years. By way of example, the DPPS settled a bribery investigation with SBM Offshore in 2014 for USD240m and participated in the settlements with Vimpelcom (USD795m, of which USD397.5m was for the DPPS) and Telia Company (USD965m, of which USD274m for the DPPS). This settlement practice has increasingly been criticised, and in November 2018, this criticism culminated in a proposal by the Dutch Parliament to order the government to introduce a judicial review mechanism for high-profile settlements.

## *Settlements*

The high-profile settlements mentioned above were reached using a so-called ‘transaction’, whereby the DPPS offers the suspect one or more conditions (such as the payment of a monetary amount) to prevent prosecution. In essence, this is a contract between the DPPS and the suspect and there is a relatively high degree of freedom in drafting the relevant contractual terms. However, for settlements exceeding EUR50,000, the DPPS must follow a specific procedure which requires approvals from the executive board of the DPPS and from the Minister of Justice and Security.

## *Criticism on settlements*

Although settlements of high-profile criminal investigations have always resulted in criticism, this criticism has increased markedly over the last years. This criticism has come from various groups, and has concentrated on (i) the perception of backroom politics and the lack of transparency on the conduct being settled due to the absence of any public hearing, (ii) the lack of development of relevant case law, (iii) the perceived class justice of the high-profile settlement practice and (iv) the risk that the DPPS will abuse its power in cases where the suspect has a significant interest in settling a case quickly. In response to some of these criticisms, the DPPS has changed its practice over the last years, notably increasing transparency through the publication of an (increasingly elaborate) statement of facts and, recently, the publication of the signed settlement agreement.

## *Judicial oversight*

In 2018, the criticism on high-profile settlements not only increased in tone and intensity, but was also echoed in formal judicial documents. Most notably, the Dutch Council for the Judiciary (a representative body of courts in the Netherlands) voiced similar concerns publicly and through a formal advice to change the Dutch Code of Criminal Procedure by introducing judicial oversight of high-profile criminal settlements. In November 2018, this resulted in the Dutch Parliament ordering the government to introduce a judicial review mechanism for high-profile settlements. The Dutch Minister of Justice and Safety stated that he will, in consultation with the DPPS and the judiciary, draw up such a mechanism. It is at this time unclear how and when judicial oversight to high-profile criminal settlements will be introduced, with some suggesting to adopt a system similar to the UK’s DPA procedure.

Although much of the criticism on the current high-profile settlements assumes that companies entering into such settlement are ‘getting a sweet deal,’ that does not mean that the introduction of a judicial review mechanism is necessarily detrimental for the settling company. As noted above, some criticism focuses on the risk that the DPPS abuses its powerful position in settlement negotiations. Depending on the way that judicial oversight would be implemented, companies might be better protected against pressure to settle crimes that cannot be proven beyond reasonable doubt. In the meantime, the one thing that is clear, is that the procedure through which high-profile corruption cases will be resolved, is likely to change significantly in the coming period. This is particularly relevant for companies currently facing investigations as this creates even more uncertainty with respect to the expected consequences of such investigations.



# The Increasing Pressure on Dutch Statutory Auditors to Detect Corruption

The role of statutory auditors in detecting and combatting fraud, particularly corruption, is a frequent topic of discussion in the Netherlands. Some say detecting corruption is one of the main tasks of statutory auditors, while others say statutory auditors are not equipped to detect corruption. Regulatory pressure on statutory auditors is increasing, which in turn is leading to increased pressure by statutory auditors on their audit clients to disclose information regarding potential corruption.

## *Increased regulatory pressure*

One of the parties that have put pressure on statutory auditors to detect and combat corruption is the Dutch Authority for the Financial Markets (**AFM**). The AFM is the primary external regulator of statutory auditors and has not only issued sector-wide warnings with regard to detection and reporting of corruption by statutory auditors, but is also engaged in multiple regulatory investigations of individual audit firms. These investigations can cover a multitude of requirements that apply to statutory auditors in relation to the detection and reporting of corruption, although the most relevant requirements stem from the Dutch anti-money laundering legislation, which also applies to statutory auditors.

Although the current trend of increased regulatory enforcement of existing legislation is already having a significant impact on statutory auditors and their audit clients, this is not the only source of increased regulatory pressure. The statutory audit sector as a whole is subject to intense criticism by the AFM and the Dutch Minister of Finance, which has led to the formation of a commission which will review the structure and business model of accounting firms in the Netherlands and propose structural changes. The role of statutory auditors in detecting and combatting financial crime, including corruption, is likely to be one of the focal points of this commission.

## *Increased criminal enforcement*

Statutory auditors do not only face increased regulatory pressure from the AFM and the Dutch Minister of Finance. In recent years, the Dutch Public Prosecution Service (**DPPS**) has increasingly focused its investigative resources on so-called “facilitator” of corruption, such as statutory auditors, banks and civil notaries who, according to the DPPS, play a facilitating role in the concealment of criminal activities and gains. These parties are seen as having an especially important role as “gatekeepers,” and are subject to a wide range of requirements further to the Dutch anti-money laundering legislation. This includes the requirement to report any transaction where the institution has reason to assume that the transaction may relate to money laundering. A violation of this requirement is a criminal offense, which can give rise to investigation and prosecution by the DPPS. The DPPS is actively publicizing their increased efforts in this area, which has already resulted in a number of high-profile cases.

### *How are statutory auditors, their clients and the DPPS responding to these developments?*

Statutory auditors have responded to the increasing pressure to detect and report corruption by significantly increasing their attention and resource allocation to this topic, but also by requiring more information from their audit clients. This is particularly visible when an audit client discloses indications of potential irregularities to its statutory auditor. Following such disclosure, it is not uncommon for the statutory auditor to demand vast amounts of information, including information that is subject to legal privilege.

This trend has not gone unnoticed by the DPPS. The files of statutory auditors are now often confiscated at an early stage of any corruption investigation. Concurrently, the DPPS is increasingly challenging claims of legal privilege regarding documents uncovered through this method. This trend obviously makes some audit clients more hesitant to disclose sensitive information to their statutory auditors. This can lead to a conflict between the statutory auditor and the audit client on the completeness of audit information, which can ultimately affect the audit opinion. Indeed, the first cases of statutory auditors issuing qualified opinions with a qualification referencing bribery or corruption risks have already hit the news. Such news reports are in turn often a red flag for the DPPS.

### *Takeaways*

The ultimate result of the aforementioned trends is that corruption cases are more likely to come to the attention of the DPPS at an early stage. Furthermore, given the regular confiscation of statutory auditors' files, the DPPS is more likely to have detailed information on the company's position and investigation and remediation efforts at an early stage of the investigation. This obviously increases the importance of careful information management whenever indications of potential irregularities arise, including careful consideration of the timing and content of information to be provided to the statutory auditor.



# Singapore



# Singapore Introduces a Deferred Prosecution Agreement Scheme for Companies

In 2017, Singapore ranked fifth in the Transparency International Corruption Perceptions Index. It is a country that stands out in the Asia Pacific region as a regional hub for multinational business and a jurisdiction where corruption is perceived to not be endemic and where there is active enforcement of anti-bribery and corruption laws. In 2018, Singapore introduced a new measure designed to assist in the enforcement of anti-bribery laws against companies.

The *Prevention of Corruption Act* (Chapter 241) (the **PCA**) is the primary anti-corruption law in Singapore. The PCA covers both public and private bribery and prohibits the giving and taking of bribes. Corruption is broadly defined under the PCA to mean a bribe offered in return for a favor. The bribe can be in the form of monetary or non-monetary nature, including:

- Money, gifts, loans, fees, rewards, commissions or other property of any description
- Any office, employment or contract
- Any payment, release, discharge or liquidation of any loan, obligation or other liability
- Any other service, favor or advantage of any description
- Any offer, undertaking or promise of any gratification

The criminal offense of bribery under the PCA is punishable by up to five years in prison, a fine of up to SGD100,000 or both.

## *Overview of the DPA Scheme*

On March 19, 2018, the Singapore Parliament passed the Criminal Justice Reform Act (**CJRA**). Among other changes introduced by the CJRA, it introduced a framework for Deferred Prosecution Agreements into the current Criminal Procedure Code enabling companies to reach agreement with the Public Prosecutor for the deferral of prosecution in exchange for the imposition of certain requirements.

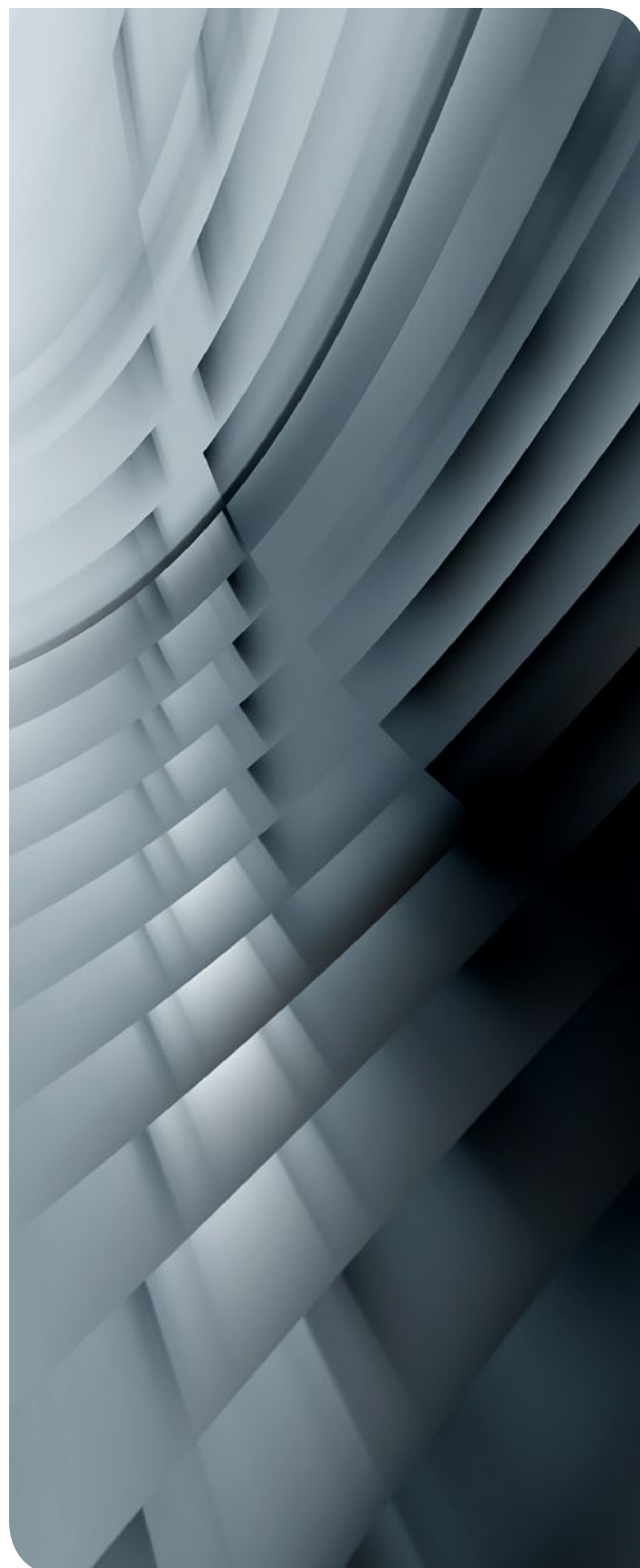
Many of the elements of Singapore's DPA scheme will be familiar to those aware of DPAs in the UK and U.S. In fact, the new law largely copies provisions from the UK DPA law,<sup>1</sup> with a few key differences: (1) Singapore DPAs will apply to far fewer criminal offenses, and (2) the law does not require Singapore prosecutors to issue guidelines on when a DPA is appropriate. The key features of the DPA scheme include the following:

- The Singapore scheme makes DPAs available only to companies, not individuals.
- Similar to the DPA scheme in the UK, court approval of the DPA is required. That approval requires that the court determine that the DPA is “in the interests of justice” and the terms are “fair, reasonable and proportionate.”
- The details of the DPA will be made public (the DPA, a statement of facts and the court approval will all be made public).
- DPAs will contain content such as a financial penalty, compensation to victims, disgorgement, and the implementation of a compliance program.
- The law also includes language requiring ongoing cooperation in any investigation relating to the alleged offense or other offenses arising from the same or substantially the same facts. This is similar to DPAs in the U.S., which regularly require cooperation for the investigation at issue and other investigations focusing on the same type of criminal conduct that are conducted during the term of the DPA.

<sup>1</sup> *Crime and Courts Act 2013*, Schedule 17, “Deferred Prosecution Agreements”

– DPAs will only be available in relation to prescribed offenses, such as corruption and money laundering, rather than all crimes.

The newly introduced DPA regime will give the Singapore authorities greater flexibility in sanctioning corporates, to the extent that corporates can be prosecuted for the offense under Singapore criminal law. This remains difficult, as corporate criminal liability in Singapore is often founded on requiring an individual who is the company's 'directing mind and will' to have the relevant criminal intent. Singapore does not have the broader corporate liability found, for example, in section 7 of the UK Bribery Act or vicarious liability under U.S. criminal law.



# *South Africa*



# State Capture in South Africa

On August 20, 2018, the Presidential Commission of Inquiry, appointed by South African's new President, Cyril Ramaphosa, to investigate allegations of State Capture, corruption and fraud in the South African public sector commenced hearings in Johannesburg. A term of art, "State Capture" refers to manipulation of government processes by individuals or small groups to influence state policies and laws to their benefit, typically to their financial gain.

In South Africa, "State Capture" is being used in reference to the efforts of the Gupta family, closely connected to former President Jacob Zuma and his son, Duduzane, to influence cabinet appointments and the award of government contracts. The phenomenon has recently captivated the South African national attention and resulted in concessions by several global firms, including McKinsey and SAP, that they benefitted from the phenomenon and were associated with entities owned and controlled by the Gupta family. Bain and KPMG have also suffered significant reputational damage as a consequence of their involvement in questionable dealings in the South African public sector.

The Guptas first drew significant adverse public attention when it was revealed that, in 2013, they had procured the use of a South African military base to land an aircraft carrying VIP guests from India for a family wedding. The scandal drew the attention of the media and civil society, who have largely filled the vacuum created in recent years by a police force and prosecuting authority compromised by rampant corruption under former President Zuma. The subsequent media investigations revealed an unhealthy close relationship between the Guptas and then-President Zuma.

The scandals and rumors surrounding the Guptas and their influence over Zuma continued to capture headlines. Eventually, opposition political parties and civil society groups requested an investigation by the Public Protector, an independent state institution with the mandate to investigate, report on, and remedy improper conduct in all state affairs. In late 2016, the Public Protector published a report detailing the extent of State Capture, revealing that Zuma had effectively abdicated certain of his executive functions to the Guptas, permitting them influence over key

state institutions and resources, most notably State Owned Enterprises (SOEs). Just over a year later, South Africa had a new president and the Guptas had fled to Dubai.

The Guptas' influence was most pernicious at two SOEs, Eskom and Transnet. Both are wholly owned by the South African Government and responsible for the provision of public goods. Eskom is South Africa's only electricity utility. Transnet is responsible for rail and logistics infrastructure in South Africa.

## *McKinsey*

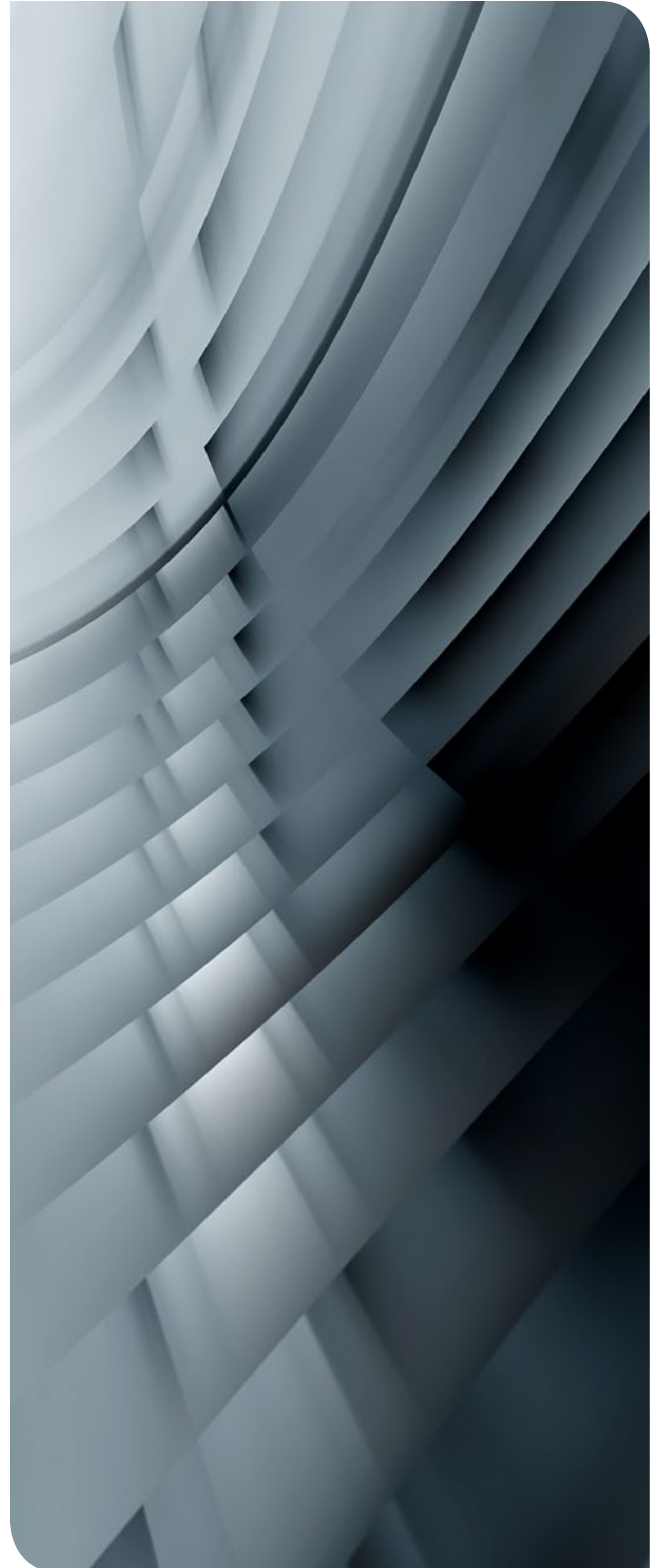
In 2015, McKinsey signed its largest ever contract in Africa. The contract concerned a much-vaunted turnaround and reorganization strategy for the then-embattled Eskom. At the time, the utility was in turmoil, with significant power shortages and massive overspend. Although McKinsey asserts it provided consulting services to Eskom, of concern was the revelation that it subcontracted a large part of its mandate to a Gupta-linked entity, Trillian Capital Partners, which apparently provided little to no services to Eskom. Between McKinsey and Trillian, the two earned ZAR1.6bn (~USD115m) for just over a year's work and expected to make another ZAR7.8bn (approximately USD563m) in coming years. Eskom recently cancelled the contract.

McKinsey initially denied any wrongdoing, but has since withdrawn that denial and delivered an apology. In July this year, and as a result of a significant backlash, it agreed to pay back almost ZAR1bn (approximately USD72m) to Eskom. The Eskom contract was described by The New York Times as the worst mistake in the nine-decade history of the company. A South African Police Services (SAPS) investigation and a United States Department of Justice investigation are ongoing.

## *SAP*

In July 2017, it was alleged that SAP, the world's third largest software provider, had paid ZAR128.6m (approximately USD9.29m) to Gupta-linked software companies to secure work from Transnet and Eskom. Despite initial denials, in March 2018, and as a consequence of an internal investigation, SAP admitted that it had paid hundreds of millions of Rand to Gupta-linked entities in respect of contracts with SOEs. Like McKinsey, it has subsequently issued an apology, reported itself to the DOJ and United States Securities and Exchange Commission (for possible breaches of the FCPA) and is reportedly cooperating with an investigation into its conduct. SAP also reported that it had strengthened its anti-bribery and corruption procedures; including banning sales commissions on public sector contracts in countries with poor corruption ratings, including South Africa.

The Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State (**State Capture Inquiry**) is expected to continue well into 2019. Current estimates on the losses incurred by the South African Government as a consequence of State Capture range as high as ZAR250bn (approximately USD18bn). The process is expected to reveal more malfeasance between the private and public sector. With the attention of international regulators now focused on the southern tip of Africa, the consequences could be dire for multinational corporations with government contracts in South Africa.





# Thailand



# Thailand Introduces New Anti-bribery Law that for the First Time Covers Foreign Companies

Continuing a trend we have seen in other jurisdictions in Asia in 2018, Thailand introduced new anti-bribery and corruption legislation in July that increases enforcement risk for foreign companies operating in Thailand. Officially named the *Act Supplementing the Constitution Relating to the Prevention and Suppression of Corruption B.E. 2561 (2018)* (the **New Anti-Corruption Law**), it came into force on July 22, 2018. The New Anti-Corruption Law replaces the *Organic Act on Counter Corruption B.E. 2542 (1999)* (the **OACC**).

Pursuant to the New Anti-Corruption Law, legal entities (ie corporations) can be criminally liable for bribes given to Thai state officials, foreign state officials, and officials with intergovernmental organizations. Similar to the UK Bribery Act, the legal entity is also liable when the bribe is provided by an “associated person”, which can include employees, joint venture partners and agents.

Importantly, the New Anti-Corruption Law expands the definition of legal entities who can commit bribery to include foreign companies. This means that it applies to organizations that are registered abroad but operating in Thailand through, for example, local agents to win contracts.

The New Anti-Corruption Law also allows legal entities to reduce their liability if they have proper internal controls. This was also possible under the OACC. In 2017, the National Anti-Corruption Commission (the **NACC**), Thailand’s main anti-corruption enforcement agency, issued the *Guidelines on Appropriate Internal Control Measures for Juristic Persons to Prevent Bribery of State Officials, Foreign Public Officials, and Agents of Public International Organizations (Guidelines)* which describe what the NACC deems to be appropriate internal controls under the OACC, and now the New Anti-Corruption Law. The Guidelines comprise eight principles that will be familiar to FCPA and UK Bribery Act practitioners:

- Principle 1 Strong, visible policy and support from top-level management to fight bribery
- Principle 2 Risk assessment to effectively identify and evaluate exposure to bribery

- Principle 3 Enhanced and detailed measures in high risk and vulnerable areas
- Principle 4 Application of anti-bribery measures to business partners
- Principle 5 Accurate books and accounting records
- Principle 6 Human resource management policies complementary to anti-bribery measures
- Principle 7 Communication mechanisms that encourage reporting of suspicion of bribery
- Principle 8 Periodic review and evaluation of anti-bribery measures and their effectiveness

The New Anti-Corruption Law also seeks to streamline the process by which the NACC can seek international cooperation in their investigations, and also allows the NACC to refer matters to its foreign counterparts. As we have discussed elsewhere in this update, these changes reflect the trend of anti-corruption investigations frequently involving multi-jurisdictional activity and a number of countries and regulatory authorities.

The New Anti-Corruption Law also introduces a government-subsidized fund called the “National Anti-Corruption Fund” to support the NACC’s investigation costs, provide rewards to informants, and raise anti-corruption awareness in Thai society.

# *United Kingdom*



# New Director, New Direction? Initial Insight into the Next Era at the Serious Fraud Office

The question on everyone's mind since the announcement of the Director of the SFO on June 4, 2018 has been: how (if at all) will the new Director change the SFO's strategic direction and enforcement priorities?

We have had the first insight into that topic with the speech delivered in September by Lisa Osofsky in her capacity as the new Director of the SFO at the Cambridge International Symposium on Economic Crime. The take home message was that Ms Osofsky expects the SFO to remain committed to ensuring that the United Kingdom is, and will continue to be, a high risk place for the world's most sophisticated criminals to operate. She anticipates achieving that through global cooperation, the potentially expanded use of DPAs and technological advancements.

## *The Importance of Co-operation to the SFO's Continuing Success*

The Director discussed the need for international cooperation due to the increasingly multi-jurisdictional and complex nature of cases in order to help the SFO achieve global settlements, as achieved with Rolls Royce. The Director stressed her focus on strengthening and deepening international relationships to achieve more global settlements similar to Rolls Royce, including the need for further cooperation with newcomers to DPAs involving countries such as Argentina, Canada and Australia. The Director discussed how DPAs are no longer just a U.S. only phenomenon. She cited her familiarity with the DPA process and indicated a commitment to a continued and potentially increasing use of DPAs under her tenure at the SFO.

The Director also highlighted the continuing work with national law enforcement organizations, including the contribution of the SFO to the development of the National Economic Crime Centre and the SFO's continuing work with the National Crime Agency. A controversial topic surrounding the SFO's administration has been the continued speculation over a potential merger with the National Crime Agency. This was not expressly mentioned within the Director's speech, although she has publicly come out since her appointment was announced to share a view that this would not be in the SFO's interest, and the suggestion has similarly been dropped from the Conservative Party's most recent manifesto. Nevertheless, it is clear from her speech that domestic cooperation with a number of agencies and institutions is going to be intrinsic to the Director's approach.

The Director briefly touched on the SFO's secondment and exchange program as part of her vision of cooperation, including the DOJ secondee currently with the SFO. On the topic of secondments, the Director discussed the exciting development and future cooperation with the National Economic Crime Centre (the **NECC**), highlighting the potential opportunities for SFO employees to be seconded to the NECC. The Director also talked of the "natural ally" she saw in HM Revenue and Customs, stating that the SFO and HM Revenue and Customs could build "very strong" cases.

### *The Future of Privilege at the SFO?*

In one of her first major decisions, the Director has chosen not to appeal the SFO's recent defeat in the Eurasian Natural Resources Corporation (**ENRC**) case.<sup>1</sup> Whether or not this signifies a break in term of attitude towards privilege compared to her predecessor, the Director's speech only briefly touched on the topic of privilege; her primary focus in this regard was on enhancing the SFO's use of technology in the process of identifying privileged documents produced in the course of investigations. For example, Osofsky discussed the deployment of an AI robot which helped to check for legal professional privilege material in the Rolls Royce case which led to cost savings of 80%.

This is consistent with the Director's commitment to the advancement and the importance of the strategic use of cutting edge technology within the SFO. The Director discussed the SFO's creation of an "eDiscovery" platform, a feature that will assist with the future review of new investigations to create greater efficiencies, hopefully bringing quicker decisions and shorter trials. Committed to improving the SFO's intelligence function, the Director stated how there is a need to have an ability to collect and analyze data to improve knowledge of priority or emerging threats to enable the SFO to identify proactive investigative lines of inquiry.

While the thrifty element of this new approach in criminal investigations is to be welcomed as a process to utilizing financial resources, and may also be helpful for firms negotiating with the SFO in structuring their own investigation, the approach to the SFO's treatment of privilege remains somewhat uncertain post ENRC, and the criticism leveled by the Court in *R (AL) v Serious Fraud Office* [2018] EWHC 856. The Director's focus on the Rolls Royce case though does suggest that investigation subjects may still face pressure to voluntarily disclose interview memoranda, should they want credit for a course of "full and extraordinary cooperation" with the SFO in a Deferred Prosecution Agreement.

It leaves open the question of whether the changed position

on privilege will result in a practical difference from the SFO when it comes to measuring cooperation credit, or whether there will still be some expectation from the SFO that parties subject to investigations will waive the protection offered by privilege in return for an amicable settlement.

### *Technological Innovation*

Discussing the technological challenges that the SFO investigations face, including data-heavy criminal investigations, the Director set out how the SFO is exploring technology to find the right solutions for these challenges, including the use of technology to overcome issues arising through encryption. The SFO will also continue to focus on making the most out of witnesses to bring the most compelling evidence before judges and juries, as well as prioritizing the recovery of criminal proceeds.

The expected importance of extensive international and national cooperation, the continued pursuit of deferred prosecution agreements and a commitment to technology highlights the Director's commitment to becoming a "different kind of Director."

<sup>1</sup> <http://www.allenoverly.com/publications/en-gb/Pages/ENRC-v-SFO-appeal-internal-corporate-investigation-documents-are-protected-by-privilege.aspx>

# Prosecutor Attitudes and Resources: SFO can Request Overseas Documents from Non-UK Companies

The Serious Fraud Office can validly issue a section 2 notice with extraterritorial application. It can compel production of documents held extraterritorially by a UK company, or issue a notice to foreign companies in respect of documents held outside the UK if there is a “sufficient connection” between that company and the UK. The ruling comes at a time when the SFO is testing the limits of its powers to seek disclosure of documents. Although unsuccessful in *SFO v ENRC* when contesting the ambit of legal professional privilege, the SFO will be pleased with the outcome of this ruling on its extraterritorial reach: *The Queen on the application of KBR Inc v The Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), September 6, 2018.

Under section 2 of the *Criminal Justice Act 1987* (the **CJA**), the SFO can issue a notice requiring a person or entity under investigation or any other person to produce documents which appear to the SFO to relate to any matter relevant to the investigation. These are commonly called “section 2 notices.” Failure to comply with a section 2 notice without a reasonable excuse is a criminal offense.

The territorial scope of this power has been unclear: does it extend to documents held by UK companies overseas (including on an overseas server)? Does the SFO have the power to issue a section 2 notice to a foreign corporation that has no business presence in the UK?

These questions were answered in this case dealing with the validity of section 2 notices issued to:

- the English company: Kellogg Brown & Root Ltd (**KBR Ltd**): KBR Ltd carried out business in the UK. In February 2017, the SFO commenced a criminal investigation into KBR Ltd for suspected offenses of bribery and corruption relating to the Unaoil scandal; and
- the U.S. parent company: KBR Inc: the ultimate parent of a multinational group, including KBR Ltd, providing professional services and technologies. KBR Inc had no fixed place of business in the UK and did not independently carry on business in the UK; it only did so through its UK subsidiaries. KBR Inc was under

investigation by the U.S. Department of Justice and Securities and Exchange Commission for its dealings with Unaoil.

## *SFO Seeks Documents Held Both In And Outside The UK*

The SFO issued a section 2 notice to KBR Ltd in April 2017. Initially, the KBR Group expressed an intention to cooperate expansively in its response. It provided: (i) UK-based responsive documents already under KBR Ltd’s custody and control; (ii) documents located outside the UK and sent to KBR Ltd at KBR Inc’s direction; and (iii) purely on a voluntary basis, documents which KBR Inc had previously disclosed to the DOJ and SEC.

However, the SFO became concerned that the KBR Group was drawing what the SFO considered to be an inappropriate distinction between documents held by or under the control of KBR Ltd and documents held outside the UK and beyond the control of KBR Ltd. It therefore issued a further, largely duplicative, section 2 notice in July 2017 (the **July Notice**) addressed directly to the U.S. entity, KBR Inc.

The U.S. entity, KBR Inc, challenged the lawfulness of the notice and refused to produce documents in response to it on the grounds that:

- the July Notice was ultra vires as it requested material held outside the UK from a foreign-incorporated company;
- it was an error of law for the SFO to exercise section 2 powers despite the power to seek Mutual Legal Assistance (MLA) from the U.S. authorities; and
- the July Notice had not been effectively served on KBR Inc when it was handed to an officer of KBR Inc who had temporarily been present in the UK in order to, at the request of the SFO, attend a meeting with the SFO.

The court rejected all of these arguments and upheld the validity of the notice.

### *Section 2 Notice Capable Of Extending To Documents Held Overseas By UK Companies*

There is a general principle that, absent contrary intention, statutes have only territorial (not extraterritorial) application: i.e. they are restricted in operation to the UK.

However, the court concluded that section 2 notices issued to UK companies had to have at least some extraterritorial reach. This was because it was “scarcely credible” that a UK-based company could refuse to provide documents solely because the documents were contained on a server abroad, as this would mean that a company could thwart an investigation by moving documents overseas. While section 2 had been drafted pre-internet, and had to be construed accordingly, the underlying policy behind section 2 was to prevent the “determination and ingenuity” of persons trying to obstruct investigations. Even in a pre-internet age, this would have required section 2 notices served on UK companies to have extraterritorial application.

### *Section 2 Notice Capable Of Extending To Non-UK Companies In Respect Of Documents Held Outside The UK*

There was no express statutory limitation on who could be a potential recipient of a section 2 notice. The court concluded that section 2 was directed at facilitating the investigation and prosecution of top end fraud, which by its nature would have an international dimension. While the international spread of documents has been amplified by technological developments since 1987, the court did not consider that an international dimension to such investigations was “unknown or not appreciated” when the Criminal Justice Act 1987 was drafted. Excluding any consideration of MLA, the court saw a “very real risk” that the section 2 power would be frustrated if the SFO was unable to seek documents located abroad from a foreign company. The court recognized the strong public interest in section 2 having an extraterritorial ambit, and concluded that section 2 notices could be validly issued to non-UK companies for documents held both in and outside of the UK.

### *Section 2 Notice Issued To Non-UK Company – Must Be A “Sufficient Connection” With The UK*

The court applied a new limitation – a section 2 notice can only validly be given to a non-UK company in respect of documents held outside the UK where there is a “sufficient connection” between the company and the UK.

The court found a sufficient connection between KBR Inc and the UK for the July Notice to be valid. This was because the SFO’s investigation focused on a large number of suspected corrupt payments made by KBR Inc’s UK subsidiaries to Unaoil. The SFO had formed the view that those payments had required express approval by KBR Inc’s U.S.-based compliance function and were processed by KBR

Inc's U.S.-based treasury function. Further support arose from the fact that a corporate officer of KBR Inc was based in the group's UK office and appeared to carry out his functions from the UK.

The following factors, said the court, would not, without more, amount to a "sufficient connection" between a non-UK company and the UK:

- the non-UK company is the parent company of a company under UK investigation;
- the non-UK parent company cooperates to a degree with the SFO's request for documents and remains willing to do so voluntarily; or
- a senior officer of the non-UK parent company attends an in-person meeting with the SFO.

### *Mutual Legal Assistance Regime Curtailed?*

The court found that the MLA regime provides an additional, alternative route to obtain documents for the SFO but its availability does not affect the lawfulness of the SFO's decision to issue a section 2 notice to a non-UK company with sufficient connection to the UK. Even when there is an available MLA regime, there may be good practical reasons for the SFO to proceed with a section 2 notice (as it had in this case). The SFO has recently used the MLA regime to try to obtain documents in Monaco.

### *How Is A Section 2 Notice Served On A Non-UK Company?*

A section 2 notice should be given to a person within the jurisdiction: there is no additional formality or traditional "service" required beyond the giving of the notice.

In this case, the July Notice was handed to an officer of KBR Inc voluntarily attending a meeting in the UK with the SFO, at the SFO's request. The officer was present in the UK for the purpose of representing KBR Inc, which was sufficient to establish KBR Inc was present in the jurisdiction at the time it (through its officer) was given

the July Notice. While the court found it unappealing that the SFO insisted on a KBR Inc representative attending the meeting with the intention to serve the July Notice, this did not affect its validity.

### *Safeguards/Defenses*

The court pointed to statutory "safeguards" in place in the CJA: the SFO must decide whether to exercise the power to issue a section 2 notice, the issue of such a notice is subject to judicial review and a person may rely on a statutory defense of reasonable excuse if they do not comply. However, it is unclear what the practical value of these safeguards and defenses would be to a foreign company facing a potential fishing expedition. The English court has traditionally been reluctant to interfere, by way of judicial review, with the SFO's decision-making powers; for example the 2016 failed attempt, via judicial review, by Soma Oil & Gas to stop an SFO investigation.

### *Comment*

While the court was careful to note that it was not engaging in "impermissible judicial legislation," it is difficult to conclude that the decision involves anything else. The CJA imposes criminal penalties for failure to comply with a section 2 notice, which would not usually align with an extraterritorial reach without specific extraterritorial statutory provision (as in, for example, the UK Bribery Act).

There is no suggestion in the CJA of the "sufficient connection" test and in other similar contexts (for example, the *Proceeds of Crime Act 2002*) and the Supreme Court has limited disclosure orders to having jurisdictional reach only. While similar tests have been generated in the insolvency context, the statutory safeguards surrounding the exercise of such powers are quite different to those involved in questioning the SFO's power to issue a section 2 notice, which are limited to very narrow grounds.



The “sufficient connection” test for when a non-UK company may be issued with a section 2 notice involves considering the factual connection of the company to the UK, not in terms of (as might be expected) the strength of the business connections to the UK or storage of documents here, but rather its connection to the subject matter of the SFO’s investigation (in this case, it was the U.S. company’s role in the UK company allegedly making improper payments). As such, it is unclear what can be done by a non-UK company to insulate itself from the reach of a section 2 notice, barring avoiding receipt of such a notice by refraining from having its officers enter the UK.

The court did not consider the practicalities of a non-UK company complying with a request for documents. For example, there was no discussion regarding data protection or other overseas laws or arrangements which may restrict a company’s ability to comply, and the invidious position a non-UK company may then be put in of facing competing criminal or civil liability (a difficulty which may be overcome through appropriate use of the protections built into the MLA regimes). The practical ability of the SFO to enforce such a notice against a non-UK company without any UK presence may also be called into question, in particular where a foreign company may face domestic blocking statutes or other compelling local law prohibitions against compliance with a UK section 2 notice.

A strong pointer that the legislature itself views the SFO’s section 2 power as not being intended for extraterritorial use is the proposed introduction of a new UK law that will allow law enforcement agencies (including the SFO) to apply for a UK court order to obtain stored electronic data directly from a company or person based outside the UK. The Crime (Overseas Production Orders) Bill 2018 contains specific safeguards surrounding the extraterritorial use of production powers. The need for additional UK legislation governing extraterritorial production orders is consistent with the international approach taken in such cases. The Microsoft case in the U.S. (in which the U.S. government sought to compel Microsoft to disclose information stored on servers abroad) was based on unclear drafting in the U.S. Stored Communications Act (**SCA**). To clarify this ambiguity, the U.S. Clarifying Lawful Overseas Use of Data Act (the **CLOUD Act**) was passed. The CLOUD Act amends the SCA expressly to require a provider to provide data within its “possession, custody, or control, regardless of whether [such data] is located within or outside the United States.”

While the Court did not consider that extending the jurisdiction of the SFO to issue section 2 notices extraterritorially would “raise eyebrows” in this case, it certainly does raise questions about international cooperation and comity, and (if the decision stands) the ongoing use of MLA procedures by the SFO in the UK.

# *ENRC v SFO* Appeal: Internal Corporate Investigation Documents were Protected by Privilege

Documents, including interview notes, generated by mining company ENRC during an internal corruption investigation were protected by privilege and therefore did not have to be disclosed to the Serious Fraud Office (SFO).

This unanimous Court of Appeal decision overturns the controversial High Court ruling last year which threw into question how businesses could investigate possible wrongdoing without creating material, including potentially incriminating documents, that would have to be handed over to investigators.

The decision will be welcomed by businesses and their lawyers as it increases the likelihood of a successful claim to litigation privilege in England when entities are facing the prospect of a criminal prosecution or regulatory enforcement action. The SFO has announced that it will not be appealing to the Supreme Court.

The Court also expressed helpful, but non-binding, views on the question of who is the “client” for the purposes of legal advice privilege – i.e. which individuals within a corporation can communicate with the corporation’s lawyers on a privileged basis.

## *ENRC Conducts Internal Investigation*

In December 2010, ENRC received an email from an apparent whistleblower containing allegations of bribery and financial wrongdoing in relation to its Kazakh subsidiary. This led ENRC to instructing lawyers and carrying out an internal fact-finding investigation. In April 2011, following press reports suggesting that the SFO had been asked to investigate ENRC on the matter, forensic accountants were also instructed to investigate.

In August 2011, the SFO became directly involved. It contacted ENRC, drew its attention to the SFO’s self-reporting guidelines and suggested a meeting. There

followed a lengthy period of dialog between ENRC and the SFO, including a series of meetings in which ENRC updated the SFO on the progress of its internal investigation.

## *SFO Starts Criminal Investigation of ENRC And Demands Documents*

The SFO formally commenced a criminal investigation in April 2013 and compelled ENRC to produce a range of documents including:

- notes taken by lawyers of the evidence given to them by ENRC’s employees, former employees, subsidiaries, suppliers and other third parties; and
- materials generated by forensic accountants, as part of a “books and records” review, with a focus on identifying controls and systems’ weaknesses and potential improvements (together, the **Documents**).

The SFO cannot compel the production of documents which a corporation would be entitled to refuse to disclose on grounds of legal privilege in proceedings in the English court. ENRC claimed the Documents were privileged and refused to produce them. The SFO then commenced these proceedings disputing that claim and seeking production of the Documents.

### *Court Of Appeal Rules That Litigation Privilege Applies*

Litigation privilege applies to communications between clients or their lawyers and third parties for the purpose of obtaining information or advice in connection with existing or contemplated litigation when, at the time of the communication in question:

- litigation is in progress or reasonably in contemplation;
- the communications are made with the sole or dominant purpose of conducting that litigation or anticipated litigation; and
- the litigation is adversarial, not investigative or inquisitorial.

At first instance, Andrews J denied a claim for litigation privilege for the Documents. This was on the basis that:

- ENRC needed to have a criminal prosecution in contemplation at the time the Documents were created and, on the facts, Andrews J concluded that ENRC did not contemplate criminal prosecution at that time;
- even if a prosecution had been reasonably in contemplation, none of the documents had been created with the dominant purpose of being used in such litigation; and
- litigation privilege does not extend to documents created in order to obtain legal advice as to how best to avoid contemplated litigation or a future regulatory or criminal investigation.

The Court unanimously disagreed with these conclusions and upheld ENRC’s claim that the Documents were protected by litigation privilege.

### *Criminal proceedings against ENRC were reasonably in contemplation*

The Court held that a criminal prosecution was reasonably in contemplation when ENRC initiated its investigation and was certainly in contemplation from when ENRC was contacted by the SFO.

Ultimately, this was a question of fact (and the Court noted that it was not sure that “*every SFO manifestation of concern would properly be regarded as adversarial litigation*”). However, the Court stated that, when the SFO specifically makes the prospect of its criminal prosecution clear to a corporation (over and above the general principles set out in the SFO’s Guidelines), and legal advisors are engaged to deal with that situation, there was “*clear ground*” to contend that a criminal prosecution was in reasonable contemplation. This was the case for ENRC.

Indeed, the Court held that “*the whole sub-text of the relationship between ENRC and the SFO was the possibility, if not the likelihood, of prosecution if the self-reporting process did not result in a civil settlement*”.

The Court diverged from the views of Andrews J on some important points of general principle, finding that:

- while a party anticipating possible prosecution will often need to make further investigations before it can say with certainty that proceedings are likely, that uncertainty does not of itself prevent proceedings being in reasonable contemplation;
- Andrews J was wrong that litigation privilege cannot attach until either: (a) the defendant knows the full details of what is likely to be unearthed; or (b) a decision to prosecute has been taken; and
- the fact that a formal criminal investigation has not yet been commenced will be a part of the factual matrix when determining whether litigation is reasonably in contemplation, but it will not necessarily be determinative.

### *Documents were generated by ENRC for dominant purpose of resisting or avoiding criminal proceedings*

At first instance, Andrews J concluded that ENRC's dominant purpose was to investigate the facts to see what had happened and deal with compliance and governance, rather than defend contemplated criminal proceedings. Andrews J also concluded that there was overwhelming evidence that the interview notes were created for the specific purpose of being shown to the SFO.

The Court disagreed, taking a more pragmatic approach. The Court found that:

- the fact that solicitors prepare a document with the ultimate intention of showing it to the other side (which, in any event, the Court found was not supported by the evidence in this case) does not automatically deprive the preparatory legal work of litigation privilege;
- legal advice given to head off, avoid or even settle reasonably contemplated legal proceedings remains protected by litigation privilege as much as advice on defending or contesting such proceedings would be; and
- while reputable corporations will certainly want to ensure high ethical standards for their own sake in their business, realistically, the legal sanction used to enforce appropriate standards in business is the criminal or civil law. As such, where a corporation is facing a clear threat of criminal investigation and prosecution, the reason the corporation is investigating whistleblowing allegations must be “*brought into the zone*” where the dominant purpose is to prevent or deal with litigation.

In addition, the Court found on the facts that, while ENRC had indicated to the SFO it would make “*full and frank disclosure*,” it did not in fact do so and it had never gone so far as to agree to disclose all of the materials it created in the course of its investigation to the SFO.

The Court noted that, had it been asked to approve a deferred prosecution agreement between ENRC and the SFO, ENRC's failure to make good on its promises to be full and frank would undoubtedly have counted against it. However, the Court was clear that this would not affect whether the Documents were covered by litigation privilege in the first place.

The Court found that the Documents were brought into existence for the dominant purpose of resisting or avoiding proceedings and so were protected by litigation privilege.

### *Legal Advice Privilege – Three Rivers 5 Criticized*

Legal advice privilege attaches to confidential communications between a client and its lawyers, acting in their professional capacity, in connection with the provision of legal advice.

The Court declined to determine whether the Documents were protected by legal advice privilege, in part because there was no need to do so, given its conclusions on litigation privilege, and in part because the Court took the view that in light of previous Court of Appeal authority in *Three Rivers 5*, any change to the test for legal advice privilege would have to be determined by the Supreme Court.

However, the Court did express a non-binding view on how it would have decided the matter if it could have done so.

The Court said that:

- *Three Rivers 5* decided that communications between an employee of a corporation and the corporation's lawyers could not attract legal advice privilege unless that employee was tasked with seeking and receiving such advice on behalf of the client; and
- it would have departed from *Three Rivers 5* if it had had the choice.

In particular, the Court noted that in the modern world, the law needs to cater for legal advice sought by large national and multinational corporations. It recognised that, where small corporations are concerned, the relevant information will normally be held by members of the corporation's board (who will almost always be authorised to seek and receive legal advice on the corporation's behalf), whereas this is less likely to be the case for multinationals. The Court's view was that, if *"a multi-national corporation cannot ask its lawyers to obtain the information it needs to advise that corporation from the corporation's employees with relevant first-hand knowledge under the protection of legal advice privilege, that corporation will be in a less advantageous position than a smaller entity seeking such advice."* The Court said that, whatever the rule is, it should be equally applicable to all clients, whatever their size or reach.

The Court also noted that English law was out of step with the common law in other jurisdictions on this question, referring specifically to decisions of the Singapore and Hong Kong Courts of Appeal. The Court said that it was *"undoubtedly desirable"* for the common law to remain aligned in different countries where its development was not specifically affected by different commercial or cultural environments. In the Court's view, *"legal professional privilege is a classic example of an area where one might expect to see commonality between the laws of common law countries, particularly when so many multinational companies operate across borders and have subsidiaries in numerous common law countries."*

As the Court felt unable to depart from *Three Rivers 5*, it concluded that Andrews J was right in deciding that legal advice privilege did not apply.

## *Impact of ENRC v SFO Court of Appeal ruling*

### **Lower bar for reasonable contemplation of criminal prosecution**

Decisions of the English court which narrowed the scope of legal professional privilege available to businesses involved in regulatory and criminal investigations had become the unfortunate norm. That trend is now starting to reverse.

The decision is positive news for those facing criminal or regulatory investigation and strikes a sensible balance on when litigation privilege should be available in those circumstances. The Court recognized a clear public interest in encouraging companies to investigate allegations from whistleblowers or investigative journalists under the protection of legal professional privilege before approaching the authorities: otherwise, companies might be tempted not to investigate such allegations at all.

Businesses are now in a position where, on the right facts, they can make a successful claim for litigation privilege at a much earlier stage than the first instance judgment suggested, and therefore obtain the benefit of protection for communications with third parties, including external expert advisors and employees (or ex-employees) who are not specifically tasked with seeking legal advice. The impact resonates beyond criminal proceedings: the Court's conclusions are relevant to internal investigations in anticipation of regulatory action by bodies such as the Financial Conduct Authority, Competition and Markets Authority or Her Majesty's Revenue and Customs (**HMRC**).

Businesses will still need to demonstrate, on the facts of each case, that civil litigation or criminal prosecution (or its equivalent) is reasonably in contemplation. But the fact that a corporation has not yet comprehensively established whether there is truth in claims of wrongdoing is no longer a bar to litigation being reasonably in contemplation.

Although the Court's conclusions of fact are specific to this case, they indicate the factors that might help in demonstrating a reasonable contemplation of adversarial litigation. The Court said that it was "*not sure*" that adversarial litigation would automatically be in contemplation whenever an entity is contacted by the SFO and noted that, where an SFO investigation is reasonably in contemplation, it is not inevitable that an SFO prosecution can also be said to be reasonably in contemplation.

Here, however, ENRC was able to provide contemporaneous documents and witness evidence that the Court found pointed clearly towards contemplation of a criminal prosecution if the self-reporting process was not successful in heading it off. Being able to point to examples of similar evidence will be helpful in future cases when seeking to establish a claim to litigation privilege. Factors which the Court considered relevant included:

- ENRC's receipt of a whistleblower email and subsequent appointment of external lawyers to investigate the allegations;
- contemporaneous views of both ENRC's general counsel and head of compliance (expressed by email) that they expected an SFO investigation, and actions taken within the company which were consistent with this view (e.g. upgrading its dawn raid procedures);
- contemporaneous views of the firm's lawyers that privilege would attach to the documents and that litigation was reasonably in contemplation; and

- the fact that, when the SFO wrote to ENRC, it asked ENRC to consider the self-reporting guidelines carefully, which included express statements that "*no prosecutor can ever give an unconditional guarantee that there will not be a prosecution,*" and the SFO's expression of similar views in later meetings.

One other practical consequence of the decision is that the SFO (and regulators) will have to confront the question of how they will deal with privileged documents involuntarily produced under statutory compulsion based on the (now overturned) first instance decision. It also remains to be seen whether the SFO will modify the content of its communications with targets of new investigations in response to this decision.

### Three Rivers still with us for now

Parties will also have to consider whether the Court of Appeal's non-binding comments disagreeing with *Three Rivers 5* should affect their approach in relation to legal advice privilege, including on the key issue of whether notes of interviews with employees are disclosable when created in circumstances which do not attract litigation privilege. The Court's decision provides a strong indication that it believes *Three Rivers 5* should be overturned, but a party may need to be willing to take that issue to the Supreme Court for resolution.

The SFO has announced that it will not be appealing.

# *Vietnam*



# Significant Expansion to Vietnam's Anti-corruption Regime

Vietnam remains a challenging jurisdiction for multinational companies to operate in terms of bribery and corruption risk related to business conduct. The Transparency International Corruption Perceptions Index scored Vietnam 35 (out of a possible 100) in 2017, ranking Vietnam at 107 out of 180 countries.

We wrote last year about the anti-corruption campaign underway in Vietnam that has focused on investigations into corrupt government officials, including leaders of prominent state-owned companies and financial institutions. Many view this latest anti-corruption drive as part of an effort to rehabilitate perceptions about the quality of management at state-owned enterprises in an environment where the government has been embarking on a major divestment campaign, the success of which will depend on Vietnam's ability to attract foreign investors. Foreign companies looking at investment into Vietnam or with existing businesses or joint ventures could be indirectly caught in this campaign if their Vietnamese business partners are also implicated.

Against this backdrop of a challenging risk environment for multinational companies to operate and the ongoing anti-corruption campaign, on January 1, 2018, Vietnam's new Penal Code (**Amended Penal Code**) became effective, introducing several significant changes to Vietnam's anti-corruption landscape, particularly with respect to private sector bribery. The Amended Penal Code sets out numerous corruption-related offenses. Those key changes are set out below:

– **Giving and promising bribes in the public and private sector:** The Amended Penal Code introduces a prohibition on “giving and promising of bribes” to any public or private office-holder, person, or organization. This offense may be committed by individuals only (i.e. there is no corporate liability), directly or through a third party. The penalty for giving or promising to give a bribe will largely depend on the value of the benefit given or promised. The minimum value of tangible benefits to trigger a violation of the law is VND2m (approximately USD 88). Penalties range from relatively low fines of VND20m (about USD 880) and six months' to 20 years' imprisonment.

- **Giving and promising bribes to foreign government officials:** A subset of the prohibition detailed above, the Amended Penal Code also introduces a new prohibition on bribery by individuals involving foreign government officials and officials with public international organizations. Again, there is no corporate liability for this offense. As a significant recipient of overseas development assistance and loans from multilateral development banks, this is an important change.
- **Brokerage of bribes:** The Amended Penal Code introduces the concept of “brokerage” of bribes in the private sector, which essentially amounts to criminalizing the conduct of a third party intermediary in the private sector who sits between a bribe payer and bribe recipient. If the broker voluntarily reports the bribe before the crime is discovered, the broker may be exempt from criminal responsibility.
- **Receiving bribes in the public and private sector:** Pursuant to the Amended Penal Code, government officials as well as individuals in the private sector are criminally liable for taking bribes. Penalties range from a minimum of two years' imprisonment to life imprisonment and death. The Amended Penal Code contains a VND2m minimum threshold at which receiving a bribe violates the law.
- **Corporate criminal liability for a variety of crimes but not corruption offenses:** Importantly, the Amended Penal Code does not extend corporate criminal liability to the crime of corruption. For both private-sector and public-sector corruption offenses, only individuals can be punished. The Amended Penal Code does, however, provide for corporate criminal liability for certain corruption-related offenses, such as money laundering, tax evasion, and terrorism financing where the offense is committed in the entity's name and for its benefit by those authorized to bind the company. Penalties for these



offenses will differ depending on the amount in issue. Other potential sanctions for companies include prohibition from operating in certain business areas and even termination of the company's ability to operate.

Of these changes to Vietnam's anti-corruption regime described above, the introduction of corporate criminal liability for offenses related to corruption (but not corruption itself), as well as the introduction of prohibitions on bribes offered to or accepted by any public *or* private office-holder, person, or organization are both significant changes. The move to prohibit private sector bribery is particularly important given that Vietnam's criminal laws have historically targeted the bribery of public officials only.

Questions remain as to how these changes will impact the conduct of business in Vietnam. For example, do the responsible authorities in Vietnam have the ability and the appetite to prosecute such offenses, particularly the new private sector offenses? Despite the imposition of severe criminal penalties for certain bribery offenses in Vietnam (up to and including the death penalty) and the politicization of anti-corruption efforts in recent years, Vietnam's enforcement record has remained poor. Visible enforcement will likely have an important deterrent effect.

Further, while the ongoing anti-corruption campaign in Vietnam has focused mainly on Vietnamese officials, foreign investors also need to be alert and remain in compliance with local law given their newly heightened exposure to criminal liability.

At a minimum, it is likely that the Amended Penal Code's introduction of criminal liability for private sector corruption will have flow-on effects for how multinational companies manage compliance in Vietnam. The Amended Penal Code will potentially serve as a deterrent to individuals who may be engaging in or contemplating engaging in improper conduct. It may also help organizations carry out internal investigations of wrongdoing as employees who face the real possibility of criminal sanction in the private sector may feel compelled to cooperate and disclose the full extent of any wrongdoing in the hope of avoiding prosecution. It is recommended that organizations in Vietnam should educate their employees on the new law as part of their overall internal anti-corruption training and compliance efforts.



Appendix:  
*Summaries of  
Corporate FCPA  
Enforcement Actions  
in 2018*

# Elbit Imaging



## 1. Introduction

- 1.1 On March 12, 2018, Elbit Imaging Ltd (**Elbit**) agreed to pay USD500,000 to the U.S. Securities and Exchange Commission to settle violations of the U.S. Foreign Corrupt Practices Act's books and records and the internal controls provisions. The SEC alleged that Israel-based Elbit and its subsidiary, Plaza Centers NV (**Plaza**), paid millions of dollars to third party offshore consultants and a sales agent "for services," without knowing if the services were ever provided. The case was resolved through an internal administrative order and did not go to court.
- 1.2 The SEC Administrative Proceeding against Elbit provides an important reminder of the bribery and corruption risks present in the real estate investment and development sector. It also serves as a reminder of the expansive reach of the FCPA's books and records provision as bribes paid to government officials do not have to be identified/proven by the SEC for a violation of the FCPA's books and records to be established, and business activities in the U.S. can result in violations of the FCPA's books and records provision.



## 2. Jurisdictional basis

- 2.1 Elbit is listed on the NASDAQ and is therefore considered an issuer under the FCPA.
- 2.2 Elbit exerts functional control over its subsidiary, Plaza, and between 2007 and 2012 Plaza's financial statements were consolidated into Elbit's own financial statements for the purpose of SEC reporting. Plaza is incorporated in the Netherlands.



## 3. Summary background

- 3.1 Between 2007 and 2012, Elbit and Plaza directly and indirectly paid approximately USD27m to third party offshore consultants and sales agents for their apparent services in relation to a real estate development project in Romania and the sale of a large portfolio of real estate assets in the United States.
- 3.2 Elbit and Plaza made the payments even though they had no evidence that the consultants and sales agents had actually provided the contracted services. They failed to record the payments in a manner that accurately and fairly reflected the nature of the payments in their books and records and failed to devise and maintain internal accounting controls sufficient to provide reasonable assurances that company funds would only be used for legitimate corporate purposes.



## 4. Detailed background

### 4.1 Romanian shopping mall development project

- (a) In 2006, Plaza entered into a contract with a third party offshore entity (**Consultant 1**) to assist procurement of an invitation from the Romanian government to participate in a real estate development project involving a shopping mall, and to acquire the government approvals needed to perform development work on the shopping mall. The SEC did not identify any evidence to suggest Plaza conducted any due diligence on Consultant 1. There was also no evidence or documentation showing that Consultant 1 provided any services in connection with the purchase of the interest in the shopping mall development, or with the agreement to develop the site.

- (b) In 2011 another offshore entity (**Consultant 2**) was engaged under the guise of providing consulting services in relation to the same shopping mall project in Romania. The consultant was engaged to assist Plaza in acquiring all government approvals to develop the site, and to arrange for the purchase of an additional 15% interest in the project from the Romanian government. Again, the SEC identified no evidence to suggest that Plaza conducted any due diligence on Consultant 2, nor that Consultant 2 performed any work related to acquiring the government approvals or the purchase from the Romanian government of the additional interest in the site.
- (c) Altogether, around USD14m was paid to Consultants 1 and 2 over five years. Plaza's senior management authorized the payments even though documentation supporting the payments did not identify the services the consultants provided.
- (d) The SEC found that Plaza entered the payments into its books and records as legitimate business expenses for services rendered when some or all of the funds may have been used to make corrupt payments to Romanian government officials.
- (c) A day after the sales agent contract was executed, Sale Agent A entered into a subcontract with another offshore entity (**Sales Agent B**), assigning its rights and obligations under the sales agent contract to Sales Agent B. At the time, Sales Agent B was indirectly beneficially owned by Executive A. This was not disclosed to Elbit or Plaza.
- (d) Approximately a month and a half prior to the execution of the contract with Sales Agent A, the JV hired another financial institution to serve as its financial advisor for the shopping center portfolio sale. The financial advisor was retained to provide nearly the same services to the JV as Sales Agent A agreed to perform for Elbit and Plaza.
- (e) The financial advisor fulfilled its obligations to the JV pursuant to its contract. The SEC did not identify any evidence suggesting Sales Agent A or B did anything similar in respect of Elbit and Plaza.
- (f) The JV sold the Portfolio, and Elbit and Plaza paid Sales Agent A USD13m, nearly double that paid to the financial advisor by the JV. Elbit and Plaza made these payments even though documentation supporting the payments did not identify any services that the consultants provided. Sales Agent A then paid Sales Agent B, without the knowledge of employees at Elbit or Plaza, other than Executive A.

#### 4.2 Joint venture sale of shopping center assets in the U.S.

- (a) Separately, in 2011 a joint venture of investors (**JV**) sought to sell a portfolio of 47 shopping center real estate assets in the United States. Elbit, and Plaza held a 45% interest in the JV.
- (b) Without the knowledge of the other investors in the JV, Elbit and Plaza together entered into a contract with a third party offshore entity (**Sales Agent A**) to assist in selling the shopping center portfolio. No due diligence was conducted on Sales Agent A. Further, an executive from Elbit (**Executive A**) did not obtain a second signature for the sales agent contract with Sales Agent A, as required by Elbit's signature authorization policy and executed the contract on behalf of Elbit.



### 5. Key takeaways

- 5.1 Due diligence on third parties** – This case emphasizes the importance of conducting due diligence on third parties and maintaining evidence that shows third parties have in fact provided the contracted services.

### 5.2 Follow existing internal policies and procedures

– The SEC identified the fact that the contract with Sales Agent A was not executed in accordance with Elbit's signature authorization policy as a failure of internal controls.

### 5.3 ABC (Anti-Bribery & Corruption) policies, procedures and training are critical

– Elbit and Plaza did not have policies and procedures in place to detect corruption risks and provided little if any anti-corruption training to employees during the relevant time period. The SEC found this to be evidence of inadequate internal controls.

### 5.4 Independent oversight of contractual arrangements

– According to the SEC, Plaza's legal department had limited involvement with, and supervision of, contracts entered into between Plaza and third party consultants or agents. The Administrative Proceeding emphasized the importance of independent oversight of contracts/agreements.

### 5.5 No evidence of bribes paid to government officials

– This case is another example of the SEC bringing FCPA books and records/internal accounting controls charges when there is no actual evidence of bribes paid to government officials.

### 5.6 Onus on FCPA investigation subjects to prove they have adequate internal controls in place

– This case shows the onus is on the subject of an FCPA investigation to provide evidence of adequate internal controls and mechanisms in place that would counter the presumption that bribes had been paid.

### 5.7 FCPA captures conduct/business in the United States

– This case is an example of the FCPA's books and records provision being used to capture domestic conduct in the U.S. where no foreign government officials are involved. The books and records provision can and has been used expansively to catch conduct not related to interactions with foreign government officials.

### 5.8 Embezzlement captured by the FCPA's books and records provisions

– This case also shows that offenses other than bribery can be captured by the FCPA's books and records provisions. Although it is unknown where the approximately USD27m paid to the consultants and sales agents ended up, there is a possibility the funds were embezzled by Executive A rather than being used to bribe government officials. The books and records provisions of the FCPA does not require bribery of a foreign government official for a violation to be found; any underlying criminal offense (eg embezzlement) that results in inaccurate books and records will be enough to establish a violation of the books and records provision of the FCPA.

### 5.9 Mitigating factors

– Elbit self-reported, cooperated and conducted an internal investigation, and voluntarily provided detailed reports to SEC staff. The cooperation contributed to limiting Elbit's penalty to USD500,000.

# Transport Logistics International



## 1. Introduction

1.1 On March 12, 2018, Transport Logistics International, Inc. (**TLI**) entered into a deferred prosecution agreement with the DOJ after the DOJ filed a single count information in the District of Maryland against TLI alleging conspiracy to violate the FCPA's anti-bribery provisions. TLI's penalty was reduced from USD21m to USD2m because of its inability to pay a fine.

1.2 The DOJ has also taken action against TLI's senior management and the foreign government official involved in the scheme:

- (a) On January 10, 2018, the DOJ filed an indictment in the District of Maryland against TLI co-president Mark Lambert, which charged Lambert with one count of conspiracy to violate the FCPA and to commit wire fraud, seven counts of violating the FCPA, two counts of wire fraud and one count of international promotion money laundering. On January 25, 2018, Lambert pled not guilty. The case is ongoing.
- (b) On June 17, 2015, TLI co-president Daren Condrey pleaded guilty to conspiracy to violate the FCPA's anti-bribery provisions and commit wire fraud.
- (c) On August 31, 2015, Vadim Mikerin, a Russian government official and director of JSC Techsnabexport (**TENEX**) that supplied uranium and uranium enrichment services to nuclear power companies throughout the world on behalf of the government of the Russian Federation, pleaded guilty to conspiracy to commit money laundering involving violations of the FCPA. Mikerin was sentenced to 48 months in prison on December 15, 2015.



## 2. Jurisdictional basis

2.1 TLI is a U.S. company headquartered in Maryland and is therefore considered to be a domestic concern under the FCPA.



## 3. Summary background

3.1 Between 2004 and 2014, TLI, along with Condrey and two co-conspirators, agreed to make corrupt payments of over USD1.7m to Mikerin in order to obtain and retain business with TENEX, a subsidiary of Russia's State Atomic Energy Corporation. The payments were funnelled through at least three offshore shell companies. These offshore companies did not have any legitimate business relationships with TLI. The payments were reimbursed via fake invoices from TENEX for services that TENEX never performed for TLI.



## 4. Detailed background

- 4.1 According to the DPA, from 2004 to 2014, TENEX contracted with TLI to transport uranium to and from the United States.
- 4.2 Mikerin communicated directly with a TLI executive (**Co-Conspirator One**) about bribe payments from TLI to secure business with TENEX. In 2009, both Condrey and Lambert were aware that Co-Conspirator One was making corrupt payments to Mikerin in order for TLI to continue to win contracts from TENEX. Condrey and Lambert then agreed to enter into the conspiracy that they would continue to make corrupt payments to Mikerin. These payments were made to Mikerin via several offshore bank accounts.

4.3 In order to disguise the bribery scheme, Condrey, Lambrey, Mikerin and Co-Conspirator One would use code words like “lucky figures,” “lucky numbers,” and “cake” to refer to these corrupt payments.

4.4 In addition, to further conceal the corrupt payments, Condrey, Lambert and others allegedly caused the preparation of fake invoices from TENEX to TLI that described services TENEX never performed.

4.5 Mikerin allegedly conspired with the TLI executives to wire payments for those purported services to bank accounts in Cyprus, Latvia, and Switzerland.



## 5. Key takeaways

### 5.1 DOJ takes into account TLI's inability to pay

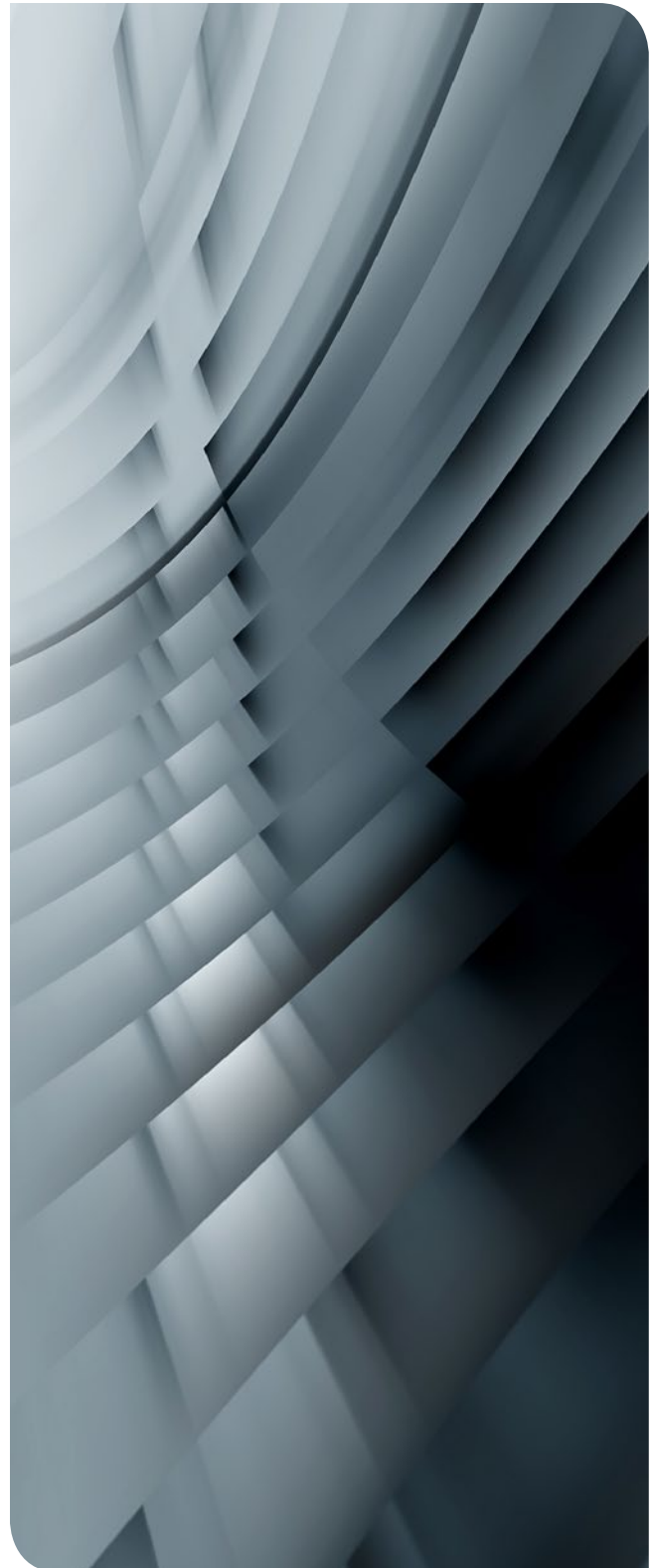
**the assessed fine** – USD21.4m was the fine assessed against TLI pursuant to the U.S. sentencing guidelines, however, because that amount would “substantially jeopardize the continued viability of the Company” it was reduced to USD2m.

### 5.2 Review your internal controls, particularly invoice

**payment systems** – Following an investigation, TLI's compliance program enhancements focused on its invoice payment controls. TLI adopted policies prohibiting: (i) payment to bank accounts that are not in the name of the company/vendor who is owed the payment; (ii) payments to a country other than where the individual/company resides or where the services are rendered; and (iii) payments for rebates, discounts, commission or remuneration that are not specified in bids or contracts. TLI also adopted payment controls requiring multiple reviews for payment requests and two signatures on check registers.

### 5.3 The DOJ is focused on prosecutions of individuals

– In this case, the DOJ prosecuted three individuals who were implicated in TLI's conduct. This suggests that the DOJ is still very much committed to the strategy of individual prosecutions set out in the Yates Memo.



# Kinross



## 1. Introduction

1.1 On March 26, 2018, Kinross Gold Corporation (**Kinross**), a Canadian gold mining company, agreed to pay USD 950,000 for violating the books and records and internal accounting control provisions of the FCPA as a result of its “repeated failure” to enact anti-corruption compliance programs and adequate accounting controls at two recently acquired subsidiaries in Africa.



## 2. Jurisdictional basis

2.1 Kinross is listed on the New York Stock Exchange (**NYSE**) and is therefore considered an issuer under the FCPA. Kinross operates in North and South America, West Africa, and Russia.

2.2 Tasiast Mauritanie Limited S.A. (**Tasiast**) is a wholly owned subsidiary of Kinross and Chirano Gold Mines Limited (**Chirano**) is a majority-owned (90%) subsidiary of Kinross. Tasiast operates in the Mauritania and Chirano has operations in Ghana. Both subsidiaries were acquired by Kinross from another Canadian-based mining company, Red Back Mining, Inc (**Red Back**). Between September 2010 and 2014, both Tasiast and Chirano’s financial statements were consolidated into Kinross’ own financial statements for the purpose of SEC reporting.



## 3. Summary background

- 3.1 Kinross conducted due diligence prior to the acquisition of Tasiast and Chirano in 2010 but failed to promptly address the inadequacy of the internal controls at both entities after the acquisition that had been identified during the pre-closing due diligence. For several years after the acquisitions closed, the internal audit team at Kinross repeatedly flagged the lack of anti-bribery and corruption compliance programs and/or internal controls at both subsidiaries and advised the implementation of extensive remediation steps in their audit reports. While Kinross senior management at the two subsidiaries agreed to swiftly implement the recommended remediation, it failed to actually implement such internal controls in a timely manner, taking almost three years to start implementing the proposed program enhancements.
- 3.2 After implementing the recommended internal controls, Kinross awarded a ~USD50m logistics contract to a shipping company preferred by a high-level Mauritanian government official, despite concerns that the company was a high cost provider with poor technical capabilities. This was in contravention of Kinross’ bidding and tendering procedures that had been implemented at the two subsidiaries.
- 3.3 In the same year, Kinross failed to conduct required enhanced due diligence when hiring an independent consultant who was well connected with the Mauritanian government: The consultant acted as a liaison with high-level Mauritanian government officials and facilitated Kinross’ logistics contracts. Again, this was in contravention of existing Kinross policy that had been implemented at the subsidiaries.
- 3.4 The SEC order does not allege that these books and records and internal controls and books weaknesses led to the payment of bribes to any foreign government officials.





#### 4. Detailed background

- 4.1 On September 17, 2010, Kinross acquired Tasiast and Chirano's assets and mining operations in Mauritania and Ghana from Red Back. In the few months prior to the purchase of the mines from Red Back, Kinross conducted due diligence on Tasiast and Chirano and Red Back acknowledged a lack of anti-bribery and corruption compliance programs and/or internal controls at the subsidiaries.
- 4.2 Following the acquisition, Kinross failed to address in a timely manner the lack of anti-bribery and corruption compliance programs and/or internal controls at Tasiast and Chirano pertaining to:
- (a) the procurement and payment of vendors;
  - (b) bribery and corruption risks associated with the high percentage of vendors that were controlled by local government officials and/or their relatives;
  - (c) contracts with vendors made by low-level employees; and
  - (d) petty cash payments without appropriate approval.
- 4.3 In April 2011, the internal audit team concluded that internal controls concerning vendor selection and disbursement at both subsidiaries were not sufficient to accurately assess the commercial transactions. The internal audit team specifically pointed out that the internal accounting and disbursements system did not include sufficient details such that at both subsidiaries it was impossible to identify suspect payments such as excessive rebates and discounts, advanced payments, government commissions and unjustified business expenses. Kinross' management team failed to take any immediate action after becoming aware of the issues identified by the internal audit team. In April 2012, the internal audit team issued a nearly identical report reaching the same conclusions.
- 4.4 In January and February 2012, the internal audit team conducted reviews at Chirano and Tasiast and identified issues that required significant remediation at mines owned by the subsidiaries. These issues included, among other things:
- (a) a lack of formalized procedures for contract approval and bidding/tendering;
  - (b) a lack of a fully functioning internal accounting and disbursements system, whereby most disbursements were made without approval by the required signatories or such signatures did not provide sufficient detail to verify whether appropriate approvals were provided; and
  - (c) a failure to maintain supporting documentation required for disbursements, including invoices, purchase orders, and/or receipts. Some purchase orders were created after the invoices were received.
- 4.5 In 2012 and 2013, the internal audit team continued to conduct further reviews at Chirano and Tasiast and found little improvement had been made in relation to the issues identified by the team earlier. In fact, as noted by the internal auditor in July 2013, 100% of the reviewed contracts at Chirano were awarded directly by the functional area or department, rather than by the procurement department. The SEC stated that this was an indication that the practice of low level employees awarding contracts without independent control or oversight continued nearly three years after Kinross assumed control of Chirano.
- 4.6 The SEC settlement also stated that as a result of the weaknesses in the internal controls, there were at least three occasions where payments were made without reasonable assurances that the payments were for their stated purpose or with management's approval:
- (a) Between 2012 and 2014, personnel at Chirano paid a Ghanaian government customs officer for travel expenses although there was no evidence to suggest that the officer travelled to visit the company's mine;

- (b) In 2012, Kinross paid USD 12,000 to a third party consultant without a formal written agreement. Personnel at Kinross used petty cash to pay the third party consultant without obtaining any documentation to evidence services provided by the consultant. During that period, there was a delay in Kinross obtaining a mining production permit from the Ghana Environmental Protection Agency (**Ghana EPA**). About a month after the payment to the consultant, the Ghana EPA approved the mining production permit. The SEC stated that Kinross' books and records did not accurately reflect the nature or intended recipients of the payment.
- (c) Between 2012 and 2015, Kinross paid a third party consultant, who was a former government official, a fee to expedite the process for issuing visas and work permits. As a result, the processing time for Kinross' employees' visas and work permits decreased from ten weeks to three weeks. Again, the fees to the consultant were paid via petty cash (~USD1,000 per visa or permit). The SEC stated that there was no evidence to suggest that actual services were provided by the consultant and no "reasonably detailed" description of the fees could be identified in Kinross' books and records.
- 4.7 Kinross' Code of Conduct prohibits employees providing improper payments to government officials. In 2013, Kinross took steps to enhance its internal controls to ensure that its transactions did not violate both the FCPA and Kinross' own Code of Conduct. However, after implementing new internal controls, the SEC found that Kinross failed to maintain these internal controls on at least two occasions.
- 4.8 In a bidding contract in April 2014, instead of awarding a logistics contract to an international shipping company that offered the lowest price and possessed the best ability to fulfill the technical requirements of the contract, Kinross awarded the contract to a shipping company that was preferred by a high-level Mauritanian government official. During a presentation by Kinross' regional management in West Africa to Kinross' senior management, it was clear that senior management made a conscious decision to award the contract despite being aware that the company was unable to satisfy its technical requirements.
- 4.9 In 2014, an individual who was well connected with high-level government officials in Mauritania approached Kinross and offered to work for Kinross. The individual explicitly mentioned that he/she could establish a continuing relationship between Kinross and a particular high-level government official who had the power to influence government decisions related to logistics contract awards. The individual was ultimately hired as an independent consultant and was paid ~USD715,000 between September 2014 and August 2015. The SEC stated that Kinross failed to conduct heightened due diligence on the individual despite being aware of the individual's connections with the government official. The SEC also stated that Kinross should provide training to senior management so they recognize bribery and corruption risks when hiring individuals to work as liaisons with government officials.



## 5. Key takeaways

### 5.1 Conducting pre- and post-acquisition due diligence

– The most important lesson from this case is the requirement for timely and continued remediation of bribery/corruption issues when identified in pre- and post-acquisition due diligence.

### 5.2 Conducting increased due diligence on high risk third parties

– The SEC emphasized that heightened due diligence should be conducted on third parties where there are higher potential risk indicators, eg, direct and frequent interactions with government officials.

### 5.3 Verifying services performed under contracts

– Companies should maintain evidence that shows third parties have provided the contracted services.

### 5.4 Reviewing payments from petty cash accounts

– Payments to third parties using companies' petty cash accounts should be reviewed carefully. This case is an example of petty cash potentially being misused as a tool to funnel bribes to government officials.

### 5.5 Following recommendations of internal audits

– Senior management should address and remediate internal controls deficiencies identified by internal audits in a timely manner.

### 5.6 Following existing internal policies and procedures

– The SEC identified that Kinross' lack of heightened due diligence on third parties was in breach of the company's Supply Chain policy and as a result, a failure of internal controls.

### 5.7 Providing training to senior management

– The decision by senior management to hire individuals to work as a liaison with government officials indicated a lack of ABC training of senior management. The SEC found this to be evidence of a failure to maintain sufficient internal controls.

### 5.8 No evidence of bribes paid to government officials

– This case is another example of the SEC bringing FCPA books and records and internal accounting controls charges where there was no actual allegation of bribes paid to government officials.

# Dunn & Bradstreet



## 1. Introduction

- 1.1 On April 23, 2018 the SEC ordered Dun & Bradstreet Corporation (**D&B**) to pay a USD7m disgorgement and USD2m civil penalty to settle FCPA charges arising from improper payments made by two Chinese subsidiaries, Shanghai Huaxia Dun & Bradstreet Business Information Consulting Co., Limited (**HDBC**) and Shanghai Roadway D&B Marketing Services Co., Ltd (**Roadway**).
- 1.2 Prior to this order, the DOJ issued D&B with a declination pursuant to the FCPA Corporate Enforcement Policy.



## 2. Jurisdictional basis

- 2.1 D&B is a corporation organized under the laws of the state of Delaware and is listed on the New York Stock Exchange. It is therefore considered an issuer under the FCPA.
- 2.2 D&B is a 51% majority shareholder of Chinese limited liability company, HDBC. HDBC's books, records and financial accounts are consolidated into D&B's books and records and reported by D&B on its financial statements.
- 2.3 Roadway, a Chinese limited liability company, was a majority-owned (90%) subsidiary of D&B during the relevant time period under investigation. Roadway's books, records and financial accounts were consolidated into D&B's books and records and reported by D&B on its financial statements.



## 3. Summary background

- 3.1 D&B is a global provider of business information and the acquisition of business data is a core component of its business model. Between 2006 and 2012, D&B's subsidiaries, HDBC and Roadway, made unlawful payments using third party agents to obtain business data.
- 3.2 HDBC and Roadway failed to accurately record these unlawful payments in their books and records, which were consolidated into D&B's books and records. D&B failed to devise and maintain internal accounting controls to detect or prevent the improper payments.



## 4. Detailed background

### 4.1 HDBC Joint Venture

- (a) In 2006, D&B China and Huaxia entered into a joint venture which resulted in the formation of HDBC. Before this time, D&B's Greater China management team conducted due diligence on Huaxia's data and operations, namely, data acquisition and sources of data. The report found that Huaxia used government connections and paid bribes to obtain restricted data, including financial statement information from the Chinese State Administration of Industry and Commerce (**AIC**). D&B failed to address these findings, responding only by providing a short FCPA training session and an anti-bribery questionnaire to Huaxia executives.
- (b) Access to AIC data is highly regulated under Chinese law. D&B Greater China's management and staff knew of the commercial use restrictions and were aware of the possibility of obtaining restricted financial statement data through bribery. To mitigate the risk associated with such actions, HDBC used third party agents to unlawfully obtain financial statement data from AIC. However,

D&B's due diligence efforts also indicated that Huaxia directly obtained certain non-public AIC business data through unofficial arrangements.

- (c) Following the closing of the deal, a D&B Greater China manager stopped the practice of Huaxia employees directly making improper payments in favor of using third party agents.
- (d) In 2008, D&B considered eliminating the use of agents and allowing HDBC employees to directly obtain data from AIC officials in order to reduce costs. However, HDBC was concerned that by using this method they would be unable to obtain a proper tax receipt. Consequently, they explored ways to generate fake tax receipts for the unlawful payments made to AIC officials. D&B ultimately decided to maintain the practice of using third party agents to acquire data and continued this practice until mid-2012 when it was removed as a remedial measure.

#### 4.2 Roadway Subsidiary

- (a) In June 2009, D&B acquired 90% of the shares of Roadway.
- (b) During the due diligence process, Roadway disclosed to D&B that it was not able to guarantee that unlawful payments had not been made to obtain restricted data. D&B did not conduct further due diligence to verify these payments and, post acquisition, Roadway continued to obtain data through improper payments made by agents.
- (c) In March 2015, a television news program featured a Roadway sales executive who made statements that Roadway sold data containing citizen information to companies for marketing purposes. Shanghai police subsequently raided Roadway's offices. As a result, in January 2013, Roadway and five of its employees were convicted with illegally obtaining private information of Chinese citizens.

- (d) In addition to these convictions, from July 2009 through to March 2012, Roadway employees and agents made improper payments to customer "decision-makers" to obtain and retain business. These expenses were inaccurately recorded in Roadway's books and records as legitimate promotion expenses.



### 5. Key takeaways

- 5.1 SEC's ability to order disgorgement not removed by a declination from the DOJ** – This case highlights that the receipt of a declination by the DOJ will not impede the SEC's ability to order disgorgement. In this case, disgorgement was the key remedy in the absence of prosecution for anti-bribery violations. In addition, civil penalties may still be levied against the corporate by the SEC, and will not be nominal where there has been a failure to remedy issues as soon as practicable.
- 5.2 Due diligence** – This case emphasizes the importance of conducting thorough due diligence prior to an acquisition of entities in high risk and highly-regulated jurisdictions, and responding to the findings of that due diligence in a timely manner.
- 5.3 Post-closing integration** – Related to the immediately preceding point, this case is another example of the need to ensure the development and implementation of a post-closing integration plan for newly acquired subsidiaries.
- 5.4 Access to data** – In this case, the SEC penalized a company for obtaining data in breach of local laws and for taking steps to conceal payments made to obtain that data.

# Panasonic



## 1. Introduction

- 1.1 On April 30, 2018, Panasonic Avionics Corporation (**PAC**), a wholly owned subsidiary of Panasonic Corporation (**Panasonic**), agreed to pay the SEC and the DOJ USD280m to settle allegations of violations of the FCPA. The settlement related to payments to consultants of PAC's U.S. in-flight entertainment products in the Middle East and Asia, and involved several violations of the internal accounting controls provisions of the FCPA. PAC was also charged by the DOJ with one count of "knowingly and wilfully causing the falsification of the books, records and accounts" of Panasonic and accepted the imposition of an independent compliance monitor for a period of two years.
- 1.2 The PAC enforcement action provides an important reminder of the reach of the FCPA's books and records provisions and the importance of adequate due diligence of sales agents in high risk jurisdictions.



## 2. Jurisdictional basis

- 2.1 Until April 22, 2013 (and again for a brief period between 2015 and 2016), Panasonic was listed on the NYSE and was therefore considered an issuer under the FCPA.
- 2.2 PAC is a Delaware corporation headquartered in Lake Forest, California and is considered a "domestic concern" for the purposes of the FCPA. PAC specialises in providing in-flight entertainment products and services to airlines. During the relevant period, PAC's books and records and financial accounts were fully consolidated into Panasonic's financial statements.



## 3. Summary background

- 3.1 Between 2008 and 2014, PAC paid USD 875,000 to a former government official in exchange for valuable information in relation to a supply agreement between PAC and a government airline in the Middle East where the former government official was a key executive.
- 3.2 From at least 2007 through to at least January 2014, various purported consultants were engaged and paid by PAC, using a slush fund designated as the "Office of the President Budget" (the **President Budget**), in exchange for non-public information regarding airline customers and PAC competitors.
- 3.3 In early 2007, PAC introduced due diligence screening procedures for its sales agents in the Middle East and Asia, including in China. However, several sales agents that failed or refused to complete PAC's vetting process were secretly retained by PAC employees through sub-agreements with a Malaysia-based sales agent that had passed the company's screening process. PAC falsely recorded the payments to the sub-agents in its books and records as legitimate payments to the Malaysia-based sales agent.



## 4. Detailed background

### 4.1 Bribery in the Middle East Region

- (a) In 2004, PAC signed a ten year supply agreement (valued at over USD1bn) with a government airline in the Middle East (the **Government Airline**) for the provision of in-flight entertainment products and services to the Government Airline's fleet.
- (b) In July 2007, a PAC sales representative (**Sales Rep**) began negotiating a consulting position with a foreign government official at the same time as the foreign official was involved in negotiating a lucrative amendment to the supply agreement on behalf of the Government Airline.

- (c) When the government official retired from the Government Airline, he was offered a position as a PAC consultant for USD 200,000 per year, plus travel expenses.
- (d) Payments to the government official (which ultimately amounted to USD 875,000) were made with the express approval of a PAC executive through an unrelated third party vendor (**Vendor**). The payments were made regularly over a period of six years, even though the government official provided little to no actual services to PAC. Over the course of his engagement, PAC earned over USD92m in profits from the Government Airline, attributable to 12 programs over which the government official had some influence.
- (e) PAC's internal audit group ultimately identified the payments to the government official as "high risk," stating that the, "[Vendor] consultant payment should be carefully reviewed in light of FCPA regulation due to lack of clarity in deliverables." The payments were also mischaracterized as "consultant payments" on PAC's general ledger and as "selling and general administrative expenses" in Panasonic's books. However, none, or very few, of the payments were for actual consulting services.
- (f) PAC continued to employ the Sales Rep until 2016, despite learning in 2015 that he had destroyed electronic data on devices provided to him by PAC after he became aware of a subpoena issued by SEC staff.

#### 4.2 Retention of Consultants Through the Office of the President Budget

- (a) Between 2007 and 2013, PAC paid a former employee who had worked as a consultant to one of its largest American airline customers USD 825,000 in exchange for non-public information regarding the airline customer and PAC's competitors. The former PAC employee frequently sent such information to PAC employees through emails that were marked "Confidential" or "Do Not Forward."

- (b) All payments to the consultant were made from the President Budget and falsely recorded in PAC's general ledger as legitimate consulting payments to the Vendor. In exchange, between 2008 and 2013, PAC earned over USD22m in profits from business with the American airline customer.
- (c) The DOJ noted that the payments were made in the absence of effective internal accounting controls, and without sufficient documentation to substantiate the nature and value of the services provided by the consultant.
- (d) Despite knowing that PAC was recording these payments as legitimate consulting expenses in its books and records, a PAC executive falsely made a Sarbanes-Oxley certification that PAC's financial reporting controls were functioning effectively.

#### 4.3 Retention of Sales Agents

- (a) In early 2007, PAC began to implement due diligence procedures for the screening of sales agents, including those agents who had established relationships with PAC. At the time, PAC's procedures required all sales agents to obtain a TRACE compliance certification.
- (b) Despite this requirement, a number of sales agents who did not obtain a TRACE certification or refused to participate in the new due diligence process were secretly rehired by PAC employees through an existing and approved sales agent based in Malaysia. The Malaysia-based agent entered into sub-agreements with the relevant sales agents and, in exchange for a fee, acted as a conduit for payments to the sub-agents.
- (c) PAC falsely recorded such payments in its books and records as legitimate commission payments to the Malaysia-based sales agent.
- (d) The above practice continued unobstructed until at least 2015. From 2008 to 2015, PAC paid over USD10m to the Malaysia-based sales agent for the benefit of at least 13 different unapproved sub-agents.

- (e) Despite warnings, PAC's personnel took no action to prevent the continued use of the Malaysia-based agent to funnel payments to unapproved sub-agents. Moreover, PAC's compliance personnel lacked appropriate qualifications and training. As a result, they failed to act on numerous red flags in connection with the retention of sales agents.

#### 4.4 Fraudulent Reporting of Revenue

- (a) According to the SEC, PAC's revenue recognition policy, consistent with Generally Accepted Accounting Principles (GAAP), provided guidance on the recognition of certain revenue in PAC's books.
- (b) Despite this policy, as early as 2006, several PAC employees backdated certain customer contracts to recognize revenue in time periods prior to when those contracts were actually signed.
- (c) For example, in 2012, PAC and the Government Airline were unable to reach an agreement regarding an amendment to their ten year supply agreement. However, various PAC employees (with senior management's approval) falsely represented to PAC's auditors that the contract had been signed prior to June 30, 2012.
- (d) As a result of PAC's premature recognition of revenue, Panasonic materially overstated pre-tax income by at least USD38.5m, or 9%, and net income by at least USD22.4m, or 16%, in its Form 6-K for the first quarter of 2012.



### 5. Key takeaways

**5.1 Follow and maintain existing internal policy, procedures and accounting controls** – PAC continued paying sales agents even after its internal auditors identified such payments as high risk and noted that such agents were retained without the oversight of the procurement team. In addition, PAC designated a special slush fund under the guise of the “Office of the President Budget” to funnel payments to such agents. The DOJ and SEC found this to be evidence of inadequate internal accounting controls. Companies should heed the warnings of their auditors and adequately investigate any red flags identified.

**5.2 Due diligence and concealment of the use of sales agents** – This case emphasizes the importance of ensuring that due diligence policies are implemented adequately and compliance with such policies is monitored on an ongoing basis. At PAC, there was clearly a failure of internal controls, with employees hiding payments to corrupt agents through the use of an approved Malaysia-based agent. There was no requirement for the agent to disclose sub-agent relationships or for sub-agents to be re-screened. Companies should ensure that their due diligence policies cannot easily be circumvented and that they monitor all agents for material changes in ownership, structure and commission rates, as well as any use of sub-agents.



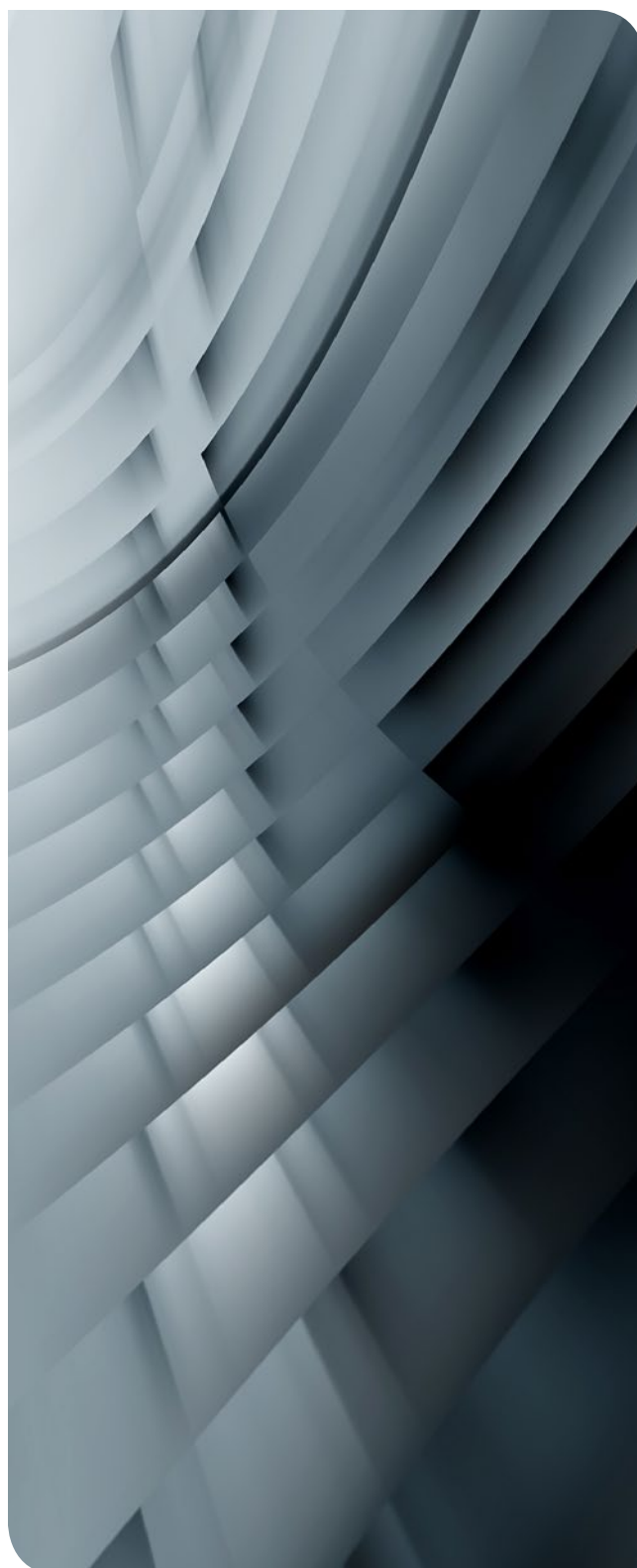
**5.3 Accurate recording of consulting payments in a company's books and records**

– Payments to sales agents should always be accurately recorded in a company's books and records. The company should always seek to obtain sufficient documentation to substantiate the nature of an agent's services and the value of such services.

**5.4 Corporate slush funds** – PAC created a slush fund of money to pay its sales agents. The President Budget exceeded several hundred thousand dollars annually and was overseen by a PAC executive who had complete control over how the funds were spent. The President Budget was also never meaningfully reviewed or approved by any Panasonic or PAC personnel. Such slush funds should be a clear red flag for any compliance professional.

**5.5 Compliance training is critical** – PAC's personnel lacked appropriate qualifications and training, and as a result failed to act on numerous red flags in connection with the retention of sales agents. The misconduct also reached the upper echelons of the company, with senior PAC executives involved in the bribery scheme and knowingly falsifying the company's books and records. If enough personnel had been adequately trained on the company's compliance controls and policies, the conduct may have been spotted and discontinued earlier.

**5.6 Mitigating factors** – Panasonic undertook remedial efforts and cooperated with DOJ and SEC investigations. In particular, it replaced the senior PAC executives involved in the accounting and internal controls violations, established an Office of Compliance and Ethics led by a new Chief Compliance Officer, implemented new compliance and accounting procedures, and enhanced internal accounting controls to prevent and detect similar types of misconduct. As a result, it received a more lenient penalty.



# Société Générale/Legg Mason



## 1. Introduction

- 1.1 On June 4, 2018, Société Générale S.A. (**SocGen**) and Legg Mason Inc (**Legg Mason**) agreed to pay almost USD650m in criminal penalties to resolve FCPA charges in relation to bribery of Libyan officials in the Gaddafi era. SocGen will pay a total of USD585m to the DOJ and French regulator Parquet National Financier (**PNF**), and Legg Mason will pay a penalty of USD64.2m to the DOJ. SocGen also paid a fine of USD750m to resolve other charges relating to the manipulation of Libor.
- 1.2 Separately, on August 27, 2018, in relation to the same Libyan bribery scheme, Legg Mason also agreed to pay more than USD34m (including USD27.6m in disgorgement damages and USD6.9m in prejudgment interest) to the SEC. The SEC found that Legg Mason had breached the internal accounting controls provision of the Securities Exchange Act of 1934.

## Société Générale



## 2. Summary background—FCPA

- 2.1 According to the DOJ, between 2004 and 2009, SocGen paid bribes to Libyan officials through a Libyan broker in connection with 14 investments made by Libyan state-owned financial institutions with SocGen. Although SocGen is not a U.S. entity, the bribes were part of a bribery scheme conducted in conspiracy with U.S. company Legg Mason, and so SocGen was subject to the jurisdiction of the DOJ.
- 2.2 For each of the transactions, SocGen paid the Libyan broker a commission of between 1.5% and 3% of the nominal amount of the investments made by the Libyan state institutions. The Libyan broker then paid portions of the commissions to high-level Libyan officials in order

to secure investments from the Libyan state institutions for the bank, in contravention of the anti-bribery provisions of the FCPA.

- 2.3 In total, SocGen paid the Libyan broker over USD90m to obtain investments from Libya which were worth a total of approximately USD3.66bn and generated profits of approximately USD523m for the bank. Legg Mason and its wholly owned subsidiary, Permal Group Ltd (**Permal**), also benefitted from the bribes paid in respect of seven of the 14 investments made by Libyan state institutions. In these transactions, SocGen acted as the “structuring bank,” receiving the money invested by the Libyan state institutions. SocGen then agreed with Permal that, for certain products, the money invested by the Libyan institutions would be placed in funds managed by Permal.



## 3. Summary background—Libor

- 3.1 SocGen admitted that between May 2010 and October 2011, it made falsely deflated U.S. Dollar Libor submissions to give the impression that it was able to borrow at more favorable interest rates than was in fact the case. This downward manipulation allowed SocGen to create the appearance that it was stronger and more creditworthy than it was.
- 3.2 SocGen admitted that in 2006, certain employees in the London and Tokyo offices worked together to manipulate Japanese Yen Libor submissions.



## 4. Charges laid against individuals

- 4.1 Two individuals, the former SocGen Global Treasury Head, Danielle Sindzingre, and former Paris Treasury Head, Muriel Bescond, have been indicted by the U.S. for their involvement in the Libor manipulation scheme.

## Legg Mason



### 5. Jurisdictional basis

- 5.1 Legg Mason is listed on the NYSE and is an “issuer” under the FCPA.
- 5.2 Permal was a U.S. headquartered investment management company within Legg Mason’s International Division. Permal was a wholly owned subsidiary of Legg Mason and its financial statements were consolidated into Legg Mason’s financial statements. Permal was an “agent” of an issuer under the FCPA.



### 6. Summary background

- 6.1 Between 2004 and 2010, Legg Mason, through Permal, partnered with SocGen to solicit investment business from Libyan state-owned financial institutions (**Libyan Financial Institutions**). Bribes were paid through a Libyan intermediary (**Intermediary**) to obtain investments from Libyan Financial Institutions.
- 6.2 From 2005 to 2008, SocGen paid the intermediary approximately USD26.25m for “introductory” services. Two Permal employees were aware that the Intermediary was paying bribes to Libyan government officials to secure investments. Despite this, they continued to use the Intermediary.
- 6.3 SocGen sold the Libyan Financial Institutions seven structured notes that linked to funds managed by Permal. The total value of these notes was approximately USD950m. For each of the seven transactions, SocGen, on behalf of Permal, paid a commission of 1.5% to 3% of the nominal amount of the investments made by the Libyan Financial Institutions to an entity incorporated in Panama and controlled by the Intermediary (the

**Panamanian Company**). Permal’s net revenue from these transactions was approximately USD31.6m.

- 6.4 Legg Mason admitted that this occurred in seven of the 14 investment transactions discussed above. In total, the seven transactions generated USD31.6m in profits for Permal (and therefore for Legg Mason).



### 7. Detailed background

- 7.1 In 2004, the Intermediary met with Permal employees to discuss investment opportunities in Permal and the possibility of various Libyan Financial Institutions purchasing financial products from SocGen. Libyan government officials were present during the discussions with Permal.
- 7.2 The parties arranged for the commission earned by the Panamanian Company to be used by the Intermediary to pay Libyan government officials. The government officials would then help secure investments from various Libyan Financial Institutions for SocGen.
- 7.3 Two former Permal employees were aware that the Intermediary was paying bribes and providing other improper benefits to Libyan government officials and at least one relative of a Libyan government official. These included free travel and entertainment.
- 7.4 Employees in Permal and SocGen used coded language when they referred to the Libyan bribery scheme. At least one Permal employee knew that SocGen was trying to conceal the payments to the Intermediary from the Libyan Financial Institutions.
- 7.5 SocGen sold the Libyan Financial Institutions seven structured notes with a total value of approximately USD950m altogether. Permal earned approximately USD31.6m in net revenue from these transactions.



## 8. Key takeaways

### 8.1 Importance of maintaining an adequate system of internal account controls in emerging markets

– SocGen and Legg Mason’s widespread use of brokers and other intermediaries increased the risk of bribery and corruption. The regulators recommended that they devise and maintain an efficient internal controls system to prevent and detect similar types of misconduct.

### 8.2 Due diligence on agents and business partners

– The importance of conducting due diligence on agents and business partners, and maintaining continuous oversight, cannot be stressed enough when operating in high risk jurisdictions such as Libya. Such controls appear to be the best safeguard against the funnelling of improper payments by agents and business partners to government officials.

### 8.3 Adequate steps taken to identify and mitigate the bribery and corruption risk in using intermediaries

– Legg Mason failed to take any steps when employees knew its intermediary was paying bribes to government officials. The SEC emphasized the way the company proactively identified the bribery and corruption risks inherent in engaging intermediaries. Once a company detects the risk, it should take steps to immediately mitigate associated risks, including termination of the intermediaries.

**8.4 Compliance and ethics program** – Implementing a strong compliance and ethics program designed to prevent and detect violations of the FCPA and other applicable anti-corruption laws throughout a company’s operations is important. Companies should also implement the same compliance and ethics program in its subsidiaries, affiliates, agents, and joint ventures, and those of its contractors and subcontractors whose responsibilities include interacting with foreign officials or engaging in other activities that carry a high risk of corruption.

**8.5 U.S./French coordination** – The case highlights the fact that France is now one of the countries working with the DOJ on cross-border foreign bribery investigations. Previously, the DOJ alone pursued foreign bribery cases against French companies. More generally, the case is an example of the heightened potential for multi-jurisdictional coordination between government authorities in investigating alleged misconduct.

**8.6 Difference in treatment between Legg Mason and SocGen** – The Legg Mason penalty is significantly smaller than the SocGen penalty, even though Legg Mason did not voluntarily self-disclose its conduct. Of note in terms of points of difference between the two companies is that Legg Mason’s misconduct reportedly involved only mid-to-lower level former employees of a subsidiary company. Also seemingly significant was the fact that Legg Mason did not maintain the relationship with the Libyan intermediary or originate or lead the corruption scheme. Legg Mason’s profits from the corrupt transactions were also a fraction of those of SocGen.

# Beam Suntory



## 1. Introduction

1.1 On July 2, 2018, Beam Suntory Inc (**Beam**), a liquor manufacturer with worldwide operations, agreed to pay more than USD8m to resolve FCPA charges with the SEC arising from improper payments made by its Indian subsidiary (**Beam India**). The administrative proceedings against Beam highlight the dangers of operating in high risk jurisdictions without adequate oversight of third party sales promoters and distributors, and the importance of adequate post-acquisition remediation of improper business practices identified during the diligence process of a potential acquisition target.



## 2. Jurisdictional basis

2.1 Beam is considered a “domestic concern” for the purposes of the FCPA. It is organized under the laws of the state of Delaware and headquartered in Chicago, Illinois. At the time of the misconduct under investigation, Beam was also listed on the NYSE.

2.2 Beam delisted from the NYSE in April 2014, after it was acquired by Suntory Holdings Limited (a Japanese corporation).



## 3. Summary background

3.1 Beam manufactures and sells branded alcoholic beverages worldwide. Beam India bottles and sells Beam products in India, and uses third party sales promoters, distributors and other third parties in connection with sales, promotion and other commercial activities in India.

3.2 From 2006 to 2012, Beam India used its third party sales promoters and distributors to make illicit payments to government officials to increase sales and distribution of its products, and to expedite the process for gaining license and label registrations in India. In addition, Beam made both direct and indirect improper payments to Indian government officials in connection with government inspections of its premises and to secure advantageous product placement and promotion of its products in government and retail stores.

3.3 The SEC found that the Indian subsidiary reimbursed third party agents for the illicit payments through the use of fabricated or inflated invoices, and then falsely recorded the expenses at the subsidiary level.

3.4 Beam also failed to remediate red flags identified by an accounting firm, a U.S. law firm and an Indian law firm in respect of the payments made to third party agents and sales promoters, and failed to conduct additional reviews and remediation as recommended by its external counsel.



## 4. Detailed background

4.1 The alcoholic beverage industry in India is highly regulated by government authorities. Prior to its acquisition by Beam in 2006, the predecessor entity of Beam India regularly made direct and indirect payments to Indian government officials in connection with inspections of its bottling facilities, distribution of its products, label registrations required to distribute its brands, warehouse license applications and renewals, and advantageous product placement and promotion in government retail channels. The Indian entity maintained a second set of financial records that tracked these payments and disguised their nature.

4.2 Following the 2006 acquisition, Beam retained the existing management of the Indian entity who had orchestrated the bribery schemes. Those managers continued the schemes at Beam India from 2006 to 2012, and engaged in improper conduct. Some examples of the conduct are as follows:

- (a) Senior executives of Beam India directed funds to various third party promoters to make improper payments to government officials in connection with obtaining or retaining business in the Indian market. These promoters, with Beam India's knowledge and authorization, also directed improper payments to government officials at retail stores and depots to secure orders of Beam products and the placement of Beam products in a prominent shelf position.
  - (b) Senior executives made improper payments to ensure timely inspections at its manufacturing facility and to secure and expedite the processing of label registration for distribution of Beam's products and warehouse licenses. In particular, Beam India paid INR1m (approximately USD 18,000) to an Indian excise official to issue a label registration for a new product.
  - (c) Third parties were reimbursed for the illicit payments by providing fabricated or inflated invoices to Beam India. The payments would then be falsely recorded in Beam India's books and records as legitimate business expenses, included as payments related to "*Customer Support*," "*Off-Trade Promotions*" and "*Commercial Discount, Ongoing*."
- 4.3 Beam also failed to remediate deficiencies in its controls in a timely manner. In 2008, Beam instituted annual internal audits and, from 2010, Beam hired a global accounting firm, as well as a U.S. and Indian law firm to conduct compliance reviews of Beam India. The investigations revealed the third party bribery scheme and Beam was advised to further examine potential FCPA issues.

4.4 While Beam India revised its agreements with third party promoters after hearing of SEC enforcement action concerning FCPA violations by a direct competitor of Beam, it did not conduct additional transactional testing or due diligence on third parties as advised by the accounting firm and U.S. law firm.

4.5 Finally, in November 2011, when a former Beam India employee alleged that a Beam India manager was using false invoices from third parties to generate funds, an internal review was instigated by the company that confirmed this conduct and concluded that the funds had been used to bribe government officials. Beam moved up a planned FCPA compliance review, but did not expand the review to other third parties or markets with similar risks.



## 5. Key takeaways

### 5.1 Conducting adequate due diligence when acquiring a new target and remediating any misconduct identified

– The SEC enforcement action shows the risks inherent in making acquisitions of businesses in challenging jurisdictions, and the retention of managers of predecessor entities in those jurisdiction without adequate oversight. The U.S. parent company acquired an Indian subsidiary but did not detect or remediate conduct that subsequently created an FCPA liability. The action underscores the importance of conducting robust anti-corruption due diligence of targets in high risk jurisdictions and maintaining adequate integration processes in mitigating corruption issues.

### 5.2 Beam's in-house counsel putting a halt to further reviews

– The SEC order specifically highlighted that a Beam in-house lawyer put an end to further internal reviews recommended by Beam's external advisors. The SEC noted the comments by a Beam lawyer that he was *“concerned about [the Indian law firm] digging and finding information that we cannot impact, specifically finding activities and practices by [promoters] that we cannot remediate or change.”* Despite receiving recommendations that more transaction testing and review was required, Beam elected not to proceed with such a review and was criticised by the SEC for the scope and timeliness of its response.

### 5.3 Maintaining adequate oversight of operations in other jurisdictions

– Although Beam conducted internal audits and an FCPA review at its subsidiary in India, it did not remediate the misconduct identified after being made aware of a similar enforcement action against its competitor, Diageo, in India. The SEC order indicates that the SEC will penalise companies that do not remediate identified red flags, in particular those that are aware of the enforcement environment in similar jurisdictions and industries.

### 5.4 Maintaining independent oversight of third party agents of the company

– This enforcement action is symbolic of what goes wrong when there is a lack of oversight of third party agents in a high risk jurisdiction.

The corrupt conduct of third party agents hired by Beam India was ingrained in the operations of the company, and concealed by senior management in the form of false invoices and two sets of accounting records. Any indication of a second set of accounts should immediately raise concerns about the adequacy of a company's books and records and the potential for fraudulent or improper payments.

**5.5 Due diligence on third parties** – The importance of due diligence on third parties and the maintenance of evidence that shows third parties have provided the contracted services cannot be stressed enough when operating in high risk jurisdictions such as India. Such controls appear to be the best safeguard against the funnelling of illicit funds by third parties to government officials.

**5.6 Resolution of SEC case prior to resolution of DOJ matter** – Beam resolved the case with the SEC prior to the resolution of the DOJ investigation. It is common for companies to resolve SEC and DOJ investigation simultaneously. It will therefore be interesting to see if the DOJ will grant Beam a declination or seek a criminal penalty, in addition to the SEC's civil order.



# Credit Suisse



## 1. Introduction

1.1 On July 5, 2018, Credit Suisse Group AG (**CSAG**), a Swiss-based corporation, agreed to pay the SEC and DOJ a total of USD77m to settle allegations of violations of the FCPA. The allegations mainly concern breaches of the anti-bribery and internal accounting controls provisions of the FCPA by Credit Suisse (Hong Kong) Limited (**CSHK**). CSAG was charged with:

- (a) hiring, promoting and retaining individuals who had been referred by government officials and Chinese state-owned enterprises (**SOEs**); and
- (b) failing to maintain sufficient internal controls to minimize bribery and corruption risks.



## 2. Jurisdictional basis

2.1 CSAG is listed on the NYSE and is therefore an issuer under the FCPA.

2.2 CSHK is a wholly owned subsidiary of CSAG. CSAG's global investment banking business is headquartered in the U.S., but business in the Asia Pacific region is conducted primarily through CSHK and its employees. CSHK is therefore an agent of the issuer under the FCPA.



## 3. Summary background

3.1 From 2007 to 2013, CSAG offered employment to more than 100 individuals referred by, or having some connection to, government officials in the APAC region, including more than 60 employees and interns at more than 20 different Chinese SOEs.

3.2 According to the DOJ, CSHK and its affiliates obtained deals from hiring referrals that amounted to at least USD46m.

3.3 These hires, referred to as "relationship hires," had significantly less relevant experience in banking and lacked technical skills when compared with other candidates hired through other channels (eg, a merit-based campus recruiting program).

3.4 From at least 2007, CSAG recognized the FCPA risks in hiring relatives of government officials, knowing it could be regarded as giving things of value to government officials to secure improper advantage. CSAG had in place a Global Anti-Bribery Policy (the **Global Policy**) at that time, which prohibited relationship hires. The Global Policy was updated in 2011 to prohibit ad hoc training activities and internships for relatives of government officials if the government officials were clients of CSAG. CSHK senior management was aware of the Global Policy but repeatedly hired relatives of government officials.



## 4. Detailed background

### 4.1 CSHK's hiring of candidates to assist in winning/retaining business or obtaining favorable treatment

- (a) CSAG maintained spreadsheets that tracked the contribution of the relationship hires (ie, deals the relationship hires brought in). The spreadsheets also contained information identifying the referring client or the relationship with the government ministry.
- (b) Most relationship hires lacked technical skills and were less qualified than candidates hired through CSAG's proper hiring channels. These candidates were hired to assist in winning or retaining business from the SOEs or obtaining favorable treatment with the government ministries.



- (c) In or around March 2010, CSHK pitched for an investment banking mandate involving a Chinese energy-related company. The relationship hire was the daughter of a high-ranking official at a Chinese energy-related SOE. The official was also the controlling shareholder of the company CSHK was pitching for. A CSHK vice president asked the CSHK colleagues not to conduct too many interviews because the relationship hire was “*a princess [who was] not used to too many rounds of interview[s].*” CSHK employees also drafted a resume for the relationship hire and were “creative” in completing the details. The relationship hire joined CSHK on or about July 1, 2010. In April 2011, CSHK obtained a mandate from the Chinese energy-related SOE for a convertible bond offering. According to the SEC, the relationship hire was not vetted or approved by the Legal and Compliance Department (**LCD**).
- (d) In 2009, Credit Suisse offered employment to another relationship hire who was the daughter of an influential official with a powerful Chinese government ministry. The senior managers sought to use her connections with her mother to secure business for CSHK and secured a lucrative Initial Public Offering (IPO) mandate from a Chinese financial SOE, generating approximately USD8.9m in revenue for CSHK. CSHK employees did not disclose the hire’s connection to the LCD.
- (e) In March 2008, CSHK gave a full-time position in Hong Kong to a relationship hire who had been referred by a high-ranking official from a Chinese SOE. Subsequently, CSHK received a mandate from a subsidiary of the Chinese SOE to act as a bookrunner on its IPO, generating approximately USD21.9m in revenue for CSHK by the time the deal closed in 2009. During the relationship hire’s four-year employment at CSHK, senior management emphasized the importance of including the relationship hire in all deals related to the Chinese SOE even though he lacked the experience and expertise.
- (f) In June 2010, Credit Suisse hired a relationship hire from a large energy-related SOE in order to obtain business from the SOE. The relationship hire started as an associate and was promoted to vice president in the same year. Three days after the relationship hire joined CSHK, the bank was awarded a mandate to act as a joint bookrunner in an IPO of an affiliate of the SOE and earned approximately USD 986,439 in revenue when the deal closed.

#### 4.2 Senior Credit Suisse Managers in APAC had actual knowledge of the prohibitions

- (a) CSHK senior managers were aware that hiring referrals from SOEs and government ministries on a quid pro quo basis was prohibited under the Global Policy. From 2007 to 2013, multiple senior CSHK managers hired, promoted and retained relationship hires as a means of assisting CSHK to win lucrative investment banking mandates and obtain favorable treatment.
- (b) In particular, senior managers in CSHK expressly agreed to hire the relationship hires before conducting any interviews. Furthermore, they instructed other CSHK employees to conduct interviews so that the relationship hires would automatically score highly, without regard for their actual performance.
- (c) On a number of occasions, the LCD was not informed of or involved in the hiring of the relationship hires. The connection between the relationship hire and the government official was not always properly disclosed to the LCD.
- (d) Certain Credit Suisse managers in the U.S. were aware of CSHK’s hiring of relationship hires. Certain hires were approved by senior managers in the U.S. and were placed to work in the U.S. There were complaints about the quality of the relationship hires’ work, but CSAG failed to take adequate steps to mitigate the known risks of hiring relationship hires in CSHK.



## 5. Key takeaways

### 5.1 Follow existing internal policies, procedures and accounting controls

– Even though CSAG maintained the Global Policy, which restricts the hiring of relatives of government officials, the DOJ and SEC found that senior managers in the APAC region knowingly and repeatedly offered employment to relationship hires in disregard of the Global Policy. The DOJ and SEC found this to be evidence of inadequate internal accounting controls as senior management worked around the internal policies and procedures.

### 5.2 Identify all candidates referred by government officials and SOEs

– It should be compulsory for all candidates for employment to be screened by an independent service for connections to government officials, SOE employees and other “politically exposed persons” (PEPs).

### 5.3 Put in place additional post-hiring controls to ensure compliance

– The DOJ emphasizes the importance of having sufficient post-hiring controls to avoid bribery and corruption risks resulting from the employment of PEP-related personnel. Periodic reviews of the policies and procedures of hiring controls and evaluation of the validity of the screening process for PEPs are also necessary to identify potential red flags in the hiring process.

### 5.4 Provide compulsory compliance training for all senior managers

– All senior managers should be required to attend relevant compliance training to ensure that they understand the company’s internal policies and procedures. The training should be tailored to the senior managers with an emphasis on the different scenarios and penalties in place for violating the company’s policies.

### 5.5 Mitigating factors

– CSAG received only partial credit for its cooperation with the investigation. Full cooperation credit was not given to CSAG because the cooperation was reactive rather than proactive. CSAG also did not receive full remediation credit because it did not sufficiently discipline the employees who engaged in the misconduct.



# Sanofi



## 1. Introduction

1.1 On September 4, 2018, French pharmaceutical company Sanofi SA (**Sanofi**) agreed to pay USD25.2m to end the SEC's investigation into alleged bribes by a number of the company's international subsidiaries. The SEC brought administrative proceedings on the basis of Sanofi's violations of the internal accounting controls and record-keeping provisions of the FCPA.



## 2. Jurisdictional basis

2.1 Although Sanofi is a corporation organized in France, it has issued and maintains a class of securities traded on the NYSE.



## 3. Summary background

3.1 Between 2007 and 2011, a Sanofi subsidiary in Kazakhstan allegedly agreed to give distributors a discount of between 20% to 30% on pharmaceutical orders, and used a portion of that discount to bribe Kazakh officials. In return, the officials would accept Sanofi's bids to provide drugs to certain institutions, generating about USD11.6m in profits for the company.

3.2 In Lebanon, Sanofi bribed officials with items such as donations, and consulting and clinical trial fees in exchange for increased prescriptions of its products, generating about USD4.2m in profits. Sanofi bribed officials similarly in the United Arab Emirates.

3.3 The funds used for the illicit payments were generated through fake expenses, clinical trial and consulting fees, product samples, distributor discounts and credit notes which were improperly recorded in Sanofi's books and records.



## 4. Detailed background

4.1 In Kazakhstan, Sanofi managers devised a scheme to bribe foreign government officials responsible for awarding public tenders. They worked with distributors to submit bids for public tenders. If won, the sale price between Sanofi and the distributor included a pre-determined discount or credit note from the sale price agreed between the distributor and the public institution.

4.2 The distributor and Sanofi designated a portion of the discount as funds to bribe Kazakh officials, and kicked these back to Sanofi employees to deliver to the officials. The kickbacks were tracked in an internal spreadsheet and referred to as "marzipans."

4.3 In Lebanon, Sanofi Levant employees and agents participated in schemes to pay doctors to boost sales through increased prescriptions. In particular, the company used sponsorships, gifts, donations, product samples, consulting agreements, clinical studies and grants to funnel money to doctors. In one example, Sanofi Levant gave an influential hospital doctor almost 20% of the hospital's requirement of an oncology product in samples. Similarly, it retained a pharmacist as a consultant who over a five-year period was paid a total of USD 237,300 in consulting fees.

4.4 In the Gulf, Sanofi sales managers and medical representatives submitted false travel and entertainment reimbursement claims to create a pool of proceeds to distribute to medical professionals to increase prescriptions. An audit into Sanofi's Gulf operations found that monitoring of outsourced distributor promotional activities was lacking, however no action was taken to remedy this.



## 5. Key takeaways

### 5.1 The life sciences industry continues to be exposed to significant FCPA risks

– This case is another example of a life sciences company facing FCPA scrutiny. The conduct at issue will be very familiar to those aware of the history of FCPA enforcement in the life sciences industry. Discounts, product samples, relationships with distributors, public tendering, gifting and entertainment are traditional risk areas faced by the pharmaceutical industry.

### 5.2 Adequate financial and accounting controls

– Where slush funds are created that allow employees to funnel illicit funds to government officials, internal controls have broken down. Conducting audits and reviews of potentially risky transactions and accounts is key, and these should be conducted on a periodic basis. Invoices should also be checked for veracity and accuracy.

### 5.3 Relationships with distributors

– In this case, Sanofi's relationship with distributors allowed for the establishment of funds that were used to bribe officials to win public tenders. Independent reviews of distributors, and oversight by the compliance team of the public tendering process as well as discounts and credit notes to distributors is warranted.

### 5.4 Gifts and entertainment, consultancies and product samples are all risk areas

– All forms of gifts provided to healthcare professionals are risks and can be used to curry improper favor with medical professionals. Companies should take care to implement and follow strict guidelines on when such entertainment, consultancies and product samples are appropriate and implement strict approval thresholds and limits.

### 5.5 Provide compulsory compliance training for all senior managers

– All senior managers should be required to attend relevant compliance training to ensure that they understand the company's internal policies and procedures. The training should be tailored to the senior managers with an emphasis on the different scenarios and penalties in place for violating the company's policies.



# United Technologies



## 1. Introduction

1.1 On September 12, 2018, United Technologies Corporation (**UTC**) agreed to pay USD13.9m to the SEC to resolve charges that it violated the books and records provisions in the FCPA by making illicit payments through its elevator and aircraft engine businesses in China, Azerbaijan, and six other countries.



## 2. Jurisdictional basis

2.1 UTC is a Delaware corporation with shares traded on the NYSE.



## 3. Summary background

3.1 From approximately 2012 through 2014, UTC's subsidiary Otis Elevator Co. (**Otis**) made unlawful payments to Azerbaijani officials to facilitate the sales of elevator equipment for public housing in Baku and as part of a kickback scheme to sell elevators in China.

3.2 The SEC order also found that UTC, through its joint venture International Aero Engines (**IAE**), made payments to a Chinese sales agent between 2009 and 2013 in a bid to obtain confidential information from a Chinese official that would help the company win engine sales to a Chinese state-owned airline.

3.3 Finally, UTC also improperly provided trips and gifts to various foreign officials in China, Kuwait, South Korea, Pakistan, Thailand, and Indonesia through its Pratt & Whitney division and Otis subsidiary in order to obtain business between 2009 and 2015.

3.4 In respect of the above payments, UTC failed to accurately and fairly record the transactions in its books and records and failed to devise and maintain a sufficient system of internal accounting controls.



## 4. Detailed background

### 4.1 Russian and Azerbaijani Improper Payment Scheme

- (a) In 2012, Otis engaged in various schemes to sell Otis elevator equipment to Baku Liftremont, a municipal entity in Azerbaijan, responsible for procuring and maintaining the elevators in Baku's public housing. The schemes involved the use of sham subcontractors and intermediaries to make improper payments to Liftremont officials. No due diligence was performed on the subcontractors, and they were paid over USD 790,000, which represented nearly 44% of the total contract value for the elevators sold.
- (b) Between February 2013 and December 2014, Otis sought to win additional contracts from Liftremont. At the direction of a Liftremont official, Otis Russia involved four different intermediaries which acted as conduits to make improper payments in order to secure nine contracts from Liftremont. As part of the scheme, Liftremont officials were also allowed to use Otis Russia signature stamps to falsify documents.
- (c) Other methods were also used to funnel improper payments to Liftremont officials. In one scheme, Liftremont was made a distributor so that certain Liftremont officials could receive additional monies from the sale of Otis elevator equipment and services.
- (d) Otis' JV partner, which sold Otis elevators in the Baku market, raised numerous concerns about improper transactions between Otis and Liftremont. In the summer of 2014, Otis ignored additional red flags when the Liftremont official instructed Otis Russia to replace one intermediary with a new intermediary.

- (e) As a result of the schemes, the intermediaries obtained at least USD11.8m, some of which was intended for Liftremont officials, to ensure Otis would win the nine contracts.

#### 4.2 China Aviation Scheme

- (a) From 2009 to 2013, IAE engaged a Chinese sales agent and paid USD55m in commissions to that agent to sell airplane engines to Chinese state-owned commercial airlines. With the help of the agent, IAE obtained confidential information about competing bids for an Air China contract, allowing it to modify its bid and win the contract.
- (b) Between March and December 2009, the agent made at least six payments totalling over USD 160,000 to the airline official who provided the confidential document. Additionally between 2009 and 2013, the agent was paid USD4.3m in success fee payments for the Air China contract.
- (c) In addition to requests for advance commission payments for an “office expansion,” the Chinese sales agent also requested advance payments for sponsorship of an event for Chinese officials. In November 2009, the agent asked IAE to co-sponsor a golf event for senior executives of Chinese state-owned airlines that was to take place in January 2010. The request was approved and USD 60,000 was paid towards the golf event.

#### 4.3 Improper Payments for Otis Elevator Sales in China

In 2012, Otis China paid a kickback to a Chinese official at a state-owned bank in Wuhan, China for a contract to sell and install four elevator units at a branch of the bank. A distributor was engaged to bid for the bank contract, and then used to pass USD 98,000 to an Otis sales employee who paid a kickback to the Chinese bank official.

#### 4.4 Leisure Travel

- (a) Between 2009 and 2015, UTC and its subsidiaries funded leisure travel and entertainment for foreign officials from several countries, including China, Kuwait, South Korea, Pakistan, Thailand, and Indonesia. In particular:
- (i) Pratt & Whitney provided entertainment and leisure travel for up to five officials of the Republic of Korea Air Force (**ROKAF**) on seven occasions. At the time, ROKAF was purchasing aftermarket spare parts and repair services from Pratt under short-term contracts, and Pratt was seeking to enter into a long-term contract.
- (ii) Otis also provided improper travel in connection with sales in China. For example, in 2008, the Hangzhou branch of Otis China obtained a USD27.6m contract for the Hangzhou Metro Line 1 project. In 2010, the Otis China project manager approved a 2011 trip to Italy and Greece for seven foreign officials associated with the project. In 2011, the Otis China major project manager approved travel to the United States for seven foreign officials.
- (iii) In 2008, the Shenzhen branch of Otis China obtained a USD3.3m contract for the Shenzhen Metro Line 5 project.
- (b) In total, between 2009 and 2015, UTC improperly recorded over USD 134,000 in improper travel and entertainment for foreign officials in the company’s books and records as legitimate business expenses.



## 5. Key takeaways

### 5.1 Due diligence on sales agents and distributors

– UTC, Pratt & Whitney and Otis used a number of sales agents and distributors to make illicit payments to government officials or to obtain confidential information on competing bids. In most cases, the due diligence on such agents was inadequate or indicated that the agent did not have experience in the relevant industry or bid process. Due diligence of sales agents and distributors should always be conducted and high risk agents reviewed by the compliance team. Payments made to agents and distributors also warrant periodic monitoring.

### 5.2 Adequate financial and accounting controls over

**foreign subsidiaries** – In this case, it is clear that UTC did not have adequate oversight over its foreign subsidiaries and JVs in high risk jurisdictions. Funds were easily funneled to inappropriate sales agents, intermediaries or distributors. Conducting audits and reviews of potentially risky transactions and accounts are key, and these should be conducted on a periodic basis. Invoices should also be checked for veracity and accuracy, and any large payments to sales agents and distributors verified.

**5.3 Travel, gifts and entertainment as a risk area** – As apparent in this case, leisure trips and travel were used by the company to influence government officials. Many of the contracts won by the business were linked to some form of travel received by government officials responsible for approving the contract. All forms of entertainment and travel for government officials are a risk area, and can be used to curry favor with such individuals. Companies should take care to implement and follow strict guidelines on when such travel is appropriate and can be approved.

### 5.4 Provide compulsory compliance training for all

**senior managers** – All senior managers should be required to attend relevant compliance training to ensure that they understand the company's internal policies and procedures. The training should be tailored to the senior managers with an emphasis on the different scenarios and penalties in place for violating the company's policies. Such training is particularly important in high risk jurisdictions such as China.



# Petroleo Brasileiro S.A. – Petrobras



## 1. Introduction

1.1 On September 27, 2018, Petróleo Brasileiro S.A. – Petrobras (**Petrobras**) agreed to pay approximately USD933.4m as a civil penalty to the SEC (USD711m in disgorged profits plus interest of USD222.4m), though this amount may be reduced by the amount of any payment Petrobras makes to a related class action. In addition to this payment, Petrobras agreed to make a further payment of USD853.2m as a criminal penalty pursuant to a non-prosecution agreement with the U.S. DOJ, with USD85.32m to be credited against the SEC's civil penalty, USD85.32m to be paid to the U.S. Treasury and the remaining USD682.56m to be paid to Brazilian authorities. These agreements were entered into to resolve, without civil or criminal charges, U.S. and Brazilian investigations into Petrobras' facilitation, payment and concealment of bribes and violations of the books and records and internal controls provisions of the FCPA. The resolution of this matter marked a significant landmark in Operation Car Wash, the investigation by Brazilian authorities of a corruption scandal which led to prosecutions of a number of other companies and the arrest of former Brazilian president Luiz Lula da Silva.



## 2. Jurisdictional basis

2.1 Petrobras is a Brazilian company, headquartered in Rio de Janeiro, Brazil. It is controlled by the Brazilian government but a large number of its shares are traded on the NYSE as American Depositary Shares (**ADS**). It is therefore considered an "issuer" under the FCPA, and its stock is registered with the SEC.



## 3. Summary background

- 3.1 Petrobras is a Brazilian government-controlled entity, whose Board of Directors was primarily appointed by the Brazilian government. Between 2003 and 2012, Brazilian politicians appointed individuals to these roles and demanded payments in return for these appointments. In the same period, Petrobras engaged in an expansion of its oil and gas infrastructure.
- 3.2 From 2004 to 2012, several senior Petrobras executives and managers (the **Executives**) conducted bid-rigging schemes for the infrastructure projects. Working with Petrobras contractors and suppliers, the Executives inflated the costs of Petrobras' infrastructure projects and used the inflated costs to pay kickbacks to themselves, Brazilian politicians, Brazilian political parties and others who assisted in the scheme. The inflated invoices were recorded in Petrobras' financial statements, submitted in its SEC filings.
- 3.3 Petrobras also received bribes from companies who sought contracts with Petrobras, and facilitated payments to politicians and political parties.
- 3.4 Several of the Executives additionally falsified the company's books and records by signing or causing to be signed sub-certifications confirming the accuracy of Petrobras' disclosures to the SEC. The Executives failed to implement Petrobras' internal controls and exploited the deficiencies in them. As such, Petrobras failed to maintain accurate books and records and had no sufficient system of internal controls preventing the facilitation of corrupt payments and processes.





## 4. Detailed background

### Bid-rigging schemes and corruption in procurement process

- 4.1 From 2004 to 2012, in undertaking its infrastructure projects, Petrobras conspired with several large Brazilian construction companies to create a cartel to influence bidding processes. The Executives ensured that cartel companies were selected to participate in bidding rounds for contracts and would then influence the bidding process so that specific companies within the cartel secured the contracts. In particular, they gave the cartel inside information, manipulated the bidding process for the benefit of those companies, voted to approve contracts that did not conform with Petrobras' procurement rules and found ways to influence the bidding process so specific companies in the cartel would win. The companies then overcharged Petrobras under the contracts and used these overpayments to fund bribes, which were paid to the Executives and their political patrons. As part of the scheme, between 1% and 3% of the contract values were paid as bribes.
- 4.2 These payments were recorded in Petrobras' books as part of legitimate expenses, being a portion of the money paid to contractors to acquire and improve assets. As such, the illicit payments were hidden as part of the contracts.
- 4.3 The SEC and DOJ described three examples of the bribery scheme:
- (a) In or around 2005, Petrobras announced its intention to construct the Abreu e Lima Refinery (**RNEST**). During the course of this project, the Executives conspired with contractors and suppliers to facilitate payments to politicians from contractors that obtained business from Petrobras. In or about 2008 or 2009, Petrobras issued tenders for two contracts worth over BRL4.67bn. Before the tenders were announced, an executive gave confidential project information to one of the potential contractors, who took the information to the other cartel companies. They then agreed among themselves which companies would form a consortium and submit the lowest tender for the contracts. Upon the consortium winning the tender, one of the Executives requested the consortium pay BRL15m to a Brazilian political party and BRL15m to himself. An intermediary was also used to pay bribes received from Petrobras contractors to pay BRL 20 million to a politician who oversaw the location of the RNEST refinery, and an additional BRL30m was paid to the Executives to assist with any future issues the RNEST project may encounter.
  - (b) In another project, the Rio de Janeiro State Petrochemical Complex (**COMPERJ**), the Executives facilitated payments to a politician who oversaw the COMPERJ site. In 2010, one of the executives arranged a meeting between six of the contractors working on the COMPERJ project and a government official representing the politician. Payments funding the politician's re-election campaign totalling BRL30m were later made by the contractors present at the meeting, as well as several others. In exchange for bribes, the Executives further leaked confidential information used to review bid proposals, accelerated completion schedules and provided contracting opportunities to bribe-paying contractors.
  - (c) Additionally, in or about 2007, the Executives awarded a contract to a ship operating company in order to assist a politician to reduce their campaign debt to the company's affiliated bank. The Executives awarded the contract without undertaking a competitive bidding process, and awarded it to the company despite it not being the top choice to provide the service.

### General Bribery Schemes

4.4 Petrobras also sought illicit payments from companies who sought to win contracts with Petrobras:

- (a) Between 2004 and 2012, one of the Executives facilitated the payment of bribes from a Singaporean shipyard company to a political party on at least six separate Petrobras projects. They also received bribes on their own behalf. The SEC alleged that in one instance, in or about 2008, a manager among the Executives at Petrobras told a consultant of the Singaporean company that if they wished to win the contract, they would need to pay a percentage of the contract value to a Brazilian political party and to the manager. The Singaporean shipping company accordingly paid the consultant a number of commissions which were then used to pay bribes of approximately USD8.8m to the political party and the manager. The shipping company won the contract.
- (b) The DOJ found that in 2006, Petrobras purchased a Texas oil refinery on the recommendation of one of the Executives. The Executive knew that the refinery was in disrepair and did not meet Petrobras' needs, but made the recommendation in return for a USD2.5m bribe.
- (c) In or around 2009 and 2010, bribes were paid by a drillship company to one of the Executives, a Brazilian political party and various intermediaries to win a Petrobras contract valued at USD 1.8bn. Bribes totalling USD20.8m were paid via commission agreements with two separate agents, who then funnelled the payments to the Executive and others.



## 5. Key takeaways

### 5.1 Failure to implement sufficient internal controls

– In this case, high-level employees responsible for implementing controls willfully failed to do so and in fact facilitated and benefitted from a corruption scheme that allowed illicit payments to be made by third parties. Although Petrobras had detailed procurement procedures, senior managers did not follow these. The DOJ recommended Petrobras develop policies and procedures as well as a system of internal reporting and investigation to detect and remove this misconduct.

**5.2 Public tenders and bidding processes** – Petrobras and its executives had significant control over several public tenders and were able to influence processes such that tender procedures were circumvented and bidders that were less qualified were selected. It was also clear that Petrobras had very close ties to political parties and supported political campaigns, and that the bribes these bidders were willing to pay supported these political parties. Petrobras was able to bypass its procurement rules to award contracts to cartel companies that were willing to pay kickbacks to its executives and politicians. A company's tender process, particularly where it engages in and organizes public bidding processes, should be subject to independent review and carefully audited for irregularities. There needs to be sufficient oversight, appropriate due diligence procedures and safeguards in place to prevent the manipulation of bid participation. The same executives should not have the authority to both award and approve contracts and contract amendments without review.

### 5.3 Due diligence on third parties and contractors, and the inflating of invoices

– Petrobras used agents to funnel bribes to government officials. It was clear that these agents and intermediaries had not been reviewed or monitored appropriately. Contractors were also able to inflate invoices to create funds to pay bribes. Properly documented due diligence of third parties should always be conducted, and high risk agents reviewed and monitored by the compliance team. There should also be regular oversight of business partners, as well as their services and invoices checked for inconsistencies or irregularities.

### 5.4 Provide compulsory compliance training for all personnel, including senior managers

– In this case, the SEC found that Petrobras did not require employees to receive any anti-corruption or compliance training, despite operating in a high risk jurisdiction. All personnel should be required to attend relevant compliance training and the company should ensure people attend and certify their compliance with such training. For senior managers, the training should be tailored, with an emphasis on the different scenarios and penalties for violating the company's policies. Such training is particularly important in high risk jurisdictions such as Brazil and should not be left to the discretion of executives.

### 5.5 Independent oversight of every function and level in the company, including senior managers

– Every company should maintain an independent body to provide oversight of every function and at every level in the company. The DOJ recommended assigning responsibility for oversight of Petrobras' anti-corruption code, policies and procedures to one or more senior executives with sufficient authority, autonomy and resources to report any misconduct directly to the Board of Directors or independent monitoring bodies.

### 5.6 DOJ's non-prosecution agreement and policy discouraging "piling on"

– Despite the seriousness of the conduct, the DOJ offered Petrobras a non-prosecution agreement, a particularly lenient resolution. This is in large part attributable to the DOJ's recent policy discouraging the "piling on" of penalties where a company is being investigated by multiple agencies and governmental authorities in other jurisdictions. Brazilian authorities also investigated the company, and received 80% of the penalties paid to U.S. authorities. The non-prosecution agreement also reserves Petrobras' right to argue that "as an instrumentality of the Republic of Brazil, it is protected by sovereign immunity" in any future prosecution or civil action brought by the United States. This is an interesting development, particularly given the widespread nature of the bribery scheme and its impact on the Brazilian political system and economy.



# Stryker Corp.



## 1. Introduction

- 1.1 On September 28, 2018, Stryker Corp. (**Stryker**) agreed to pay USD7.8m to the SEC to resolve charges that Stryker had violated the books and records and internal accounting control provisions of the FCPA by failing to detect the risk of and prevent improper payments to public healthcare professionals (**HCPs**) in India, China and Kuwait.
- 1.2 This is the second enforcement action the SEC has brought against Stryker. In October 2013, Stryker paid USD13.2m to settle charges alleging that it had violated the FCPA by failing to implement robust compliance programs that led to the bribery of HCPs at public hospitals in Argentina, Greece, Mexico, Poland and Romania.



## 2. Jurisdictional basis

- 2.1 Stryker is a Michigan-based company, with shares traded on the NYSE. The financial records of Stryker India, Stryker China and EMEA Supply Chain Services (a subsidiary of Stryker in the Netherlands that oversees the distributors in Kuwait) are consolidated into the financial statements of Stryker.



## 3. Summary background

- 3.1 From 2010 to 2015, dealers for Stryker India, a wholly owned subsidiary of Stryker, regularly issued inflated invoices “upon the request of certain private hospitals” even though the price for the orthopaedic products had been negotiated and approved by Stryker India’s management before the invoices were submitted. The invoices would then be passed on to the patient or the patient’s insurer.

- 3.2 From 2015 to 2017, Stryker China engaged at least 21 sub-distributors to sell Sonopet products that had not been “vetted, approved, or trained, as required by Stryker’s policies.” Installation records were sometimes falsified to hide the use of unauthorized sub-distributors.
- 3.3 Until 2018, Stryker had one primary distributor in Kuwait (**Kuwait Distributor**), who sold Stryker’s orthopedic products to the Kuwait Ministry of Health. From 2015 to 2017, the Kuwait Distributor made more than USD 32,000 of improper “per diem” payments to Kuwaiti HCPs to encourage them to attend Stryker events. Stryker paid all the costs of accommodation, meals and local transportation associated with the events.
- 3.4 Although Stryker’s internal policies prohibited paying bribes to HCPs through distributors, Stryker failed to prevent distributors in India, China and Kuwait from paying bribes and making other improper payments.



## 4. Detailed background

### 4.1 India

- (a) From 2010 to 2015, Stryker India sold its medical products through third party dealers. The dealers would then sell the products, mostly to private hospitals.
- (b) Each dealer was required to comply with Stryker’s policies, which prohibited improper payments to government officials and business partners of Stryker. The dealers were also required to maintain accurate records relating to the promotion, marketing and distribution of the products.
- (c) In 2012, Stryker audited three (out of 198) dealers in India in response to allegations of dealer misconduct. The audit reports indicated that one of the dealers was issuing inflated invoices at the hospital’s request. One of the three dealers was terminated as a result.

- (d) Until 2015, Stryker took no further steps to determine how many dealers in India were inflating their invoices.
- (e) In 2015, Stryker finally audited the other dealers in India and found that dealer-inflated invoices were quite common. Certain hospitals would routinely ask dealers to mark up the cost of Stryker's products above the agreed price negotiated earlier with Stryker India before the hospital passed the invoice to the patient or the insurer. This would give a higher profit margin to the dealer.
- (f) The books and records of Stryker India were also inaccurate and incomplete. A forensic review of Stryker India's general ledger from 2010 to 2015 revealed "a complete lack of documentation for 144 out of 533 transactions selected as a sample of Stryker India's highest-risk and most compliance-sensitive accounts." Proper documentation was missing for some high risk transactions, such as:
  - (i) consulting payments to HCPs;
  - (ii) payments of HCPs' travel and accommodation;
  - (iii) payments to event organizers;
  - (iv) discounts to dealers on the price of Stryker products;
  - (v) commissions to dealers; and
  - (vi) marketing expenses.
- (g) Stryker India had as such failed to maintain books and records that truly reflected the transactions. Consulting fees paid to HCPs lacked adequate explanations of the services the HCPs had provided and the number of hours involved. Some travel expenses for the HCPs were falsified.

#### 4.2 China

- (a) Stryker China sells its Sonopet products to a state-owned distributor, which sells the products to sub-distributors.

- (b) From 2015 to 2017, Stryker China engaged at least 21 sub-distributors to sell Sonopet products. The sub-distributors had not been "vetted, approved, or trained" by Stryker in accordance with its internal controls. These sub-distributors would sometimes involve third, fourth, and even fifth tier sub-distributors to sell Sonopet products. No due diligence was conducted on the sub-distributors.
- (c) Employees in Stryker China were aware that sub-distributors that had not been approved by Stryker were being engaged and that this violated the internal controls of the company. Installation records were sometimes falsified to hide the use of unauthorized sub-distributors.
- (d) Stryker's failure to monitor the sub-distributors increased the risk of bribery. Improper payments could be funneled to government officials through these sub-distributors without Stryker's knowledge.

#### 4.3 Kuwait

- (a) Until recently, most of the orthopedic products that Stryker sold to public hospitals in Kuwait were sold through the Kuwait Distributor. The Kuwait Distributor would then sell the products to the Ministry of Health in Kuwait, which procures medical products on behalf of Kuwait's public hospitals.
- (b) From 2015 to 2017, the Kuwait Distributor made more than USD 32,000 of improper "per diem" payments to Kuwaiti HCPs in order for them to attend Stryker events. On top of the improper payments, Stryker paid for all the HCPs' accommodation, meals and local transportation costs.
- (c) Stryker had never conducted an audit on the Kuwait Distributor. When Stryker wanted to audit the Kuwait Distributor, the Kuwait Distributor refused. Even when Stryker received a complaint from a former employee of the Kuwait Distributor alleging that the Kuwait Distributor paid bribes when selling Stryker products, Stryker did not review the books and records or investigate whether improper payments had been made to government officials.

- (d) Stryker failed to assess whether the Kuwait Distributor was complying with Stryker's anti-corruption policies. Stryker also failed to implement effective internal accounting controls to detect the Kuwait Distributor's bribery conduct.



## 5. Key takeaways

### 5.1 Failures to implement sufficient internal accounting controls and keep accurate books and records

– Stryker failed to maintain effective internal controls to detect the risk of improper payments even though Stryker had been charged previously with the same violations. According to the Cease and Desist Order (Order), the conduct involved took place from 2010 to 2017, which means that some of the conduct occurred after Stryker had settled its 2013 enforcement action.

### 5.2 Due diligence on sole distributors and distributors appointed by the government

– Stryker used a sole distributor in China and also in Kuwait. The use of a sole distributor who is also a government distributor increases the risk of bribes being funneled to government officials. We understand that, in some countries, engaging a sole distributor is unavoidable. Companies should however monitor the sole distributor closely. For example, any invoices submitted should be reviewed carefully. Contracts or payment terms should be clear to make sure there are no “hidden” profit margins for the distributors. The use of sub-distributors should be prohibited unless approved by the company. Due diligence should be carried out on all distributors.

### 5.3 Adequate financial and accounting controls over foreign subsidiaries

– In this case, it is clear that Stryker did not have adequate oversight of its foreign subsidiaries in high risk jurisdictions. The Order suggests that the employees in the China office were aware that sub-distributors were being used and aware that they were defrauding the company on a massive scale. Conducting audits and reviews of potentially risky transactions and accounts is key, and these should be conducted periodically. Invoices should also be checked for veracity and accuracy, and any large payments to distributors verified.

### 5.4 Red flags ignored by Stryker

– In this case, it is clear that Stryker did not heed the red flags and took no steps to find out whether improper payments had been made by the Kuwait Distributor, even when it received a complaint from a former employee of the Kuwait Distributor alleging that the Kuwait Distributor paid bribes when selling Stryker products. After learning these facts, Stryker should have conducted its own investigation into the payments made to the Kuwait Distributor.

### 5.5 Conferences organized for HCPs and expenses incurred always warrant careful review

– Companies should always review the expenses incurred for conferences organized for HCPs. Multiple enforcement actions suggest that this is a common way for third parties to funnel bribes to HCPs. Companies should conduct regular audits on third parties. It is highly recommended that an audit clause be included in any contract with a third party so that the company can investigate when there is a suspicion of bribery.

# Vantage Drilling International



## 1. Introduction

1.1 On November 19, 2018, Vantage Drilling International (**Vantage**) agreed to disgorge USD5m to the SEC to resolve charges that Vantage Drilling Company (**VDC**), a predecessor of Vantage, had violated the internal controls provision of the FCPA. As a result of its internal controls failures, VDC had “created a risk” that substantial payments were indirectly made to officials at Petroleo Brasileiro SA Petrobras (**Petrobras**), the Brazilian state-owned oil and gas company, through VDC’s external director and third parties without VDC’s knowledge. Vantage received a declination from the DOJ in August 2017.



## 2. Jurisdictional basis for the Administrative Proceeding

2.1 VDC was an offshore drilling corporation organized in the Cayman Islands, headquartered in Houston, Texas, and traded on the NYSE before commencing liquidation proceedings in December 2015 in the Cayman Islands.

2.2 Until February 2016, Vantage was a subsidiary of VDC. It now owns and controls all of the assets and operations of VDC. Vantage is a corporation organized in the Cayman Islands and headquartered in Houston, Texas.



## 3. Summary background

- 3.1 The case primarily concerns violations of the internal controls provisions of the FCPA relating to various transactions between VDC and its former director, largest shareholder and only supplier of drilling assets. VDC also failed to implement appropriate controls in relation to its third-party marketing agents.
- 3.2 The SEC order states that, according to several agreements entered into between VDC and a newly appointed external director who had been identified as a potential investor and supplier to VDC (the **Director**) over the 2007-2008 time period, VDC paid the Director USD56m in cash, VDC acquired the rights to purchase the Director’s drilling assets, the Director became the sole source supplier of drillships to VDC, and the Director became the single largest shareholder of VDC. In return, the Director was appointed to the VDC board. These arrangements were entered into without any internal accounting controls being in place, and without VDC conducting any due diligence on the Director or his related companies. These violations occurred against a backdrop where VDC had an ineffective anticorruption compliance program, according to the SEC.
- 3.3 As a result of these internal control failures, VDC made substantial payments to the Director that, among other things, created a risk that VDC was providing or reimbursing funds that the Director intended to use to make improper payments to officials at Petrobras in connection to VDC obtaining an 8-year drilling services contract valued at over USD1.8bn that benefited both the Director, as the supplier of the drilling asset, and VDC.



## 4. Detailed background

### 4.1 VDC's relationship with the Director

- (a) VDC was established in 2006. During 2007, VDC identified the Director as a prospective investor and supplier to VDC.
- (b) Through a number of agreements with the Director, VDC acquired the rights to purchase the Director's drilling assets, including an existing drillship known as the Titanium Explorer. In return, the Director was appointed to the board, paid USD56m in cash, and acquired 40% of VDC's common stock during 2007-2008.
- (c) VDC did not conduct any due diligence regarding the Director's ability to fulfil his contractual obligations or with regard to his related companies before acquiring the drilling assets and appointing the Director to the board. Furthermore, VDC relied on the Director as its only source of drilling equipment.

### 4.2 Misrepresentation by the Director

- (a) VDC wanted to purchase another drillship, the Platinum Explorer, from the Director. The Platinum Explorer was at the time under construction in a Korean shipyard. The Director misrepresented to VDC the payment plan with the shipyard for the Platinum Explorer, stating that he needed to make payments to the shipyard in advance of receiving a corresponding amount from VDC. In September 2008, VDC provided the Director with USD32m to pay an instalment to the Korean shipyard. VDC later learned that the Korean shipyard had granted an extension to the Director and the instalment was not due in September. VDC did not review the internal accounting controls or the payment to the Director despite the Director's misrepresentation.

- (b) Ultimately, VDC was unable to obtain financing for the purchase of the Titanium Explorer outright. Instead, VDC announced in November 2008 that the Director would continue to wholly own the Titanium Explorer but that the Director would engage and pay VDC to oversee construction of and then operate the drillship. The Director also authorized VDC to market the Titanium Explorer to potential clients.

### 4.3 The Titanium Explorer Contract and the Improper Payments

- (a) In 2007, VDC's CEO contacted a Brazilian third-party agent (**Agent**) to assist in VDC's marketing to Petrobras. VDC policies required that due diligence be conducted before engaging any third party agents and that there be safeguards against improper payments in place. Neither was done before engaging the Agent.
- (b) The Agent was soon assisting VDC in responding to a marketing inquiry from Petrobras in August 2008 seeking proposals from drilling operators who could deliver a certain type of deepwater drillship (the **Contract**). During the bidding process for the Contract, the Agent was contacted by an intermediary (**Intermediary A**), who identified himself as an agent of a senior Petrobras official. Intermediary A said the Contract would be awarded to VDC in return for a payment to the senior Petrobras official. The Agent was later introduced to another intermediary (**Intermediary B**) by Intermediary A. Intermediary B explained that part of the payment to senior Petrobras official was earmarked for the Brazilian politicians that appointed the senior Petrobras official.
- (c) In November 2008, the Agent met with the Director in New York City and asked whether the Director was willing to pay the senior Petrobras official. The meeting between the Agent and Director was arranged by VDC CEO and another VDC board member; neither the VDC CEO or board member knew that this was the purpose of the New York meeting. At the meeting in New York, the Agent also asked the Director to pay a commission to the Agent



and Intermediary B. The Director agreed to personally pay a total of USD31m (approximately 1.7% of the expected contract value) to the senior Petrobras official and the Agent in three instalments:

- (i) USD6,200,000 upon signing the Contract;
  - (ii) USD4,650,000 six months after the Contract was signed; and
  - (iii) USD4,650,000 when the drillship began working for Petrobras.
- (d) Other meetings were held and payments arranged by the Director to other Petrobras officials in order to secure the Contract.
- (e) VDC did not respond to various red flags that would have alerted them to the conduct of the Director, including an email inquiry from a Brazilian journalist asking for VDC's comments on the alleged arrangement.
- (f) In February 2009, VDC signed the Contract. VDC agreed with the Director that VDC would send the Director all revenue received from Petrobras under the Contract and that the Director could continue to pay instalments to the Korean shipyard for the construction of the drillship.
- (g) VDC's internal accounting controls in regards to transactions with Director were stated by the SEC order to be insufficient in relation to the heightened risk of conducting business in the oil and gas industry in Brazil. The SEC stated that "the lack of internal accounting controls surrounding VDC's payments to [the Director] increased the risk that VDC provided or reimbursed [the Director] for the funds used to make the corrupt payments."



## 5. Key takeaways

### 5.1 FCPA violations based only on internal control

**failures** – This is an extremely rare case of the FCPA violations only being based on the FCPA's internal controls provisions. Usually, you see books and records *and* internal controls violations.

### 5.2 No charge of bribery, but disgorgement still

**obtained** – This is another example of the SEC obtaining disgorgement in the absence of a finding of violations of the anti-bribery provisions of the FCPA. This cuts against the idea that disgorgement is an equitable remedy designed to deprive defendants of the proceeds of their wrongful conduct.

**5.3 Inability to pay** – This is a case of the SEC taking into account a company's inability to pay. The SEC order states: "[I]n determining the disgorgement amount and not to impose a penalty, the Commission has considered Vantage's current financial condition and its ability to maintain necessary cash reserves to fund its operations and meet its liabilities." The TLI case was another example of such an analysis in 2018.

### 5.4 Creating a risk of bribery can violate the FCPA

– VDC's failure to maintain effective internal controls meant improper payments could be funnelled to government officials without VDC's knowledge. The ineffective accounting controls created a risk of bribery at the company. In recent years, the SEC has developed a broad definition of "books, records and accounts" and, more significantly, has charged parties with FCPA violations where they have allegedly "created a heightened risk" environment for bribery and corrupt conduct through what is deemed by the SEC to be deficient compliance policies, procedures and internal controls.

### **5.5 Monitor and audit internal policies, procedures and accounting controls for effectiveness and respond to audit findings**

– Even though VDC had internal accounting controls which prohibit improper payments to officials through third parties, the SEC found that VDC's internal accounting controls were inadequate and ignored by VDC staff. The SEC and DOJ will look to the effectiveness of your internal controls. Having anti-bribery and corruption audit and review findings that have tested the effectiveness of your controls, along with evidence you have responded to those findings and remediated deficiencies, will assist should you come under government scrutiny.

**5.6 Due diligence on agents and intermediaries** – The Agent and intermediaries were used by the Director to make illicit payments to the senior Petrobras official and others at Petrobras. VDC had policies regarding the due diligence that should be conducted on agents before they are engaged. In this case, VDC ignored its internal policies and hired the Agent without conducting any due diligence. Due diligence of agents should always be conducted and high risk agents, especially those who have a connection with government officials, should be reviewed carefully. Payments made to agents also warrant periodic monitoring.

### **5.7 Corrupt behavior ignored by VDC despite red flags**

– In this case, it is clear that VDC did not heed the red flags present and took no steps to find out whether the payments to the Director and the Agent were being funnelled as bribes to government officials. Upon learning of these allegations and red flags, and knowing the high risk environment in which it was operating, VDC should have conducted its own investigation into the payments made to the Director and the Agent.

### **5.8 Provide compulsory compliance training for all senior members, including the board of directors**

– All senior members of a company should be required to attend relevant compliance training to ensure that they understand the company's internal policies and procedures. The training should be tailored to the senior board members with an emphasis on the different scenarios that may arise and the penalties for violating the company's policies. Such training is particularly important in high risk jurisdictions such as Brazil.



# Polycom Inc.



## 1. Introduction

1.1 In December 2018, Polycom Inc. (**Polycom**) received a declination with disgorgement from the DOJ (December 20) consistent with the FCPA Corporate Enforcement Policy and entered into an administrative order with the SEC (December 26), agreeing to pay approximately USD36.6m in disgorgement and penalties for violations of the FCPA. The disgorgement and penalties relate to the conduct of employees of Polycom's subsidiary in China, Polycom Communications Solutions (Beijing) Co., Ltd. (China) (**Polycom China**).



## 2. Jurisdictional basis

2.1 Polycom is a Delaware corporation headquartered in San Jose, California. Its shares were traded on the NASDAQ from 1996 to 2016. In 2016, it was acquired by a private equity firm and then by Plantronics Inc. (**Plantronics**) on July 2, 2018. Polycom is now a wholly owned subsidiary of Plantronics and its stock is registered with the SEC.



## 3. Summary background

3.1 From 2006 to July 2014, Polycom's Vice President of China and several senior managers at its subsidiary provided significant discounts to Polycom's distributors with the knowledge and intention that the distributors would use the discounts to make payment to Chinese government officials in exchange for their assistance in obtaining orders for Polycom products.

3.2 These payments were then recorded by the subsidiary in a deal-tracking and email system in China, outside of Polycom's approved company email system. Sales personnel were instructed not to use their Polycom email addresses when discussing sales opportunities with distributors.

3.3 From September 27, 2012 to July 2014, Polycom earned approximately USD10.7m from its Chinese subsidiary's practice of making and concealing improper payments to Chinese government officials.

3.4 Although Polycom had a system of internal controls, these were circumvented by its Chinese sales operations. As such, Polycom failed to maintain a sufficient system of internal accounting controls and lacked an effective anti-corruption compliance system.



## 4. Detailed background

4.1 Polycom sells communications equipment in China through its subsidiary, Polycom China. Polycom China sells Polycom products to distributors, who sell products to resellers, who then sell the products to users. To increase business from public-sector customers, Polycom's Vice President of China facilitated the payment of bribes to Chinese government officials via Polycom's distributors.

4.2 From 2006 to July 2014, the SEC found that distributors would offer cash payments to government officials who influenced purchasing decisions. When distributors sought to make these payments, they would request Polycom to provide a discount on the equipment to be sold, equivalent to the amount paid to the Chinese government official.

4.3 The SEC found that senior management knew these discounts were not passed on to the final customer and were instead used to cover the cost of payments to officials.

- 4.4 Under Polycom's policies and procedures, all Polycom sales personnel were required to enter details of sales opportunities and deals into a centralized "customer relations management database" (**Centralized Database**). To hide the payment of bribes, Polycom China's senior managers instead directed sales personnel to enter details into a separate, parallel system unknown to personnel outside of China. The discounts requested by distributors were recorded in this system rather than the Centralized Database, and senior managers approved these discounts with the knowledge they would be used to pay bribes. Polycom's Vice President of China also maintained spread sheets recording the details of these improper payments.
- 4.5 At the same time, entries were recorded in the Centralized Database, with discounts falsely attributed to legitimate purposes. For example, in connection to a project with a state-owned entity, a discount of RMB 60,000 was authorized in order for Polycom China's channel partner to provide a bribe to a Chinese government official who could assist in securing a purchase agreement. In Polycom's Vice President of China's spreadsheet, the purpose of the discount was recorded as "in order to thank for help, we promised to give him 60,000 RMB." In the Centralized Database, however, the reason provided for the discount was competition with another provider.
- 4.6 In three other instances, authorizations of improper payments through discounts were recorded in the Centralized Database as "end user fees" or "competition" with two other communications products providers. These were for payments in the amount of RMB 170,000 in one, RMB 850,000 in another, and multiple payments of RMB 20,000, RMB 70,000 and RMB 200,000 in a third.
- 4.7 Discounts provided which were above a certain threshold had to be approved by Singapore-based personnel employed by another wholly owned Polycom subsidiary rather than Polycom China's senior managers. When this was the case, Polycom China's senior managers would cite competition, end-user budget constraints or other legitimate reasons as explanations for the discount. Singapore personnel were therefore unaware that several of the discounts Polycom China provided were being used to fund bribes.
- 4.8 During this time, sales personnel at Polycom China were also directed to use non-Polycom email addresses when discussing deals with distributors. From September 27, 2012 to July 2014, Polycom earned approximately USD10.7m attributable to Polycom China's bribes.



## 5. Key takeaways

### 5.1 Failure to implement sufficient internal accounting controls and keep accurate books and records

– Polycom did not have adequate oversight over its foreign subsidiaries in high risk jurisdictions. Polycom failed to maintain effective internal controls to detect whether any reasons for discounts either entered in the Centralized Database, or given to Singapore personnel, were accurate. This failure to maintain sufficient internal controls allowed Polycom China to use product discounts as a vehicle for funding improper payments to government officials.

**5.2 Due diligence on sales agents and distributors** – In a 2013 due diligence procedure, Polycom became aware of allegations that a distributor used by Polycom China had, on a deal several years earlier which did not involve Polycom, made improper payments to a Chinese government official. Polycom failed to complete its due diligence review of the distributor and allowed Polycom China to continue using the distributor. Polycom China used many of its distributors to make illicit payments to government officials. Due diligence of sales agents and distributors should always be conducted and high risk agents reviewed and followed up by the compliance team. Discounts given to agents and distributors warrant periodic monitoring.

**5.3 Provide compulsory compliance training for all personnel, including senior managers** – In this case the SEC found that Polycom had failed to translate certain anticorruption training materials into the local language for Polycom China. Polycom also did not ensure Polycom China personnel attended anticorruption trainings. All personnel should be required to attend relevant compliance training to ensure that they understand the company's internal policies and procedures and policies should be available in the local language. For senior managers the training should be tailored, with an emphasis on the different scenarios and penalties for violating the company's policies. Such training is particularly important in high risk jurisdictions such as China.

**5.4 Use of non-company email and systems** – The details in the SEC order are interesting as they highlight one of the common compliance risks faced by companies operating in developing markets, and that's the use of non-company email and communication systems. WeChat, Whatsapp, Telegram, Line and other such services are prevalent in many developing markets and used by sales teams and other employees to communicate on a daily basis. There can be legitimate

reasons for the use of such services, but from a compliance perspective the use of these services runs the risk that employees will be able to freely communicate among themselves and with third parties about wrongful conduct and that such communications will not be discoverable by either the company or an investigating government authority. In fact, the DOJ has recognised this challenge in the FCPA Corporate Enforcement Policy. This recognition has likely been shaped, in part, by past DOJ experiences with evidentiary trails hitting a dead-end with third-party messaging platforms. The FCPA Corporate Enforcement Policy states that certain compliance measures "will be required for a company to receive full credit for timely and appropriate remediation" including "prohibiting the improper destruction or deletion of business records, including prohibiting employees from using software that generates but does not appropriately retain business records or communications."

**5.5 Distributor discounts** – Distributors have been a focus of several FCPA enforcement actions in 2018. Make sure your business understands what discounts are given, why and how, and make sure you have controls and oversight mechanisms built around the giving of discounts.

**5.6 Dig deeper when looking at the reasoning behind discounts** – Related to the above point, compliance oversight can be difficult and time consuming when it comes to understanding discounts, but the fact that looking behind the reasons provided by your team for a discount might be challenging is not a reason not to monitor the what, why and how of discounting, particularly in high risk markets.

# Centrais Elétricas Brasileiras S.A. – Eletrobras



## 1. Introduction

1.1 On December 26, 2018, Brazil's Centrais Elétricas Brasileiras S.A. (**Eletrobras**) agreed to pay USD2.5m to the SEC to resolve charges that it violated the books and records and the internal accounting controls provisions of the FCPA uncovered as part of the wider investigation connected to Operation Car Wash. The DOJ declined to prosecute Eletrobras.



## 2. Jurisdictional basis

2.1 Eletrobras is a Brazilian company with its shares traded on the NYSE. It is therefore deemed an "issuer" under the FCPA.



## 3. Summary background

3.1 Eletrobras, based in Rio de Janeiro, Brazil, carries on business in the generation, transmission and distribution of energy. The Brazilian federal government currently owns a 51% stake in Eletrobras and appoints seven of its 11 board members.

3.2 From approximately 2009 to 2015, former executive officers at Eletrobras Termonuclear S.A (**Eletronuclear**), Eletrobras' majority-owned nuclear power generation subsidiary, engaged in an illicit bid-rigging and bribery scheme involving the construction of a nuclear power plant (**UTN Angra III**). These executive officers used their influence at Eletronuclear to aid a bid-rigging scheme among certain private Brazilian construction companies.

3.3 The officers also misused their official positions in authorizing unnecessary contractors and inflating the cost of Eletronuclear's infrastructure project. In return, the construction companies involved in the scheme paid the former Eletronuclear officers approximately USD9m.

3.4 The corruption scheme at Eletronuclear caused misstatements in Eletrobras' books and records because Eletronuclear recorded payments made to UTN Angra III contractors, a percentage of which was used for bribes, as money legitimately spent to acquire and improve assets.



## 4. Detailed background

4.1 According to the settlement, from about 2009 until 2015, the former Eletronuclear officers allowed Eletronuclear to approve and pay invoices from contractors involved in the bid-rigging and bribery scheme relating to the UTN Angra III project.

4.2 In effecting the bid-rigging and bribery scheme, the former Eletronuclear officers involved used their influence and official positions to authorize certain contractors, services and expenses connected to the scheme. The construction companies then overcharged Eletronuclear, and used the overpayment to fund the bribes to executives and political parties.

4.3 The improper payments made by the construction companies to Brazilian officials were funded, in part, using inflated contract prices or sham invoices that contractors involved in the UTN Angra III scheme submitted to Eletronuclear for payment. For example, at least 28 invoices were from a contractor used as a conduit for the bribes paid to the former Eletronuclear president.

4.4 The construction company executives agreed to pay 2% of the UTN Angra III contract value to officials associated with two of Brazil's largest political parties (1% each). The former Eletronuclear president received approximately USD4.1m relating to UTN Angra III while the former Eletronuclear officers collectively received approximately USD4.9m.

4.5 Eletrobras failed to devise and maintain a sufficient system of internal accounting controls in part because of weaknesses that allowed employees at the subsidiary level to ignore prohibitions against direct payments to subcontractors and allow the payment of upfront costs for work not performed. This occurred against a backdrop where Eletrobras' compliance policies and procedures were not specifically tailored to the inherent risks associated with Eletrobras' business operations.



## 5. Key takeaways

**5.1 Insufficient oversight over subsidiaries** – As with many FCPA enforcement actions, the parent company did not have adequate oversight over the actions of its subsidiary. Particularly where the subsidiary had influence over large public bids and could influence their outcome, it is essential that such processes are adequately supervised and controlled for corruption risk. Controls set up at the subsidiary level to prevent direct payments to subcontractors and allow payment for upfront costs were easily circumvented and used to fund the bribery scheme. Where such circumventions go undetected, it is clear that the company's controls are failing and require review and enhancement.

**5.2 Involvement of senior management** – Those implicated in the bribery scheme included the now former president of Eletronuclear who received bribes from construction company executives totalling USD4.1m relating to UTN Angra III. The other former officers at Eletronuclear collectively received approximately USD4.9m. All members of Eletrobras and its subsidiaries, particularly its senior members, should be required to attend compliance and anti-corruption training to ensure they understand the company's internal policies and procedures. Training of this nature is particularly important in high risk jurisdictions such as Brazil.

**5.3 State-owned enterprise risk** – As an SOE, employing government officials, Eletrobras was at a heightened ABC risk. Its employees also exercised significant control over significant bidding processes, involving lucrative government contracts. The subsidiary partook in a scheme that allowed it to funnel bribes from inflated contract prices and sham invoices to its senior executives and government officials. Companies that employ government officials or are SOEs should be vigilant to ensure that they are not exposed to unnecessary corruption risks and monitor their operations carefully.

**5.4 Internal policies, procedures and accounting controls** – The SEC found that Eletrobras' internal accounting controls were inadequate. Eletrobras' anti-corruption policies and accounting controls relied, in part, on "general or boilerplate prohibitions that did not apply to all employees or were ignored." For example, Eletrobras adopted a code of ethics in 2005 to ensure that competitiveness and profitability did not override ethical behavior, but it applied only to the holding company and made no mention of the subsidiaries and special purpose entities. Policies have to be applied and adopted at the group level, and apply equally to all subsidiaries, particularly those operating in high risk industries and in a high risk jurisdiction such as Brazil.

# Contacts

If you wish to receive more information on the topics covered in this publication, you may contact your regular Allen & Overy contact or any of the following people:

## AMERICAS



**David Esseks**

Partner, New York  
Tel +1 212 610 6326  
david.esseks@allenovery.com



**William White**

Partner, Washington, D.C.  
Tel +1 202 683 3876  
william.white@allenovery.com



**Eugene Ingoglia**

Partner, New York  
Tel +1 212 610 6369  
eugene.ingoglia@allenovery.com



**Ken Rivlin**

Partner, New York  
Tel +1 212 610 6460  
ken.rivlin@allenovery.com



**Bruno Soares**

Partner, São Paulo  
Tel +55 11 3848 8755  
bruno.soares@allenovery.com



**Claire Rajan**

Senior Counsel,  
Washington, D.C.  
Tel +1 202 683 3869  
claire.rajan@allenovery.com



**Maura Rezendes**

Senior Counsel,  
Washington, D.C.  
Tel +1 202 683 3864  
maura.rezendes@allenovery.com



**Michael Westfal**

Associate, New York  
Tel +1 212 610 6418  
michael.westfal@allenovery.com



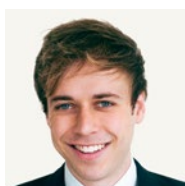
**Laila Metjahic**

Associate, New York  
Tel xxx  
laila.metjahic@allenovery.com



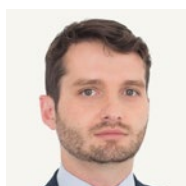
**Danna Seligman**

Associate, Washington, D.C.  
Tel +1 202 683 3894  
danna.seligman@allenovery.com



**Alexander Calthrop**

Associate, New York  
Tel +1 212 756 1155  
alexander.calthrop@allenovery.com



**André Teixeira**

Associate, São Paulo  
Tel +55 11 3848 8772  
andre.teixeira@allenovery.com



**Eduardo Kappel**

Law Clerk, São Paulo  
Tel +55 11 3848 8771  
eduardo.kappel@allenovery.com

## MIDDLE EAST AND AFRICA



**Gerhard Rudolph**

Partner, Johannesburg  
Tel +27 10 597 9888  
gerhard.rudolph@allenovery.com



**Callum O'Connor**

Counsel, Johannesburg  
Tel +27 10 597 9929  
callum.oconnor@allenovery.com



**Yassir Ghorbal**

Partner, Casablanca  
Tel +212 520478000  
yassir.ghorbal@allenovery.com



**Yaccine Francis**

Partner, Dubai  
Tel +971 4 426 7228  
yaccine.francis@allenovery.com



## ASIA PACIFIC



**Jason Gray**

Partner APAC Head of FCPA/  
U.S. White-Collar Crime  
Tel +612 9373 7674  
HK Tel +852 2974 7139  
Mob +61 488 003 786  
jason.gray@allenoverly.com



**David Shen**

Partner, Shanghai  
Tel +86 21 2036 7138  
david.shen@allenoverly.com



**Jane Jiang**

Partner, Shanghai  
Tel +86 21 2036 7018  
jane.jiang@allenoverly.com



**Simon Clarke**

Partner, Hong Kong  
Tel +852 2974 7202  
simon.clarke@allenoverly.com



**Fai Hung Cheung**

Partner, Hong Kong  
Tel +852 2974 7207  
fai.hung.cheung@allenoverly.com



**Duc Tran**

Partner, Ho Chi Minh City  
Tel +84 28 6288 4949  
duc.tran@allenoverly.com



**Harun Reksodiputro**

Partner, Jakarta  
Tel +62 21 2995 1711  
harun.reksodiputro@allenoverly.com



**Dumnern Subpaisarn**

Partner, Bangkok  
Tel +662 263 7694  
dumnern.subpaisarn@allenoverly.com



**Cliff Chow**

Of Counsel, Hong Kong  
Tel +852 2974 7057  
cliff.chow@allenoverly.com



**Shuhui Kwok**

Senior Associate, Singapore  
Tel +65 6671 6065  
shuhui.kwok@allenoverly.com



**Hai Ha**

Senior Associate,  
Ho Chi Minh City  
Tel +84 28 6288 4920  
hai.ha@allenoverly.com



**Sam Samid**

Associate, Jakarta  
Tel +62 21 29951727  
sam.samid@allenoverly.com



**Edward Einfeld**

Senior Associate, Sydney  
Tel +61 2 9373 7753  
edward.einfeld@allenoverly.com



**Caroline Marshall**

Senior Associate, Sydney  
Tel +612 9373 7690  
caroline.marshall@allenoverly.com



**Evelyn Mo**

Registered Foreign Lawyer,  
NY, Hong Kong  
Tel +852 2974 6913  
evelyn.mo@allenoverly.com



**Dylan Ding**

Associate, Beijing  
Tel +86 10 6535 4378  
dylan.ding@allenoverly.com

## EUROPE

**Igor Gorchakov**

Partner, Moscow

Tel +7 495 662 6547  
igor.gorchakov@allenoverly.com**Wolf Bussian**

Partner, Frankfurt

Tel +49 69 2648 5633  
wolf.bussian@allenoverly.com**Jan Erik Windthorst**

Partner, Frankfurt

Tel +49 69 2648 5633  
jan-erik.windthorst@allenoverly.com**Hendrik Jan Biemond**

Partner, Amsterdam

Tel +31 20 674 1465  
hendrikjan.biemond@allenoverly.com**Joost Everaert**

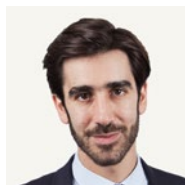
Partner, Brussels

Tel +32 2 780 26 06  
Joost.Everaert@allenoverly.com**Martin Magal**

Partner, Bratislava

Tel +421 2 5920 2412  
martin.magal@allenoverly.com**Denis Chemla**

Partner, Paris

Tel +33 01 40 06 53 03  
denis.chemla@allenoverly.com**Dan Benguigui**

Counsel, Paris

Tel +33 01 40 06 53 17  
dan.benguigui@allenoverly.com**Markéta Císařová**

Senior Associate, Prague

Tel +420 222 107 172  
marketa.cisarova@allenoverly.com

## UNITED KINGDOM

**Calum Burnett**

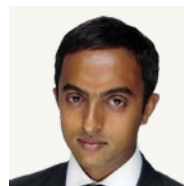
Partner, London

Tel +44 20 3088 3736  
calum.burnett@allenoverly.com**Eve Giles**

Partner, London

Tel +44 20 3088 4332  
eve.giles@allenoverly.com**Lawson Caisley**

Partner, London

Tel +44 20 3088 2787  
lawson.caisley@allenoverly.com**Arnondo Chakrabarti**

Partner, London

Tel +44 20 3088 4424  
arnondo.chakrabarti@allenoverly.com**Matthew Townsend**

Partner, London

Tel +44 20 3088 3174  
matthewtownsend@allenoverly.com**Stacey McEvoy**

Senior Associate, London

Tel +44 20 3088 3009  
stacey.mcevoy@allenoverly.com

The authors wish to acknowledge the contribution of A&O clerks James Clark, Brigitte Samaha, Pamela Vassil and Tess Wardrop and paralegal Patrick Hendy in the preparation of this publication.

# About Allen & Overy's Global FCPA and Anti-Corruption Team

Allen & Overy's global anti-corruption team includes the leading defence team in the UK, former U.S. prosecutors in New York, former SEC Enforcement Division attorneys, and a worldwide network of litigators and former prosecutors with experience investigating allegations of bribery in foreign countries.

Allen & Overy's global reach is both geographic and cultural, as the firm is expert in local law in each of the 30 jurisdictions in which we have offices, including expertise in local anti-bribery laws, data privacy laws, and investigative rules and procedures. The result is an integrated global team that can efficiently gather facts and analyse potential corruption issues globally, and then credibly present that analysis to regulators in the U.S., UK and around the world.

## MANAGING CORRUPTION EXPOSURE

Our global investigations and enforcement team has extensive worldwide experience of advising clients with respect to the FCPA, UK Bribery Act and other international anti-corruption laws and restrictions, and offers a strong integrated team that is committed to providing aggressive and cutting-edge service.

## *A global team: quick facts*

Our **UK team** is the leading anti-corruption defence practice in London and is ranked in tier 1 for corporate crime/investigations in both Chambers and Legal 500.

Our **U.S. team** includes three former federal prosecutors who are experts in the U.S. Foreign Corrupt Practices Act as well as U.S. lawyers on the ground in Asia Pacific.

Our team in **Asia Pacific**, the **Middle East** and **Africa** has extensive experience in cross-border investigations on behalf of U.S., Europe and Asia-based clients.

Our team in **Europe** includes a former Chief Public Prosecutor in the special corporate fraud team of the Dutch Prosecution Service and other experienced litigators and investigators in all our major offices.

Our anti-corruption practice is seamlessly integrated around the world in order to efficiently handle investigations wherever a company's business operations are located.

---

## GLOBAL PRESENCE

---

Allen & Overy is an international legal practice with approximately 5,500 people, including some 550 partners, working in 44 offices worldwide. Allen & Overy or an affiliated undertaking has an office in each of:

Abu Dhabi	Bucharest (associated office)	Ho Chi Minh City	Moscow	Seoul
Amsterdam	Budapest	Hong Kong	Munich	Shanghai
Antwerp	Casablanca	Istanbul	New York	Singapore
Bangkok	Doha	Jakarta (associated office)	Paris	Sydney
Barcelona	Dubai	Johannesburg	Perth	Tokyo
Beijing	Düsseldorf	London	Prague	Warsaw
Belfast	Frankfurt	Luxembourg	Riyadh (cooperation office)	Washington, D.C.
Bratislava	Hamburg	Madrid	Rome	Yangon
Brussels	Hanoi	Milan	São Paulo	

**Allen & Overy** means Allen & Overy and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy's affiliated undertakings.

© Allen & Overy 2019 | CA1901056